NEWQUAY TOWN COUNCIL DATA GOVERNANCE POLICIES

Revision History

Version	***Revision Date***	***Revised by***	***Section Revised***
2.1	17/06/2020	C Rowley	Whole Document
2.2	16/01/2023	C Rowley	Reviewed post L&R
2.3	15/04/2024	W Mercer	Review & Add 28: AI

Document Control

Document Owner:	***Document No:***	***Status:***	***Date Approved:***
Newquay Town Council	***DGP***	Adopted	***03/05/23***

Security Classification:	***Next Review Date:***	***Version:***	***Department:***
High	***2025~~ATM-2021~~***	V2.3~~2~~	IT Service

Contents

1 Policy Statement 9
2 Purpose 9
3 Scope 10
3.1 Definitions 10
4 Data Protection Background 12
4.1 National Data Protection Law 12
4.2 General Data Protection Regulation (GDPR) 12
4.2.1 Personal Data 13
4.2.2 The GDPR Principles 13
4.3 The Information Commissioners Office (ICO) 14
4.4 Data Protection Officer 15
5 Objectives 16
6 Governance Procedures 17
6.1 Accountability & Compliance 17
6.1.1 Privacy by Design 18
6.1.2 Information Audit 21
6.2 Legal Basis for Processing *(Lawfulness)* 21
6.2.1 Processing Special Category Data 22
6.2.2 Records of Processing Activities 24
6.3 Codes of Conduct & Certification Mechanisms 24
6.4 Third-Party Processors 25
6.5 Data Retention & Disposal 27
7 Data Protection Impact Assessments (DPIA) 27
8 Data Subject Rights Procedures 28
8.1 Consent & The Right to be Informed 28
8.1.1 Consent Controls 30
8.1.2 Child's Consent 31
8.1.3 Alternatives to Consent 31
8.1.4 Information Provisions 32
8.2 Privacy Notice 33
8.3 Personal Data Not Obtained from the Data Subject 35

8.3.1 Employee Personal Data 36
8.4 The Right of Access....36
8.4.1 Subject Access Request 37
8.5 Data Portability 37
8.6 Rectification & Erasure 38
8.6.1 Correcting Inaccurate or Incomplete Data 38
8.6.2 The Right to Erasure....39
8.7 The Right to Restrict Processing....39
8.8 Objections and Automated Decision Making....40
9 Oversight Procedures 42
9.1 Security & Breach Management 42
10 Transfers & Data Sharing....42
11 Audits & Monitoring 43
12 Training 44
13 Penalties....44
14 Overall Responsibilities 45
15 Data Control & Passwords 45
15.1 Briefing 45
15.2 Section Purpose 46
15.3 Section Scope....46
15.4 Section Objectives....47
16 Section Procedures, Controls and Measures....47
16.1 Logical Access Control 48
16.1.1 Role-Based Access 48
16.1.2 Manager Access 48
16.1.3 Individual Access 49
16.2 Passwords....49
16.2.1 Password Creation & Change 49
16.2.2 Default Passwords....50
16.2.3 Protecting Passwords....50
16.3 User ID's and Badges 51
16.4 Privileged Accounts 51

16.5 Authorised Access 52
16.5.1 Login Controls 52
16.5.2 Credentials & Roles 52
16.6 Physical Access Controls 52
16.6.1 Door & Window Controls 53
16.6.2 Outside Opening Hours 53
16.6.3 Direct Access 53
16.7 Leavers & End of Contract 53
16.8 Section Responsibilities 54
17 Asset Management 54
17.1 Section Introduction 54
17.2 Section Definitions 55
17.3 Section Statement 55
17.4 Section Purpose 56
17.5 Section Objectives 56
17.6 Section Guidelines and Procedures 57
17.7 Register of Information Assets 57
17.8 Assigning Asset Owners 58
17.9 Unclassified & Short-Term Information Assets 58
17.10 Remote Access & Bring Your Own Device (BYOD) 58
17.11 Acceptable Use of Information Assets 59
17.11.1 Acceptable Use Standards 60
17.11.2 Internet & Email Usage 61
17.12 Removable Media 61
17.12.1 Using Removable Media Devices 62
17.13 Information Classification 63
17.14 Non-Disclosure & Confidentiality Agreements 64
17.15 Information Labelling, Handling and Disposal 64
17.15.1 Disposal of Assets 64
17.16 Section Responsibilities 65
17.17 Information Asset Owners (IAO) 65

17.17.1 Managers and Supervisors 65
18 Information Security 65
18.1 Section Introduction 65
18.2 Section Statement 66
18.3 Section Purpose 67
18.4 Section Objectives 67
18.5 Section Procedures & Guidelines 68
18.5.1 Security Classification 68
18.5.2 Access to Information 68
18.5.3 Secure Disposal of Information 68
18.5.4 Information on Desks, Screens and Printers 68
18.5.5 Data Encryption 69
18.5.6 Remote Access 71
18.5.7 Firewalls & Malware 71
18.6 Security Breach Management 72
18.6.1 Introduction 72
18.6.2 Breach Management Approach 72
18.7 PCI DSS Compliance 73
18.7.1 Definitions 73
18.7.2 PCI DSS Approach & Protocols 74
18.7.3 Card Storage & Disposal 75
18.8 Section Responsibilities 76
19 Publication Scheme & Freedom of Information Policy 76
19.1 Section Introduction 76
19.2 Scope of this Section 76
19.3 Model Publication Scheme 77
19.4 Classes of Information 77
19.5 Methodology Statement 78
19.6 Potential Charges for Information 78
19.7 Data in alternative Formats 79
19.8 Freedom of Information 79
20 Risk Management 79

20.1 Section Statement 79
20.2 Purpose 80
20.2.1 What is Risk? 80
20.3 Objectives 81
20.4 Data Protection Risks 82
20.4.1 Data Protection Impact Assessment (DPIA) 82
20.4.2 Data Protection Officer (DPO's) 82
20.5 Approach to Risk Management 83
20.5.1 Response to Risk 84
20.6 First Line Procedures 84
20.6.1 Identify the Risk 84
20.6.2 Assess the Risk 85
20.6.3 Manage the Risk 87
20.7 Risk Register 90
20.8 Second Line Procedures 90
20.8.1 Review & Monitor the Risks 90
20.9 Third Line Procedures 91
20.9.1 Audits 91
20.10 Documenting Risk Assessments 92
20.11 Section Responsibilities 92
20.11.1 Associated Documents with this section 93
21 Data Breach 93
21.1 Section Statement 93
21.2 Section Purpose 94
21.3 Data Security & Breach Requirements 94
21.3.1 Objectives 95
21.4 Data Breach Procedures & Guidelines 95
21.4.1 Breach Monitoring & Reporting 96
21.4.2 Breach Incident Procedures 96
21.4.3 Breach Risk Assessment 97
21.5 Breach Notifications 98

21.5.1 Supervisory Authority Notification 99
21.5.2 Data Subject Notification 100
21.6 Record Keeping 100
21.7 Responsibilities 100
22 Clear Desk Policy 101
23 Section Statement 101
23.1 Section Purpose 101
23.2 Section Objectives 101
23.3 Measures and Controls 102
23.3.1 Section Guidelines 103
23.4 Section Responsibilities 104
24 Secure Disposal 104
24.1 Section Statement 104
24.2 Purpose 104
24.3 Objectives 104
25 Guidelines & Procedures 105
25.1.1 Destruction and Disposal Of Records & Data 105
25.2 Responsibilities 107
26 Data Retention & Erasure 107
26.1 Section Statement 107
26.2 Purpose 108
26.3 Personal Information and Data Protection 108
26.4 Objectives 109
26.5 Guidelines & Procedures 110
26.5.1 Retention Period Protocols 111
26.5.2 Designated Owners 112
26.5.3 Document Classification 112
26.5.4 Suspension of Record Disposal for Litigation or Claims 113
26.5.5 Storage & Access of Records and Data 113
26.6 Expiration of Retention Period 114
26.6.1 Destruction and Disposal Of Records & Data 114
26.7 Erasure 115

26.7.1 Special Category Data 117
26.8 Compliance and Monitoring 118
26.9 Responsibilities 118
26.10 Retention Periods 118
27 E-mail Usage & Archiving 118
27.1 Section Introduction 118
27.2 Section Statement 119
27.3 Section Purpose 119
27.4 Email Use and Guidelines 119
27.4.1 Acceptable Use 119
27.4.2 Prohibited Use 120
27.4.3 Best Practice 120
27.5 Personal Email 121
27.6 Email Security 121
27.7 Email Archiving & Retention 122
27.8 Monitoring Email 122
27.9 Section Responsibilities 123
28 Artificial Intelligence at Work
28.1 Section Introduction
28.2 Acceptable Use
28.3 Unacceptable Use & Potential Risks
28.4 Mitigating Risk & Promoting Responsible Use
28.4.1 Mitigation
28.4.2 Prompt Engineering Best Practice
28.4.3 Intellectual Property & Copyright
28.4.4 Ethical AI Principles
28.5 Data Access Security in the Context of AI
29 Additional Information & Relevant Contact Information 124

1 POLICY STATEMENT

Newquay Town Council *(hereinafter referred to as the **"Council"**)* needs to collect personal information to effectively carry out our everyday business functions and activities and to provide the products and services defined by our business type. Such data is collected from employees, customers, suppliers and clients and includes *(but is not limited to),* name, address, email address, data of birth, IP address, identification numbers, private and confidential information, sensitive information and bank/credit card details.

In addition, we may be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however we are committed to processing all personal information in accordance with the ***General Data Protection Regulation (GDPR)***, ***Data Protection Act 2018 (DPA18)*** and any other relevant the data protection laws and codes of conduct *(herein collectively referred to as **"the data protection laws"**).*

The Council has developed policies, procedures, controls and measures to ensure maximum and continued compliance with the data protection laws and principles, including staff and Councillor training, procedure documents, audit measures and assessments. Ensuring and maintaining the security and confidentiality of personal and/or special category data is one of our top priorities and we are proud to operate a ***'Privacy by Design'*** approach, assessing changes and their impact from the start and designing systems and processes to protect personal information at the core of our business.

2 PURPOSE

The purpose of this policy is to ensure that the Council meets its legal, statutory and regulatory requirements under the data protection laws and to ensure that all personal and special category information is processed compliantly and, in the individuals, best interest.

The data protection laws include provisions that promote accountability and governance and as such the Council has put comprehensive and effective governance measures into place to meet these provisions. The aim of such measures is to ultimately minimise the risk of breaches and uphold the protection of personal data. This policy also serves as a reference document for employees and third parties on the responsibilities of handling and accessing personal data and data subject requests.

3 SCOPE

This policy applies to all members of the Council *(meaning permanent, fixed term, and temporary staff, councillors, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Council in the UK or overseas).* Adherence to this policy is mandatory and non-compliance could lead to disciplinary action / action in reference to the Code of Conduct.

3.1 DEFINITIONS

- ***"Biometric data"*** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
- ***"Binding Corporate Rules"*** means personal data protection policies which are adhered to by the Council for transfers of personal data to a controller or processor in one or more third countries or to an international organisation.
- ***"Consent"*** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- ***"Cross Border Processing"*** means processing of personal data which: -
    - takes place in more than one Member State; or
    - which substantially affects or is likely to affect data subjects in more than one Member State
- ***"Data controller"*** means, the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
- ***"Data processor"*** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- ***"Data protection laws"*** means for the purposes of this document, the collective description of the GDPR, Data Protection Act 2018 and any other relevant data protection laws that the Council complies with.
- ***"Data subject"*** means an individual who is the subject of personal data

- ***"GDPR"*** means the *General Data Protection Regulation (EU) (2016/679)*
- ***"Genetic data"*** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
- ***"Personal data"*** means any information relating to an identified or identifiable natural person *('data subject')*; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- ***"Processing"*** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- ***"Profiling"*** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
- ***"Recipient"*** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
- ***"Supervisory Authority"*** means an independent public authority which is established by a Member State
- ***"Third Party"*** means a natural or legal person, public authority, agency or body other than the data subject, under our direct authority

4 Data Protection Background

The UK initially had The Data Protection Act 1984 in place to regulate the use of processed information that related to individuals. However, in 1995 the introduction of EU Directive 95/46/EC which set aims and requirements for member states on the protection of personal data when processing or sharing, meant an updated Act was required.

The UK subsequently developed and enacted The Data Protection Act 1998 (DPA) to ensure that British law complied with the EU Directive and to provide those with obligations under the Act, with updated rules, requirements and guidelines for processing and sharing personal data.

2018 marked the 20th anniversary of the DPA enactment and whilst there have been periodical additions or alterations to the Act, technology has advanced at a far faster rate, necessitating new regulations for the current digital age. The past 20 years has also seen a vast increase in the number of businesses and services operating across borders, further highlighting the international inconsistency in Member States data protection laws.

For this reason, in January 2012, the European Commission proposed a new regulation applying to all EU Member States and bringing a standardised and consistent approach to the processing and sharing of personal information across the EU.

4.1 National Data Protection Law

As the Council is in the UK, we are obligated under the GDPR and the UK's Data Protection Act 2018 that implements the GDPR into UK law. Our data protection policies and procedures adhere to both the GDPR and Data Protection Act 2018 requirements, as applicable to our business type.

The GDPR came into effect on 25 May 2018 and as an EU Regulation, it has direct effect in UK law and automatically applies in the UK until it leaves the EU (or until the end of any agreed transition period, if it leaves with a deal). After this date, the UK government have already noted that the GDPR will form part of UK law under the European Union (Withdrawal) Act 2018, with some technical changes to make it work effectively in a UK context.

4.2 General Data Protection Regulation (GDPR)

The ***General Data Protection Regulation (GDPR) (EU)2016/679)*** was approved by the European Commission in April 2016 and applied to all EU Member States from the 25th May 2018. As a *'Regulation*' rather than a *'Directive'*, its rules apply directly to Member States, replacing their existing local

data protection laws and repealing and replacing Directive 95/46EC and its Member State implementing legislation.

As the Council processes personal information regarding individuals (*data subjects*), we are obligated under the General Data Protection Regulation (GDPR) to protect such information, and to obtain, use, process, store and destroy it, only in compliance with its rules and principles.

4.2.1 PERSONAL DATA

Information protected under the GDPR is known as *"personal data"* and is defined as: -

"Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

The Council ensures that a high level of care is afforded to personal data falling within the GDPR's **'special categories'** *(previously* ***sensitive personal data***), due to the assumption that this type of information could be used in a negative or discriminatory way and is of a sensitive, personal nature to the persons it relates to.

In relation to the 'Special categories of Personal Data' the GDPR advises that: -

"Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited – unless one of the Article 9 clauses applies."

4.2.2 THE GDPR PRINCIPLES

Article 5 of the GDPR requires that personal data shall be: -

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ***('lawfulness, fairness and transparency')***

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or

historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ***('purpose limitation')***

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ***('data minimisation')***

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ***('accuracy')***

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ***('storage limitation')***

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ***('integrity and confidentiality').***

Article 5(2) requires that *'the controller shall be responsible for, and be able to demonstrate, compliance with the data protection laws principles'* ***('accountability')*** and requires that firms ***show how*** they comply with the principles, detailing and summarising the measures and controls that they have in place to protect personal information and mitigate the risks of processing.

4.3 THE INFORMATION COMMISSIONERS OFFICE (ICO)

The Information Commissioners Office (ICO) is an independent regulatory office who report directly to Parliament and whose role it is to uphold information rights in the public interest. The legislation they have oversight for includes: -

- The Data Protection Act 2018
- General Data Protection Regulation
- The Privacy and Electronic Communication (EU Directive) Regulations 2003
- Freedom of Information Act 2000

- The Environmental Information Regulations 2004

The ICO's mission statement is *"to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals"* and they can issue enforcement notices and fines for breaches in any of the Regulations, Acts and/or Laws regulated by them.

Under the data protection laws the ICO, as the UK's data protection authority (*Supervisory Authority*), will have a similar role as previously, when it comes to oversight, enforcement and responding to complaints with regards to the data protection laws and those firms located solely in the UK.

The Council are registered with ICO and appear on the Data Protection Register as a Controller of personal information.

Our Data Protection Registration Number is Z8853965.

4.4 DATA PROTECTION OFFICER

Articles 37-39, and Recital 97 of the GDPR detail the obligations, requirements and responsibilities on firms to appoint a Data Protection Officer and specifies the duties that the officer themselves must perform.

A Data Protection Officer (DPO) must be appointed by a firm where: -

- The processing is carried out by a public authority or body *(except for courts acting in their judicial capacity)*
- the core activities of the controller/processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale
- the core activities of the controller/processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10

Where the Council has appointed a designated DPO, we have done so in accordance with the GDPR requirements and have ensured that the assigned person has an adequate and expert knowledge of data protection law. They have been assessed as being fully capable of assisting the Council in monitoring our internal compliance with the Regulation and supporting and advising employees and associated third parties with regards to the data protection laws and requirements.

For the DPO duties and responsibilities, please refer to our DPO Responsibilities document.

5 OBJECTIVES

We are committed to ensuring that all personal data processed by the Council is done so in accordance with the data protection laws and its principles, along with any associated regulations and/or codes of conduct laid down by the Supervisory Authority and local law. We ensure the safe, secure, ethical and transparent processing of all personal data and have stringent measures to enable data subjects to exercise their rights.

The Council has developed the below objectives to meet our data protection obligations and to ensure continued compliance with the legal and regulatory requirements.

The Council ensures that: -

- We protect the rights of individuals with regards to the processing of personal information
- We develop, implement and maintain a data protection policy, procedure, audit plan and training program for compliance with the data protection laws
- Every business practice, function and process carried out by the Council, is monitored for compliance with the data protection laws and its principles
- Personal data is only processed where we have verified and met the lawfulness of processing requirements
- We only process special category data in accordance with the GDPR requirements and in compliance with the Data Protection Act 2018 Schedule 1 conditions
- We record consent at the time it is obtained and evidence such consent to the Supervisory Authority where requested
- All employees are competent and knowledgeable about their GDPR obligations and are provided with in-depth training in the data protection laws, principles, regulations and how they apply to their specific role and the Council
- Individuals feel secure when providing us with personal information and know that it will be handled in accordance with their rights under the data protection laws
- We maintain a continuous program of monitoring, review and improvement with regards to compliance with the data protection laws and to identify gaps and non-compliance before they become a risk, affecting mitigating actions where necessary

- We monitor the Supervisory Authority, the **European Data Protection Board** (*formerly The Article 29 Working Party)* and any GDPR news and updates, to stay abreast of changes, notifications and additional requirements
- We have robust and documented Complaint Handling and Data Breach controls for identifying, investigating, reviewing and reporting any breaches or complaints with regards to data protection
- We have appointed a Data Protection Officer who takes responsibility for the overall supervision, implementation and ongoing compliance with the data protection laws and performs specific duties as set out under Article 37 of the GDPR
- We have a dedicated Audit & Monitoring Program in place to perform regular checks and assessments on how the personal data we process is obtained, used, stored and shared. The audit program is reviewed against our data protection policies, procedures and the relevant regulations to ensure continued compliance
- We provide clear reporting lines and supervision with regards to data protection
- We store and destroy all personal information, in accordance with our retention policy and schedule which has been developed from the legal, regulatory and statutory requirements and suggested timeframes
- Any information provided to an individual in relation to personal data held or used about them, with be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language
- Employees are aware of their own rights under the data protection laws and are provided with the Article 13/14 information disclosures in the form of a Privacy Notice
- Where applicable, we maintain records of processing activities in accordance with the Article 30 requirements
- We have developed and documented appropriate technical and organisational measures and controls for personal data security and have a robust Information Security program in place

6 Governance Procedures

6.1 Accountability & Compliance

Due to the nature, scope, context and purposes of processing undertaken by the Council, we carry out frequent risk assessments and information audits to identify, assess, measure and monitor the impact of such processing. We have implemented adequate and appropriate technical and organisational measures to

ensure the safeguarding of personal data and compliance with the data protection laws and can evidence such measures through our documentation and practices.

Our main governance objectives are to: -

- Educate senior management and employees about the requirements under the data protection laws and the possible impact of non-compliance
- Provide a dedicated and effective data protection training program for all employees
- Identify key stakeholders to support the data protection compliance program
- Allocate responsibility for data protection compliance and ensure that the designated person(s) has sufficient access, support and budget to perform the role
- Identify, create and disseminate the reporting lines within the data protection governance structure

The technical and organisational measures that the Council has in place to ensure and demonstrate compliance with the data protection laws, regulations and codes of conduct, are detailed in this document and associated information security policies.

6.1.1 PRIVACY BY DESIGN

We operate a *'Privacy by Design'* approach and ethos, with the aim of mitigating the risks associated with processing personal data through prevention via our processes, systems and activities. We have developed controls and measures *(detailed below*), that help us enforce this ethos.

Data Minimisation

Under Article 5 of the GDPR, principle (c) advises that data should be *'limited to what is necessary'*, which forms the basis of our minimalist approach. We only ever obtain, retain, process and share the data that is essential for carrying out our services and/or meeting our legal obligations and only retain data for as long as is necessary.

Our systems, employees, processes and activities are designed to limit the collection of personal information to that which is directly relevant and necessary to accomplish the specified purpose. Data minimisation enables us to reduce data protection risks and breaches and supports our compliance with the data protection laws.

Measures to ensure that only the necessary data is collected includes: -

- Electronic collection *(i.e. forms, website, surveys etc*) only have the fields that are relevant to the purpose of collection and subsequent processing. We do not include *'optional'* fields, as optional denotes that it is not necessary to obtain
- Physical collection *(i.e. face-to-face, telephone etc*) is supported using scripts and internal forms where the required data collection is ascertained using predefined fields. Again, only that which is relevant and necessary is collected
- We have SLA's and bespoke agreements in place with third-party controllers who send us personal information (*either in our capacity as a controller or processor).* These state that only relevant and necessary data is to be provided as it relates to the processing activity, we are carrying out
- We have documented destruction procedures in place where a data subject or third-party provides us with personal information that is surplus to requirement
- Forms, contact pages and any documents used to collect personal information are reviewed every 3-months to ensure they are fit for purpose and only obtaining necessary personal information in relation to the legal basis being relied on and the purpose of processing

Pseudonymisation

We utilise pseudonymisation where possible to record and store personal data in a way that ensures it can no longer be attributed to a specific data subject without the use of separate, additional information (*personal identifiers*). Encryption and partitioning are also used to protect the personal identifiers, being kept separate from the pseudonymised data sets.

When using pseudonymisation, we ensure that the attribute(s) being removed and replaced, are unique and prevent the data subject from being identified through the remaining markers and attributes. Pseudonymisation can mean that the data subject is still likely to be identified indirectly and as such, we use this technique in conjunction with other technical and operational measures of risk reduction and data protection.

Encryption

We utilise encryption as a further risk prevention measure for securing the personal data that we hold. Encryption with a secret key is used to make data indecipherable unless decryption of the dataset is carried out using the assigned key.

We utilise encryption via secret key for transferring personal data to any external

party and provide the secret key in a separate format. Where special category information is being transferred and/or disclosed, the Data Protection Officer is required to authorise the transfer and review the encryption method for compliance and accuracy.

Restriction

Our *Privacy by Design* approach means that we use council-wide restriction methods for all personal data activities. Restricting access is built into the foundation of the Council's processes, systems and structure and ensures that only those with authorisation and/or a relevant purpose, have access to personal information. Special category data is restricted at all levels and can only be accessed by key members of the Administration team and associated senior members of staff.

Refer to our *Access Control Policy* in our Information Security program for further details.

Hard Copy Data

Due to the nature of our business, it is sometimes essential for us to obtain, process and share personal and special category information which is only available in a paper format without pseudonymisation options (*i.e. copies of patient records, hospital invoices or claims information*). Where this is necessary, we utilise a tiered approach to minimise the information we hold and/or the length of time we hold it for. *Steps include: -*

- In the first instance, we always ask the initial data controller to send copies of any personal information records directly to the data subject
- Where step 1 is not possible or feasible, we will obtain a copy of the data and if applicable redact to ensure that only the relevant information remains (*i.e. when the data is being passed to a third-party for processing and not directly to the data subject*)
- When only mandatory information is visible on the hard copy data, we utilise electronic formats to send the information to the recipient to ensure that encryption methods can be applied (*i.e. we do not use the postal system as this can be intercepted*).
- Recipients (*i.e. the data subject, third-party processer*) are reverified and their identity and contact details checked
- The Data Protection Officer authorises the transfer and checks the file(s) attached and encryption method and key
- Once confirmation has been obtained that the recipient has received the personal information, where possible *(within the legal guidelines and rules of the data protection laws*), we destroy the hard copy data and delete the

sent message

- If for any reason a copy of the paper data must be retained by the Council, we use a physical safe to store such documents as oppose to our standard archiving system

6.1.2 INFORMATION AUDIT

To enable the Council to fully prepare for and comply with the data protection laws, we have carried out a council-wide data protection information audit to better enable us to record, categorise and protect the personal data that we hold and process.

The audit has identified, categorised and recorded all personal information obtained, processed and shared by our council in our capacity as a controller/processor and has been compiled on a central register which includes: -

- What personal data we hold
- Where it came from
- Who we share it with
- Legal basis for processing it
- What format(s) is it in
- Who is responsible for it?
- Disclosures and Transfers

6.2 LEGAL BASIS FOR PROCESSING *(LAWFULNESS)*

At the core of all personal information processing activities undertaken by the Council, is the assurance and verification that we are complying with Article 6 of the GDPR and our lawfulness of processing obligations. Prior to carrying out any personal data processing activity, we identify and establish the legal basis for doing so and verify these against the regulation requirements to ensure we are using the most appropriate legal basis.

The legal basis is documented on our information audit register and in our Privacy Notice and, where applicable, is provided to the data subject and Supervisory Authority as part of our information disclosure obligations. *Data is only obtained, processed or stored when we have met the lawfulness of processing requirements, where: -*

- The data subject has given consent to the processing of their personal data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the data

subject is party or in order to take steps at the request of the data subject prior to entering into a contract

- Processing is necessary for compliance with a legal obligation to which we are subject
- Processing is necessary to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Council
- Processing is necessary for the purposes of the legitimate interests pursued by the Council or by a third party (*except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child).*

6.2.1 PROCESSING SPECIAL CATEGORY DATA

Special categories of Personal Data are defined in the data protection laws as: -

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited – unless one of the Article 9 clauses applies.

Where the Council processes any personal information classed as special category or information relating to criminal convictions, we do so in accordance with Article 9 of the GDPR regulations and in compliance with the Data Protection Act 2018 Schedule 1 Parts 1, 2, 3 & 4 conditions and requirements.

We will only ever process special category data where: -

- The data subject has given explicit consent to the processing of the personal
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law
- Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim

- Processing relates to personal data which are manifestly made public by the data subject
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- Processing is necessary for reasons of substantial public interest
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
- Processing is necessary for reasons of public interest in the area of public health
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)

Schedule 1, Parts 1, 2 & 3 of The Data Protection Act 2018 provide specific conditions and circumstances when special category personal data can be processed and details the requirements that organisations are obligated to meet when processing such data.

Where the Council processes personal information that falls into one of the above categories, we have adequate and appropriate provisions and measures in place prior to any processing. *Measures include: -*

- Verifying our reliance on one of the data protection laws Article 9(1), and where applicable The Data Protection Act 2018 Sch.1, Pt.1, Pt.2 and/or Pt.3 conditions prior to processing
- Documenting the Schedule 1 condition and Article 6(1) legal basis relied upon from processing on our Processing Activities Register (*where applicable)*
- Having an appropriate policy document in place when the processing is carried out, specifying our: -
    - procedures for securing compliance with the data protection laws principles
    - policies as regards the retention and erasure of personal data processed in reliance on the condition
    - retention periods and reason *(i.e. legal, statutory etc)*
    - procedures for reviewing and updating our policies in this area

Please refer to our Retention & Erasure Policy for further guidance and

procedures.

6.2.2 RECORDS OF PROCESSING ACTIVITIES

As an organisation with *less than* 250 employees, the Council does not maintain records of our processing activities. However, we continually review all such activities and council size to ensure that we will being to record such information as detailed in GDPR Article 30 where: -

1. We employee 250 or more employees
2. Processing personal data could result in a risk to the rights and freedoms of individual
3. The processing is not occasional
4. We process special categories of data or criminal convictions and offences
5. Such records are maintained in writing, are provided in a clear and easy to read format and are readily available to the Supervisory Authority upon request.

As part of our obligations under the UK's Data Protection Act 2018, Sch.1, Pt.4, where we are required to maintain a record of our processing activities in our capacity as a controller and are processing special category or criminal conviction data, as specified in Sch.1, Pt.1-3 of the Act, we also record the below information on the register: -

- Which condition is relied on?
- How the processing satisfies Article 6 of the data protection laws (*lawfulness of processing*)
- Whether the personal data is retained and erased in accordance with the policies described in paragraph 30(b) of the Act (*and if not, the reasons for not following those policies*).

6.3 CODES OF CONDUCT & CERTIFICATION MECHANISMS

The Council adheres to the data protection codes of conduct prepared by IT Governance and/or are certified by ISO 17024 to demonstrate that we comply with the data protection laws rules and principles.

These codes and certification mechanism are approved by the Supervisory Authority and have been disseminated throughout the council to ensure competency and compliance from all staff.

The codes of conduct that we adhere to help us to: -

- Improve transparency and accountability

- Demonstrate to the public and Supervisory Authority that we meet the requirements of the data protection law and that we can be trusted with personal data
- Mitigate against enforcement action(s)
- Improve standards by establishing best practice
- Carry out fair and transparent processing
- Ensure appropriate safeguards within the framework of personal data transfers to third countries or international organisations

We submit to frequent and unscheduled monitoring and audits by the codes of conduct association/trade body and by the data protection certification scheme and understand that where we are deemed to be non-compliant in any area relating to the data protection laws, we may lose our certification/seal of approval and/or the Supervisory Authority will be informed.

6.4 THIRD-PARTY PROCESSORS

The Council utilise external processors for certain processing activities *(where applicable*). We use information audits to identify, categorise and record all personal data that is processed outside of the council, so that the information, processing activity, processor and legal basis are all recorded, reviewed and easily accessible. *Such external processing includes (but is not limited to**): -***

- IT Systems and Services
- Legal Services
- Debt Collection Services
- Human Resources
- Payroll
- Hosting or Email Servers
- Credit Reference Agencies
- Direct Marketing/Mailing Services

We have strict due diligence and Know Your Customer procedures and measures in place and review, assess and background check all processors prior to forming a business relationship. We obtain council documents, certifications, references and ensure that the processor is adequate, appropriate and effective for the task we are employing them for.

We audit their processes and activities prior to contract and during the contract period to ensure compliance with the data protection regulations and review any codes of conduct that they are obligated under to confirm compliance.

The continued protection of data subjects' rights and the security of their personal information is always our top priority when choosing a processor and we understand the importance of adequate and reliable outsourcing for processing activities as well as our continued obligations under the data protection laws for data processed and handled by a third-party.

We draft bespoke Service Level Agreements (SLAs) and contracts with each processor as per the services provided and have a dedicated Processor Agreement template that details: -

- The processors data protection obligations
- Our expectations, rights and obligations
- The processing duration, aims and objectives
- The data subjects' rights and safeguarding measures
- The nature and purpose of the processing
- The type of personal data and categories of data subjects

Each of the areas specified in the contract are monitored, audited and reported on. Processors are notified that they shall not engage another processor without our prior specific authorisation and any intended changes concerning the addition or replacement of existing processors must be done in writing, in advance of any such changes being implemented.

The Processor Agreement and any associated contract reflects the fact that the processor: -

- Processes the personal data only on our documented instructions
- Seeks our authorisation to transfer personal data to a third country or an international organisation (*unless required to do so by a law to which the processor is subject*)
- Shall inform us of any such legal requirement to transfer data before processing
- Ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
- Takes all measures to security the personal data at all times
- Respects, supports and complies with our obligation to respond to requests for exercising the data subject's rights
- Assists the Council in ensuring compliance with our obligations for data security, mitigating risks, breach notification and privacy impact assessments
- When requested, deletes or returns all personal data to the Council after the end of the provision of services relating to processing, and deletes

existing copies where possible

- Makes available to the Council all information necessary to demonstrate compliance with the obligations set out in the agreement and contract
- Allows and supports audits, monitoring, inspections and reporting as set out in the contract
- Informs the Council immediately of any breaches, non-compliance or inability to carry out their duties as detailed in the contract

6.5 Data Retention & Disposal

The Council have defined procedures for adhering to the retention periods as set out by the relevant laws, contracts and our business requirements, as well as adhering to the GDPR requirement to only hold and process personal information for as long as is necessary. All personal data is disposed of in a way that protects the rights and privacy of data subjects *(e.g. shredding, disposal as confidential waste, secure electronic deletion)* and prioritises the protection of the personal data in all instances.

Please refer to our *Data Retention & Erasure Policy* for full details on our retention, storage, periods and destruction processes.

7 Data Protection Impact Assessments (DPIA)

Individuals have an expectation that their privacy and confidentiality will be upheld and respected whilst their data is being stored and processed by the Council. We therefore utilise several measures and tools to reduce risks and breaches for general processing. However, where processing is likely to be high risk or cause significant impact to a data subject, we utilise proportionate methods to map out and assess the impact ahead of time.

Where the Council must or are considering carrying out processing that utilises new technologies, and/or where there is a likelihood that such processing could result in a high risk to the rights and freedoms of data subjects, we always carry out a Data Protection Impact Assessment (DPIA) *(sometimes referred to as a Privacy Impact Assessment*).

Pursuant to Article 35(3) and Recitals 84, 89-96, we consider processing that is likely to result in a high risk to include: -

- Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person(s)

- Processing on a large scale of special categories of data
- Processing on a large scale of personal data relating to criminal convictions and offences
- Systematic monitoring of a publicly accessible area on a large scale (i.e. CCTV)
- Where a processing operation is likely to result in a high risk to the rights and freedoms of an individual
- Those involving the use of new technologies
- New processing activities not previously used
- Processing considerable amounts of personal data at regional, national or supranational level, which could affect many data subjects
- Processing activities making it difficult for the data subject(s) to exercise their rights

Carrying out DPIAs enables us to identify the most effective way to comply with our data protection obligations and ensure the highest level of data privacy when processing. It is part of our Privacy by Design approach and allows us to assess the impact and risk before carrying out the processing, thus identifying and correcting issues at the source, reducing costs, breaches and risks.

The DPIA enables us to identify possible privacy solutions and mitigating actions to address the risks and reduce the impact. Solutions and suggestions are set out in the DPIA and all risks are rated to assess their likelihood and impact. The aim of solutions and mitigating actions for all risks is to ensure that the risk is either: -

- Eliminated
- Reduced
- Accepted

Please refer to our external DPIA Procedures for further details.

8 Data Subject Rights Procedures

8.1 Consent & The Right to be Informed

The collection of personal and sometimes special category data is a fundamental part of the products/services offered by the Council and we therefore have specific measures and controls in place to ensure that we comply with the conditions for consent under the data protection laws.

The data protection law defines consent as; *'Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.*

Where processing is based on consent, the Council have reviewed and revised all consent mechanisms to ensure that: -

- Consent requests are transparent, using plain language and is void of any illegible terms, jargon or extensive legal terms
- It is freely given, specific and informed, as well as being an unambiguous indication of the individual's wishes
- Consent is always given by a statement or a clear affirmative action (*positive opt-in*) which signifies agreement to the processing of personal data
- Consent mechanisms are upfront, clear, granular (*in fine detail*) and easy to use and understand
- Pre-ticked, opt-in boxes are never used
- Where consent is given as part of other matters (*i.e. terms & conditions, agreements, contracts*), we ensure that the consent is separate from the other matters and is not be a precondition of any service (*unless necessary for that service)*
- Along with our council name, we also provide details of any other third party who will use or rely on the consent
- Consent is always verifiable, and we have controls in place to ensure that we can demonstrate consent in every case
- We keep detailed records of consent and can evidence at a minimum: –
    - that the individual has consented to the use and processing of their personal data
    - that the individual has been advised of our council name and any third party using the data
    - what the individual was told at the time of consent
    - how and when consent was obtained
- We have ensured that withdrawing consent is as easy, clear and straightforward as giving it and is available through multiple options, including: -
    - Opt-out links in mailings or electronic communications
    - Opt-out process explanation and steps on website and in all written communications

    - Ability to opt-out verbally, in writing or by email
- Consent withdrawal requests are processed immediately and without detriment
- Where services are offered to children, age-verification and parental-consent measures have been developed and are in place to obtain consent
- Controls and processes have been developed and implemented to refresh consent, especially those relating to parental consents
- For special category data, the consent obtained is explicit *(stated clearly and in detail, leaving no room for confusion or doubt*) with the processing purpose(s) always being specified

8.1.1 CONSENT CONTROLS

The Council maintain rigid records of data subject consent for processing personal data and are always able to demonstrate that the data subject has consented to processing of his or her personal data where applicable. We also ensure that the withdrawal of consent is as clear, simple and transparent and is documented in all instances.

Where the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent is presented in a manner which is clearly distinguishable from those matters, in an intelligible and easily accessible form, using clear and plain language. All such written declarations are reviewed and authorised by the Data Protection Officer prior to being circulated.

Consent to obtain and process personal data is obtained by the Council through: -

- Face-to-Face
- Telephone
- In Writing
- Email/SMS
- Electronic *(i.e. via website form*)

Any electronic methods of gaining consent are regularly reviewed and tested to ensure that a compliant Privacy Notice is accessible and displayed and that consent is clear, granular and utilises a demonstrable opt-in mechanism. Where consent is obtained verbally, we utilise scripts, checklists to ensure that all requirements have been met and that consent is obtained compliantly and can be evidenced.

Electronic consent is always by a non-ticked, opt-in action (*or double opt-in where applicable*), enabling the individual to provide consent after the below information has been provided. This is then followed up with an email, SMS or written confirmation of the consent to process, store and share the personal information.

Privacy Notices are used in all forms of consent and personal data collection, to ensure that we are compliant in disclosing the information required in the data protection laws in an easy to read and accessible format.

8.1.2 CHILD'S CONSENT

While the GDPR states that a child's age is defined as 16; the UK's Data Protection Act 2018 reduces this age to *13 years*, as per Article 8(1) of the data protection laws what advises that *"Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years."*

The data protection laws state that where processing is based on consent and the personal data relates to a child who is below the age of 13 years**,** such processing is only carried out by the Council where consent has been obtained by the holder of parental responsibility over the child.

We have mechanisms in place to verify the age of any child prior to obtaining consent and review such consents annually for transferring from parental consent over to the child after age 13.

8.1.3 ALTERNATIVES TO CONSENT

The Council recognise that there are six lawful bases for processing and that consent is not always the most appropriate option. We have reviewed all processing activities and only use consent as an option where the individual has a choice.

When reviewing the processing activity for compliance with the consent requirements, we ensure that none of the below are a factor: –

- Where we ask for consent but would still process it even if it was not given *(or withdrawn).* If we would still process the data under an alternative lawful basis regardless of consent, we recognise it is not the correct lawful basis to use

- Where we ask for consent to process personal data as a precondition of a service we are offering, it is not given as an option and consent is not appropriate
- Where there is an imbalance in the relationship, i.e. with employees

8.1.4 INFORMATION PROVISIONS

Where personal data is obtained directly from the individual *(i.e. through consent, by employees, written materials and/or electronic formats (i.e. website forms, subscriptions, email etc*)), we provide the below information in all instances, in the form of a privacy notice: -

- The identity and the contact details of the controller and, where applicable, of the controller's representative
- The contact details of our data protection officer
- The purpose(s) of the processing for which the personal information is intended
- The legal basis for the processing
- Where the processing is based on point (f) of Article 6(1) *"processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party",* details of the legitimate interests
- The recipients or categories of recipients of the personal data *(if applicable)*
- If applicable, the fact that the Council intends to transfer the personal data to a third country or international organisation and the existence/absence of an adequacy decision by the Commission
    - where the Council intends to transfer the personal data to a third country or international organisation without an adequate decision by the Commission, reference to the appropriate or suitable safeguards the Council has put into place and the means by which to obtain a copy of them or where they have been made available
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
- The existence of the right to request access to and rectification or erasure of, personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability
- Where the processing is based on consent under points (a) of Article 6(1) or Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
- The right to lodge a complaint with the Supervisory Authority

- Whether providing personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data
- The existence of any automated decision-making, including profiling, as referred to in Article 22(1) and (4) and explanatory information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

The above information is provided to the data subject at the time the information is collected and records pertaining to the consent obtained are maintained and stored for 6 years from the date of consent, unless there is a legal requirement to keep the information longer.

8.2 PRIVACY NOTICE

The Council defines a Privacy Notice as a document, form, webpage or pop-up that is provided to individuals at the time we collect their personal *data (or at the earliest possibility where that data is obtained indirectly)*.

Our Privacy Notice includes the Article 13 (*where collected directly from individual*) or *14 (where not collected directly)* requirements and provides individuals with all the necessary and legal information about how, why and when we process their data, along with their rights and obligations.

We have a link to our Privacy Notice on our website and provide a copy of physical and digital formats upon request. The notice is the customer facing policy that provides the legal information on how we handle, process and disclose personal information.

The notice is easily accessible, legible, jargon-free and is available in several formats, dependant on the method of data collection: -

- Via our website
- Linked to or written in full in the footer of emails
- Worded in full in agreements, contracts, forms and other materials where data is collected in writing or face-to-face
- In employee contracts and recruitment materials
- Verbally via telephone or face-to-face
- Via SMS
- Printed media, adverts and financial promotions
- Digital Products/Services

- On Mobile Apps
- Automated phone service

With lengthy content being provided in the privacy notice and with informed consent being based on its contents, we have tested, assessed and reviewed our privacy notice to ensure usability, effectiveness and understanding.

We follow the below ICO preferred steps for testing, reviewing and auditing our privacy notice(s) and opt-in consent formats prior to use and to record such assessments.

1. Privacy Notices are drafted by the Data Protection Officer using the data protection laws requirements and with Supervisory Authority guidance
2. We utilise a select customer base to test the Privacy Notice in its varying formats and provide a feedback form for completion, verifying the below points: -
    a. How did you use the Privacy Notice *(e.g. website, agreement, orally)?*
    b. Did you find the information in the Privacy Notice easy to read, understand and access?
    c. Did you gain a full understanding of how we intend to use your data, who it will be shared with and what your rights are?
    d. Did you feel confident in giving consent to use your personal data after reading the notice information?
    e. Was there anything you did not understand?
    f. Did you find any errors?
    g. What, if anything, would you like to see changed about the Privacy Notice?
3. All feedback responses are saved with a copy of the used Privacy Notice and improvements are made and recorded where applicable
4. Re-testing is carried out on a new set of customers to ensure variety and independent assessment and verification
5. After a successful test, the acceptable Privacy Notice is rechecked against the data protection laws and Supervisory Authority regulations and guidelines to ensure it still complies and is adequate and effective
6. The final Privacy Notice(s) are then authorised by Senior Management/Director(s) before being rolled out

Where we rely on consent to obtain and process personal information, we ensure that it is: -

- Displayed clearly and prominently

- Asks individuals to positively opt-in
- Gives them sufficient information to make an informed choice
- Explains the different ways we will use their information
- Provides a clear and simple way for them to indicate they agree to different types of processing
- Includes a separate unticked opt-in box for direct marketing

8.3 Personal Data Not Obtained from the Data Subject

Where the Council obtains and/or processes personal data that has not been obtained directly from the data subject, the Council ensures that the information disclosures contain in Article 14 are provided to the data subject within 30 days of our obtaining the personal data *(except for advising if the personal data is a statutory or contractual requirement).*

In addition to the information disclosures in section 8.1.4, where personal data has not been obtained directly from a data subject, we also provide them with information about: -

- The categories of personal data
- The source the personal data originated from and whether it came from publicly accessible sources

Where the personal data is to be used for communication with the data subject, or a disclosure to another recipient is envisaged, the information will be provided at the latest, at the time of the first communication or disclosure.

Where the Council intends to further process any personal data for a purpose *other* than that for which it was originally obtained, we communicate this intention to the data subject prior doing so and where applicable, process only with their consent.

Whilst we follow best practice in the provision of the information noted in the relevant section of this policy, we reserve the right not to provide the data subject with the information if: -

- They already have it and we can evidence their prior receipt of the information
- The provision of such information proves impossible and/or would involve a disproportionate effort

- Obtaining or disclosure is expressly laid down by Union or Member State law to which the Council is subject and which provides appropriate measures to protect the data subject's legitimate interest
- Where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy

8.3.1 Employee Personal Data

As per the data protection law guidelines, we do not use consent as a legal basis for obtaining or processing employee personal information. Our HR policies have been updated to ensure that employees are provided with the appropriate information disclosure and are aware of how we process their data and why.

All employees are provided with our Staff Handbook which informs them of their rights under the data protection laws and how to exercise these rights and are provided with a Privacy Notice specific to the personal information we collect and process about them.

8.4 The Right of Access

We have ensured that appropriate measures have been taken to provide information referred to in Articles 13/14 and any communication under Articles 15 to 22 and 34 *(collectively, The Rights of Data Subjects*), in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Such information is provided free of charge and is in writing, or by other means where authorised by the data subject and with prior verification as to the subject's identity *(i.e. verbally, electronic*).

Information is provided to the data subject at the earliest convenience, but at a maximum of 30 days from the date the request is received. Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months where necessary. However, this is only done in exceptional circumstances and the data subject is kept informed in writing throughout the retrieval process of any delays or reasons for delay.

Where we do not comply with a request for data provision, the data subject is informed within 30 days of the reason(s) for the refusal and of their right to lodge a complaint with the Supervisory Authority.

8.4.1 SUBJECT ACCESS REQUEST

Where a data subject asks us to confirm whether we hold and process personal data concerning him or her and requests access to such data; we provide them with: -

- The purposes of the processing
- The categories of personal data concerned
- The recipients or categories of recipient to whom the personal data have been or will be disclosed
- If the data has or will be disclosed to a third countries or international organisations and the appropriate safeguards pursuant to the transfer
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
- The existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
- The right to lodge a complaint with a Supervisory Authority
- Where personal data has not been collected by the Council from the data subject, any available information as to the source and provider
- The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

Subject Access Requests (SAR) are passed to the Data Protection Officer as soon as received and a record of the request is noted. The type of personal data held about the individual is checked against our Information Audit to see what format it is held in, who else has it has been shared with and any specific timeframes for access.

SARs are always completed within 30-days and are provided free of charge. Where the individual makes the request by electronic means, we provide the information in a commonly used electronic format, unless an alternative format is requested.

Please refer to our external *Subject Access Request Procedures* for the guidelines on how an SAR can be made and what steps we take to ensure that access is provided under the data protection laws.

8.5 DATA PORTABILITY

The Council provides all personal information pertaining to the data subject to them on request and in a format, that is easy to disclose and read. We ensure

that we comply with the data portability rights of individuals by ensuring that all personal data is readily available and is in a structured, commonly used and machine-readable format, enabling data subjects to obtain and reuse their personal data for their own purposes across different services.

To ensure that we comply with Article 20 of the data protection laws concerning data portability, we keep a commonly used and machine-readable format of personal information where the processing is based on: -

- Consent pursuant to point (a) of Article 6(1)
- Consent pursuant to point (a) of Article 9(2)
- A contract pursuant to point (b) of Article 6(1); and
- the processing is carried out by automated means

Where requested by a data subject and if the criteria meet the above conditions, we will transmit the personal data directly from the Council to a designated controller, where technically feasible.

We utilise the below formats for the machine-readable data: -

- HTML
- CSV
- XML

All requests for information to be provided to the data subject or a designated controller are done so free of charge and within 30 days of the request being received. If for any reason, we do not act in responding to a request, we provide a full, written explanation within 30 days to the data subject or the reasons for refusal and of their right to complain to the supervisory authority and to a judicial remedy.

All transmission requests under the portability right are assessed to ensure that no other data subject is concerned. Where the personal data relates to more individuals than the subject requesting the data/transmission to another controller, this is always without prejudice to the rights and freedoms of the other data subjects.

8.6 Rectification & Erasure

8.6.1 Correcting Inaccurate or Incomplete Data

Pursuant to Article 5(d), all data held and processed by the Council is reviewed and verified as being accurate wherever possible and is always kept up to date. Where inconsistencies are identified and/or where the data subject or controller

inform us that the data we hold is inaccurate, we take every reasonable step to ensure that such inaccuracies are corrected with immediate effect.

The Data Protection Officer are notified of the data subjects request to update personal data and are responsible for validating the information and rectifying errors where they have been notified. The information is altered as directed by the data subject, with the information audit being checked to ensure that all data relating to the subject is updated where incomplete or inaccurate. Once updated, we add an addendum or supplementary statement where applicable.

Where notified of inaccurate data by the data subject, we will rectify the error within 30 days and inform any third party of the rectification if we have disclosed the personal data in question to them. The data subject is informed in writing of the correction and where applicable, is provided with the details of any third-party to whom the data has been disclosed.

If for any reason, we are unable to act in response to a request for rectification and/or completion, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

8.6.2 THE RIGHT TO ERASURE

Also, known as *'The Right to be Forgotten'*, the Council complies fully with Article 5(e) and ensures that personal data which identifies a data subject, is not kept longer than is necessary for the purposes for which the personal data is processed.

All personal data obtained and processed by the Council is categorised when assessed by the information audit and is either given an erasure date or is monitored so that it can be destroyed when no longer necessary.

Please refer to our Data Retention & Erasure Policy for exact procedures on erasing data and complying with the Article 17 requirements.

8.7 THE RIGHT TO RESTRICT PROCESSING

There are certain circumstances where the Council restricts the processing of personal information, to validate, verify or comply with a legal requirement of a data subjects request. Restricted data is removed from the normal flow of information and is recorded as being restricted on the information audit.

Any account and/or system related to the data subject of restricted data is updated to notify users of the restriction category and reason. When data is restricted it is only stored and not processed in any way.

The Council will apply restrictions to data processing in the following circumstances: -

- Where an individual contest the accuracy of the personal data and we are in the process verifying the accuracy of the personal data and/or making corrections
- Where an individual has objected to the processing (*where it was necessary for the performance of a public interest task or purpose of legitimate interests*), and we are considering whether we have legitimate grounds to override those of the individual
- When processing is deemed to have been unlawful, but the data subject requests restriction as oppose to erasure
- Where we no longer need the personal data, but the data subject requires the data to establish, exercise or defend a legal claim

The Data Protection Officer reviews and authorises all restriction requests and actions and retains copies of notifications from and to data subjects and relevant third parties. Where data is restricted, and we have disclosed such data to a third-party, we will inform the third-party of the restriction in place and the reason and re-inform them if any such restriction is lifted.

Data subjects who have requested restriction of data are informed within 30 days of the restriction application and are also advised of any third-party to whom the data has been disclosed. We also provide in writing to the data subject, any decision to lift a restriction on processing. If for any reason, we are unable to act in response to a request for restriction, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

8.8 Objections and Automated Decision Making

Data subjects are informed of their right to object to processing in our Privacy Notices and at the point of first communication, in a clear and legible form and separate from other information. We provide opt-out options on all direct marketing material and provide an online objection form where processing is carried out online. *Individuals have the right to object to: -*

- Processing of their personal information based on legitimate interests or the performance of a task in the public interest/exercise of official authority *(including profiling*)

- Direct marketing (*including profiling*)
- Processing for purposes of scientific/historical research and statistics

Where the Council processes personal data for the performance of a legal task, in relation to our legitimate interests or for research purposes, a data subjects' objection will only be considered where it is on *'grounds relating to their particular situation'*. We reserve the right to continue processing such personal data where: -

- We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual
- The processing is for the establishment, exercise or defence of legal claims

Where we are processing personal information for direct marketing purposes under a previously obtained consent, we will stop processing such personal data immediately where an objection is received from the data subject. This measure is absolute, free of charge and is always adhered to.

Where a data subject objects to data processing on valid grounds, the Council will cease the processing for that purpose and advise the data subject of cessation in writing within 30 days of the objection being received.

We have carried out a system audit to identify automated decision-making processes that do not involve human intervention. We also assess new systems and technologies for this same component prior to implementation. the Council understands that decisions absent of human interactions can be biased towards individuals and pursuant to Articles 9 and 22 of the data protection laws, we aim to put measures into place to safeguard individuals where appropriate. Via our Privacy Notices, in our first communications with an individual and on our website, we advise individuals of their rights not to be subject to a decision when: -

- It is based on automated processing
- It produces a legal effect or a similarly significant effect on the individual

In limited circumstances, the Council will use automated decision-making processes within the guidelines of the regulations. *Such instances include: -*

- Where it is necessary for entering into or performance of a contract between us and the individual
- Where it is authorised by law *(e.g. fraud or tax evasion prevention)*
- When based on explicit consent to do so

- Where the decision does not have a legal or similarly significant effect on someone

Where the Council uses, automated decision-making processes, we always inform the individual and advise them of their rights. We also ensure that individuals can obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it.

9 Oversight Procedures

9.1 Security & Breach Management

Alongside our *'Privacy be Design'* approach to protecting data, we ensure the maximum security of data that is processed, including as a priority, when it is shared, disclosed and transferred. Our *Information Security Policies* provide the detailed measures and controls that we take to protect personal information and to ensure its security from consent to disposal.

We carry out information audits to ensures that all personal data held and processed by us is accounted for and recorded, alongside risk assessments as to the scope and impact a data breach could have on data subject(s). We have implemented adequate and appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Whilst every effort and measure are taken to reduce the risk of data breaches, the Council has dedicated controls and procedures in place for such situations, along with the notifications to be made to the Supervisory Authority and data subjects (where applicable).

Please refer to our *Data Breach Policy & Procedures* for specific protocols.

10 Transfers & Data Sharing

The Council takes proportionate and effective measures to protect personal data processed by us; however, we recognise the high-risk nature of disclosing and transferring personal data and as such, place an even higher priority on the protection and security of data being transferred. Data transfers within the UK and EU are deemed less of a risk than a third country or an international organisation, due to the data protection laws covering the former and the strict regulations applicable to all EU Member States.

Where data is being transferred for a legal and necessary purpose, compliant with all Articles in the Regulation, we utilise a process that ensures such data is

encrypted with a secret key and where possible is also subject to our data minimisation methods.

We use approved, secure methods of transfer and have dedicated points of contact with each Member State organisation with whom we deal. All data being transferred is noted on our information audit so that tracking is easily available, and authorisation is accessible. The Data Protection Officer authorises all EU transfers and verifies the encryption and security methods and measures.

Please refer to our International Data Transfer Procedures for further details.

11 AUDITS & MONITORING

This policy and procedure document details the extensive controls, measures and methods used by the Council to protect personal data, uphold the rights of data subjects, mitigate risks, minimise breaches and comply with the data protection laws and associated laws and codes of conduct. In addition to these, we also carry out regular audits and compliance monitoring processes that are detailed in our *Compliance Monitoring & Audit Policy & Procedure*, with a view to ensuring that the measures and controls in place to protect data subjects and their information, are adequate, effective and compliant at all times.

The Data Protection Officer has overall responsibility for assessing, testing, reviewing and improving the processes, measures and controls in place and reporting improvement action plans to the Senior Management Team where applicable. Data minimisation methods are frequently reviewed, and new technologies assessed to ensure that we are protecting data and individuals to the best of our ability.

All reviews, audits and ongoing monitoring processes are recorded by the Data Protection Officer and copies provided to Senior Management and are made readily available to the Supervisory Authority where requested.

The aim of internal data protection audits is to: -

- Ensure that the appropriate policies and procedures are in place
- To verify that those policies and procedures are being followed
- To test the adequacy and effectiveness of the measures and controls in place
- To detect breaches or potential breaches of compliance
- To identify risks and assess the mitigating actions in place to minimise such risks
- To recommend solutions and actions plans to Senior Management for

improvements in protecting data subjects and safeguarding their personal data

- To monitor compliance with the data protection laws and demonstrate best practice

12 TRAINING

Through our strong commitment and robust controls, we ensure that all staff understand, have access to and can easily interpret the data protection laws requirements and its principles and that they have ongoing training, support and assessments to ensure and demonstrate their knowledge, competence and adequacy for the role. Our *Training & Development Policy & Procedures* and *Induction Policy* detail how new and existing employees are trained, assessed and supported and include: -

- GDPR Workshops & Training Sessions
- Assessment Tests
- Coaching & Mentoring
- 1:1 Support Sessions
- Scripts and Reminder Aids
- Access to GDPR policies, procedures, checklists and supporting documents

Employees are continually supported and trained in the data protection laws requirements and of~~ut~~ own objectives and obligations around data protection.

13 PENALTIES

The Council understands its obligations and responsibilities under the data protection laws and recognises the severity of breaching any part of the law or Regulation. We respect the Supervisory Authority's authorisation under the legislation to impose and enforce fines and penalties on us where we fail to comply with the regulations, fail to mitigate the risks where possible and operate in a knowingly non-compliant manner.

Employees have been made aware of the severity of such penalties and their proportionate nature in accordance with the breach. *We recognise that: -*

- Breaches of the obligations of the controller, the processor, the certification body and the monitoring body, are subject to administrative fines up to €10,000,000 or 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

- Breaches of the basic principles for processing, conditions for consent, the data subjects' rights, the transfers of personal data to a recipient in a third country or an international organisation, specific processing situations (*Chapter IX*) or non-compliance with an order by the Supervisory Authority, are subject to administrative fines up to €20,000,000 or 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

14 Overall Responsibilities

The Council has appointed a Data Protection Officer whose role it is to identify and mitigate any risks to the protection of personal data, to act in an advisory capacity to the business, its employees and upper management and to actively stay informed and up-to-date with all legislation and changes relating to data protection.

The DPO will work in conjunction with the Compliance Officer, IT Manager and Training Officer to ensure that all processes, systems and staff are operating compliantly and within the requirements of the data protection laws and its principles.

The DPO has overall responsibility for due diligence, privacy impact assessments, risk analysis and data transfers where personal data is involved and will also maintain adequate and effective records and management reports in accordance with the data protection laws and our own internal objectives and obligations.

Staff who manage and process personal or special category information will be provided with extensive data protection training and will be subject to continuous development support and mentoring to ensure that they are competent and knowledge for the role they undertake.

15 Data Control & Passwords

15.1 Briefing

It is **Newquay Town Council's** policy to protect and secure the information and systems within our remit and we take this function very seriously. We have developed and implemented several physical, logical and procedural measures and controls to enforce our approach. We understand that it is vital to protect the systems and information held and used by us from unauthorised use or access and are fully aware of how such access can affect security, personal

information and individuals. ***The types of measures and controls used by The Council are: -***

- **Physical Access Controls** ensuring the availability of systems and information is restricted to authorised persons only, thus preventing locations and information from being accessible to non-authorised individuals. This includes the Paxton and Texecom integrated platforms for physical security, with additional coverage using HikVision CCTV to monitor any breaches.
- **Logical Access Controls** utilise tools and protocols for identification, authentication and authorisation of our computer information systems (*including remote access, laptops and phone systems*). The Council's logical access controls enforce access measures to our systems, programs, processes, and information and include password protocols, user authentication methods, data and authentication credentials encryption and network, system and user-level firewalls.
- **Procedural Access Measures** include our defined policies and procedures that are followed by all staff and third parties and provide the steps for areas such as access control, information security, password protocols and clear desk measures.

15.2 Section Purpose

The purpose of this section is to ensure that system based and physical access to any information, location and/or system is controlled and where applicable restricted using controls and procedures that protect the associated information systems and data. The Council is committed to the security of the information and assets within our remit and enforce and stress test all access measures to ensure their functionality, effectiveness and purpose.

This Data Control & Password Policy aims to restrict access to controlled information and/or systems to only those staff or third parties who are authorised or have written permission from the Council. Where temporary and/or partial access to information or systems is required, we follow strict protocols to only enable access to the information or for the duration required by the activity.

15.3 Section Scope

This section applies to all councillors and staff within the Council *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Council in the UK or overseas)*. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

15.4 Section Objectives

The Council is committed to ensuring compliance with the rules, standards and regulations as laid out by its regulating and governing bodies and confirms that it has developed and implemented the appropriate procedures, systems, controls and measures to manage and mitigate against risk.

For systems containing restricted and personal information and data, an access control matrix must be developed to record role based authorised access recorded on an individual basis. Authorisation procedures must be in place for managers to authorise all access (*including short term and temporary access*) recorded on the matrix. The access matrix must be continually updated and maintained to reflect accurate records of access.

As a Council, we have a full understanding of the compliance standards that we are obligated to meet and confirm that we have in place effective and efficient tools and controls for meeting these obligations under the current regulatory system.

The Council's objectives regarding compliance are to: -

- To gain access to specific systems and information, employees follow a formal request process which are submitted in writing to the IT Service Manager.
- Generic logons are not permitted across the Council systems, however, use of generic accounts under 'controlled' circumstances can be permitted at the discretion of the Town Clerk and IT Service Manager.
- To ensure relevant Council, contractual, regulatory and legislative security standards are met and adhered to, employee screening checks, including DBS, CRB and referencing are undertaken if required.
- The appropriate level of access to systems and information will be determined based on the user-level, role-based requirements and ad-hoc job functions and roles.
- If authorisation to use systems and information is granted, unique logon credentials and password will be provided to the employee, utilising the strong password controls detailed in this policy.
- Access for remote users shall be subject to authorisation by line managers via the request form to the IT Service Manager. No access is granted without a completed and authorised request form.

16 Section Procedures, Controls and Measures

It is pivotal to operating our business and providing services to constituents that the Council use computers, telephone systems, software, hardware devices and data storage systems. Due to the nature of our business, such systems are often

used to store information and assets that are of a personal and confidential nature. It is therefore essential that we protect and secure such information and therefore access to the systems using a variety of access controls and measures.

We take a multi-tiered approach when securing systems and restricting access and detail in this policy the procedures and methods used throughout the Council. This information is disseminated to all employees and forms part of our information security program.

16.1 Logical Access Control

Access to systems within the Council are governed by our tiered logical access control measures. Access to any system is classified as one of the below access levels and restrictions are implemented at the user level. Levels can be changed at the discretion of the Town Clerk and IT Service Manager and pending a completion of an access change form. ***Considerations for granting access is assessed based on: -***

- An employee or user's need of access to complete their job and/or task
- Duration of access
- Level of access
- Information types located on the system in questions
- Security measures in place if access is granted
- Ability to remove access at a predetermined time
- Access is decided and allocated on a case by case basis and can only be assigned by the Town Clerk or IT Service Manager.

16.1.1 Role-Based Access

Users are identified as being part of a group (*such as employee and/or service)* and their level of access is generic to all required areas. This level of access is inherited by all group members and is controlled by the IT Service Manager. Such group access is considered necessary for each employee to enable them to carry out their job and includes access to areas such as email, printers, The Council collection system and phone system. The Town Clerk, Deputy Town Clerk and IT Service Manager can assign role-based access.

16.1.2 Manager Access

System access is granted at a higher level for managers and Directors who can access more system areas than generic employees. Such access is deemed essential to their oversight role and enables managerial staff to carry out functions and processes that require access to personal information, secure

systems or data. Manager access is not inherited by the group and only the Town Clerk and IT Service Manager can assign Manager Access.

16.1.3 INDIVIDUAL ACCESS

System access is granted at the required level based on a business and/or legal requirement and is only granted to the individual(s) who require access (*i.e. if an employee is granted extended access, this is not inherited by any other role-based group member*). Individual Access is usually granted for a limited period by the Town Clerk or IT Service Manager and is deactivated after a set period. Such access may include a role-based user needing access to sensitive information or restricted systems to perform a task or one-off project.

16.2 PASSWORDS

Passwords are a key part of the Council's protection strategy and are used throughout the Council to secure information and restrict access to systems. We use a multi-tiered approach which includes passwords at user, management, device, system and network levels to ensure a thorough and encompassing approach.

Passwords afford a high level of protection to resources and data and are mandatory requirements for all employees and/or third-parties who are responsible for one or more account, system or have access to any resource that requires a password.

16.2.1 PASSWORD CREATION & CHANGE

Only those authorised to access specific devices, information and systems are provided with the relevant passwords and such provisions are reviewed every 60 days to ensure that access is still valid and required. Employees may never share their passwords with anyone else in the Council, including co-workers, managers or IT staff and unique passwords are used for all employees and access to systems and devices.

Employees are made aware that strong passwords are required for all systems and user-access and that a strict non-disclosure protocol applies to passwords. Where applicable to the system or device being used, The Council utilises software to enforce the use of strong passwords. Employees are not allowed to share or disclose any password.

Strong passwords are enforced on systems and by users and must be: -

- More than 6 characters

- Include letters, numbers and at least 1 special characters
- Not be easily recognisable *(i.e. no names, dates of birth, places etc*)
- Must include upper and lowercase letters

Old cybersecurity advice recommended frequent password changes, but experts now agree that using a long, strong, and unique password generated and stored in a password manager is preferable to frequently changing a password. The best reason to change a password is if you think it's been compromised. The Council now utilises password management software for senior staff to generate and store complex passwords. ~~All passwords are changed every 60 days, and users are not permitted to reusethe same password within a 3-month period. This is forced using software on allsystems and a password change is automatically promoted at the start of each period. This change is enforced on the date of expiry with a reminder 7 days before.~~

If a password is forgotten, only the Town Clerk or IT Service Manager can reset the passwords. Passwords that have been forgotten are changed by default and cannot be reset to use the same password. A force change of password is also affected if the user suspects that the password has been compromised.

Where a password is reset, the individuals identify is first verified. This is essential where remote access passwords are changed or reset, and the IT Service Manager is not able to physically verify the identity of the user. A two-step identification process is used in such instances which uses multi-factor authentication against another of the user's devices (such as mobile phone).

16.2.2 Default Passwords

It is occasionally necessary to set up default password at the IT Manager level. This is usually only when a new system or user are being set up and a password change will be promoted from the first user use. Default passwords are to be changed as soon as is possible and where applicable, access to information is restricted until a strong password has been created.

Where new systems, devices or software is purchased, default passwords are immediately changed and reset to use the strong variables indicated above.

16.2.3 Protecting Passwords

The Council is aware that viruses, software and phishing scams can attempt to obtain passwords at a user level. Whilst Firewalls are used to secure and protect systems and software, employees are provided with training and guidance on phishing and are instructed to neve disclose their passwords in a physical or

online environment. This includes not disclosing passwords to third-parties, clients or representatives who may have a legitimate need to access a system.

Password fields are always displayed in a hash or star format (*i.e. ### or ****) so that clear text is not present when a password is typed. This helps to prevent

unauthorised access or password disclosure by copy & paste or electronic printing methods.

Writing down or storing passwords in any written or digital format is forbidden and all employees are made aware of this. Disclosure or unintentional loss of a password that has been written down in any format may result in disciplinary action being taken.

16.3 User ID's and Badges

The Council has adopted ID badges for all employees, visitors and third parties who are in our office building. Such badges are specific to those they are assigned to and ID's or badges not in use are stored in a secure, locked area.

Employees must always wear their ID badge whilst in the building or whilst visiting third-party offices and are not allowed to share or copy their badge. All ID badges are assigned a unique verifying employee code which is specific to the employee and is logged on an Access Control Register. If an employee loses their ID, their code is immediately deactivated, and a new code is assigned. Codes are never reused after deactivation.

Visitors to the Council are given '***Visitor ID Badges'*** which states their name, Council, position and responsible person. Visitors are always accompanied on the premises and are required to log in and out of the building, sign confidentiality agreements and are to be escorted by an employee who is responsible for them during their visit.

16.4 Privileged Accounts

The Council understands the extreme importance of securing and restricting access to privileged accounts. Such accounts enable direct access to our network, servers, firewalls, routers, database servers, systems and software and as such are treated with the utmost security and protection. Employees and third parties are never given access to privileged accounts, unless they have been assigned responsibility for a direct function. If this is the case, access is only given to the exact system or infrastructure required to complete their take.

We audit access to privileged accounts on a weekly basis and review access monthly to ensure that it is still required or is of use. Logs of access to privileged accounts are reviewed for consistency with access records.

16.5 Authorised Access

The Council keeps an Access Register and details which employees or third parties have access to which systems and information. The register also notes when the access was given, when it will be restricted (*if temporary access*), the type of data or system being accessed and the reason for access.

16.5.1 Login Controls

Systems can only be accessed by secure authentication of user validation, which consists of a username and password at the role-based user level. All computers have an active firewall and default to a lock screen with user authentication required up to 15 minutes of inactivity has taken place. All staff are aware that if they leave their workstation, their monitor is to be turned off and their system locked. All users are also aware that if they modify the inactivity period in which causes the Council a detriment then they are ultimately responsible.

16.5.2 Credentials & Roles

Access to any systems within the Council (*including sending email*), utilises authentication based on the valid credentials being used. Each user is assigned unique credentials and are not allowed to share or disclose them to any other user. It is necessary for credentials to be stored so that when they are used to access a system, database or send an email, the authentication process works. All authentication credentials are encrypted when stored and transmitted and access is restricted to the IT Service Manager.

As the Council is a small organisation, many roles are carried out by the Town Clerk or validated staff, which means that having separate roles for areas such as authorised access or setting up accounts is not always possible. However, all requests for access are verified by either the Town Clerk and/or IT Service Manager and employees are never allowed to set up their own access, disclose credentials or bypass validations. An access request form is completed for all individual access requirements and is verified by either the Town Clerk and/or IT Service Manager before being authorised.

16.6 Physical Access Controls

Access to the Council building, office sections and secure rooms are protected by our building access controls. These increase building, information and employee security and safety and ensure that no unauthorised access is possible.

16.6.1 Door & Window Controls

The Council has 8 doors providing access to the Municipal Office, which are secured via digital access control systems and physical locks.

All areas are alarmed and windows are to be kept secure when the building is vacated. Visitors are always escorted during a visit and are given an ID badge. They are also required to log in and out in our access register and sign a confidentiality agreement within the Tourist Information Centre. Where a visitor is required to carry any bag with them (*including laptops*), we reserve the right to search them on entering and leaving the building.

16.6.2 Outside Opening Hours

When the building has been vacated at the end of working hours, the alarm system is activated automatically and secures all windows and doors, with sensors in all accessible areas.

16.6.3 Direct Access

The use of keys to any buildings, rooms, secure cabinets, safes etc are always controlled and recorded and keys are only provided to employees who require them for business and/or legal reasons. When not in use, keys are stored in a secure, locked cabinets and only the Town Clerk, Deputy Town Clerk, PA to the Town Clerk and IT Service Manager have access. Locations of keys are always known and if there is any suspicion that a key has been lost or compromised, lock and access points are changed immediately and monitored until the change is affected.

A secondary key system is held within the Town Clerk's office, should secure areas be compromised for immediate replacement.

Visitors are not permitted to access the Council's servers, networks or confidential information areas without prior authorisation. Where authorisation has been given, visits are always escorted by a relevant manager or above.

16.7 Leavers & End of Contract

As the Council is a small Council, monitoring end of contracts with third parties and identifying employees who are leaving or are on annual leave is straightforward. We operate an immediate deactivation process of any credentials and access rights on termination and reactivation is only possible via a written request and authorisation from the IT Service Manager.

Leavers are required to turn in their ID badge before existing the building and strict security checks and personal searches are performed. Hard copy ID's are destroyed and where applicable, any electronic ID's are deactivated with immediate effect. It is the line managers responsibility to ensure that ID badges are returned to the IT Service Manager.

Where a project or service contract ends, any access or credentials provided during the contract are deactivated and any ID badges or keys are returned and signed back into the logbook.

Where an employee is on annual leave, we can suspend their credentials and access rights and reactivate on their return. This reduces the risk of unmanned access points, but also prevents having to reset up new credentials and access levels.

16.8 Section Responsibilities

The IT Service Manager are responsible for ensuring that all staff and managers are aware of security policies, including access control and secure passwords and The Council operates a top-down approach. Managers need to be aware they have a responsibility to ensure staff have sufficient, relevant knowledge concerning the security of information and systems and new starters and existing staff training workshops are run on an annual basis covering the access control and password policies and objectives.

17 Asset Management

17.1 Section Introduction

Asset Management is the process of identifying, classifying, managing, recording and coordinating a firm's assets (*physical, IT and information*) to ensure their security and the continued protection of any confidential data they store or give access to.

For the purposes of this section and associated asset management processes, the Council defines an ***'Asset'*** as any item, system, application or entity that has potential or actual value to our organisation. Such assets include, but are not limited to: -

- Information (*including personal data*)
    - Paper records
    - Electronic records
    - Files and folders

    - Software licenses
- Systems
- Computers or Workstations
- Networks
- Servers
- Hardware
- Software
- Telephony Systems
- Equipment
- Databases
- Technology
- Printers/Scanners
- Fax Machines

Assets can be both tangible and intangible and are of value to a council based on their importance, function and use. Whilst information is one of the Council's most valuable assets, we understand the association and importance of the IT and physical assets that use, process, store and provide access to such information. As such, all forms of assets recorded by the Council are valued and afforded a high level of protection and governance.

17.2 Section Definitions

For the purposes of our Information Security program and the references in this section, when we refer to '***Information Assets'*** we are collectively describing all assets within the Council that are identified, recorded and secured. Most of our assets, including IT and physical are in place with the main purpose of holding and protecting personal information and as such we refer to all assets collectively as ***'Information Assets'***.

17.3 Section Statement

The Council understands the importance of identifying, recording and classifying our assets and utilise an Information Asset Register (IAR) to retain a complete list of all current assets, their location, value, access and other vital data. We have a responsibility to manage our physical and information assets, stemming from various legal, regulatory, contractual and business obligations: -

- General Data Protection Regulation (GDPR)
- Data Protection Bill
- Contractual (*client agreements, business objectives etc*)

- Security Requirements (*e.g. encryption, backups, updates etc*)
- Equipment Management (*service, replacement, disposal*)

The Council ensures that all assets used and retained during business, are properly documented, are assigned an owner and are subject to this policy and subsequent procedures. Managing our assets is paramount to the continuity of our business and to the Council's reputation. Assets are protected where applicable, further aiding in the protection of personal information and confidential data.

17.4 Section Purpose

The purpose of this policy is to achieve and maintain appropriate protection of organisational assets (*tangible and intangible*) and to document those assets to ensure knowledge and understanding of their value, purpose, risk and location. The Council ensures that all assets are assigned an owner who has overall responsibility for managing, updating, recording and destroying the asset.

The nature and value of every asset is documented and understood, better enabling the Council to restrict access where applicable, develop effective recovery and continuity programs and protect the interests and assets belonging to customers and clients.

Understanding the Council's assets, enables us to manage our organisation's information and systems and the risks associated with them. For this purpose, we utilise an Information Asset Register (IAR) to identify, document and map all information assets and assign them an owner.

17.5 Section Objectives

The Council is committed to ensuring compliance with the rules, standards and regulations with regards to asset management and the protection of the personal information in our remit. Due to the nature of the services offered by the Council, we retain and process large volumes of personal data and therefore have strict aims and objectives for achieving and maintaining the appropriate protection of all organisational assets.

The Council's objectives regarding asset management are to: -

- Develop and maintain a defined and robust Asset Management Policy, including procedures for areas such as: -
    - Inventory of Information Assets
    - Assigning Asset Owners
    - Information Classification

  - Personal Information
  - Confidential Information
  - Non-Disclosure Agreements
  - Information Sharing Measures
- Ensure that compliance all information assets have been identified
- Document all assets on the Information Asset Register (IAR) and assign each one an owner for monitoring and accountability
- Define the access to each asset and apply restrictions where applicable
- Maintain an up-to-date Records Management & Retention Policy
- Ensure that all staff are aware of the regulations and their obligations regarding asset management and to provide sufficient and adequate support and training in this regard

17.6 Section Guidelines and Procedures

The Council takes several measures and steps to ensure that asset management is effective and adequate for managing and protecting information. This section is disseminated to all users, who are aware of the value and importance of good records when it comes to the information held and processed by us.

17.7 Register of Information Assets

The Council utilise an Information Asset Register (IAR) to document and categorise the assets under our remit. This not only enables us to map the flow of data within the council, but also serves as a tool for risk assessment and applying mitigating actions from the start.

The register contains all information, hardware, software, systems, applications and physical assets and is reviewed on a quarterly basis to ensure that the information is current and adequate. The register allows for descriptions and additional information fields, ensuring that all assets can be understood and assessed, but as a minimum standard, records: -

- Asset ID
- Asset Type
- Description
- Information Asset Owner (IAO)
- Associated Risks
- Classification
- Location
- Format

- Retention Period
- Whether it contains personal data

17.8 Assigning Asset Owners

Each asset is assigned an owner (IAO) who is responsible for monitoring, maintaining and managing the asset and its use. This enables us to account for each asset and ensures that all risks have been identified and mitigated. The IAO is noted on the IAR and only they are permitted to effect change on or with the asset.

17.9 Unclassified & Short-Term Information Assets

Due to the volume of information assets used by the Council during business, there are some assets which are considered minor and as such are not subject to being classified or documented. This is only applicable where the asset has no security value and will not result in any internal or external risk if accessed. Such assets are also not assigned an owner or inventoried due to their limited nature.

The Council operates under the GDPR and as such complies with the principle to never retain any information where there is no longer a purpose or reason to do so, however some records and information assets must be retained by law for specific retention periods and may come under our non-classification policy.

There is also a requirement due to the nature of our business, to obtain some information assets for limited and short-term periods. Such assets can include letters, spreadsheets, temporary files and reports. These are needed during business but are not classified or inventoried. All staff are aware of their responsibility for the documents they create, and this is further highlighted in our ***Data Retention Policy.***

17.10 Remote Access & Bring Your Own Device (BYOD)

The Council employees occasionally have a requirement to either use Council assets (*physical and information*) outside of the office. Such instance can include during business trips, client visits and during travel. There are also facilities for using a self-owned device in the workplace, such as mobile phones and laptop. We understand the important of asset management for non-council devices and council assets used away from the office and have a robust ***Remote Access & BYOD Policy*** in place.

Regarding asset management when working remotely, it is the Council's aim to protect our staff, other people (*clients, service providers, customers, suppliers*

etc), organisational assets and systems when they are off-site. Our Information Security Program consists of several sections and procedures that overlap in this area and provide our robust and structured approach, controls and measures for protecting assets and access whilst off-site.

These sections include, but are not limited to:

- Information Security Policy
- Risk Assessment Policy & Procedures
- Access Control & Password Policy
- Data Breach Policy
- Remote Access & BYOD Policy
- Asset Management Policy
- Information Asset Register (IAR)
- Clear Desk & Screen Policy
- Data Protection Policy & Procedure

Please refer to the Council's ***Remote Access & BYOD Policy*** for full guidance on measures and controls for off-site use of assets.

17.11 Acceptable Use of Information Assets

Information assets are pivotal to the services offered by The Council and to ensure a secure and effective environment. Employees, Councillors and third parties are provided with access and use of such assets to aid business functions and client assistance. This use is governed by our Acceptable Use standards and failure to comply with these principles may result in contract termination.

The Council has documented and implemented this acceptable use section in our Asset Management Policy to reiterate and provide guidelines on using our own and client assets. This information is disseminated to all employees, third parties and visitors to the Council and forms part of our agreements and terms. All assets, with emphasis on client assets are used in a professional, lawful and ethical manner at all times and are audited on a monthly basis to ensure adherence to this ethos.

Such acceptable use covers all assets and includes, but is not limited to: -

- Email systems
- Internet usage
- Telephones (*including mobiles*)

- PDAs & laptops
- VPN Access, networks and portals

Specific emphasis is placed on adhering to this policy for employees who work from home and/or off-site and use or have access to information assets. Access and activities carried out during these times are logged and audited for compliance with the acceptable use ethos and standards.

Client assets and those with restricted access are not authorised for personal use under any circumstance. Assets are not available for personal use at any time and access to non-business-related internet is restricted. Users are aware of the risks of using assets for personal use, such as personal emails that may contain viruses or permit access to restricted information.

17.11.1 Acceptable Use Standards

The Council has documented and disseminated the below acceptable use standards to provide guidance and rules for using assets. These standards are adhered to by all employees and are a contractual part of any client visit or third-party access to the Council's information assets.

Employees, third parties and visitors are informed that they: -

- Must not do anything to jeopardise the integrity of the systems, information assets or physical assets
- Are not permitted to use information assets for personal use
- Are not permitted to damage, change, reconfiguring or move any system or information asset with written authorisation and management supervision
- Are not permitted to remove any information asset from the Council building without written permission
- Must not attempt to access, delete, modify or disclose Information Assets belonging to other people without their permission
- Are not authorised to use any external systems, applications or technology with existing assets without permission and supervision
- Cannot disable or in any way alter system firewalls, anti-virus software or software/hardware protection applications
- Must not move any physical asset without written permission, including, but not limited to desktop PCs, printers, scanners, monitors or fax machines
- Are not permitted to load any unauthorised software onto The Council systems

- Must not connect to a Council network or any equipment other than in approved circumstances
- Must not create, download, store or transmit unlawful or indecent material
- Are not authorised to purchase or otherwise acquire any technology assets without the knowledge and authorisation of the IT Service Manager (or Town Clerk)
- Always agree to abide by these rules and confirm that the installation of any software on desktop PCs or laptops must only be carried out by IT
- Observe the Council's Data Protection and Information Security policies and guidance in all instances

17.11.2 Internet & Email Usage

The internet is a pivotal part of the services offered by the Council and as such, must be accessible to all employees during their work hours. However, we recognise the security risks of using the internet and so access is only available through the Council's local network or secured wireless network with the appropriate infrastructure and firewall protection. The internet is not permitted for personal use. The Council have also restricted the sharing of files on certain systems and for some individuals, dependant on their need to use such facilities.

Email is necessary for the service provision offered by the Council and is afforded to all employees. This is our main communication tool and enables quick and effective access to clients, customers and other service providers. Email is accessible via secured connection and the sending of files or personal information is restricted to a user required level. Encryption methods are used and are detailed in our Encryption Policy, along with secure credentials.

17.12 Removable Media

The Council defined *'removable media'* as any type of storage device or object that is physically able to be disconnected and removed from a system or computer whilst it is active. Such media types include, but are not limited to USB's, Media Cards, CDs, DVDs and SD cards.

We strictly control the use and oversight of removable media due to their nature and increased access and security risk. Removable media makes it easy for a person to move programs, data and content from one computer to another and as such, the Council ensures that all employees and third parties abide by this policy and our removable media rules. Documented guidance for using removable media provides working practices for the Council that can be adopted by all users, ensuring the safe storage, use and transfer of information.

We control the use of removable media devices, to enable us to: -

- Ensure the access to information is limited and restricted dependant on its purpose and content
- Maintain the integrity of the data and protect its owner and/or source
- Prevent risks and/or security breaches through loss of assets
- Comply with regulations, laws and contractual obligations
- Provide a safe and effective workplace for employees and clients
- Maintain high standards of securing and restricting personal information.
- Prohibit the disclosure of information, both for best practice and as applicable to the data protection laws

17.12.1 Using Removable Media Devices

Unless provided to an employee directly by the Council, we prohibit the use or possession of any removable media devices on-site. Employees sign an agreement to this effect as part of their employment contact and agree to be searched entering and leaving the premises to enforce this rule. Removable media devices pose a serious risk to the information held by the Council and here there is a need for using such devices, these will be owned, controlled and provided by the Council directly.

Where an employee requires a removable media device for use internally or externally, they must request this directly with the Town Clerk, Deputy Town Clerk and/or the IT Service Manager. All requests must be in writing and should state: -

- The removable media device required
- The purpose of the device
- Duration needed for
- How it will be secured and protected during use
- Where the device will be used
- What assets the device will be connected to

All removable media devices and any associated equipment and software are only available through the Council's IT Service Manager, who will place orders and take receipt of any such devices. Where removable media is used to store important, essential or personal information, this will be done so as a backup format and is never the sole location of such data. Removable devices can

become corrupt or inaccessible and there must be alternate and secure backups of all information.

For removable media devices that are needed for use outside of the Councils offices, please see our Remote Working Policy for use and guidelines. Strict encryption software is used on removable media devices that partition the media and enable a secure, segregated data section that is only accessible via login credentials and authentication.

The Council uses the latest virus and malware checking software on all assets to ensure that where removal media devices are being used, these are scanned are authorised prior to allowing access to any networks, systems or servers.

Whilst removable media are in transit, they are secured through internal credential authentication and external security measures. These including being in a locked container that is only accessible to the user and the use of additional encryptions during transit.

17.13 Information Classification

When the Council documents information assets on our Information Asset Register (IAR), each asset is given a classification to help describe the use, purpose, content and risk level associated with it. ***We utilise 5 main classification types: -***

1. **Unclassified** - assets not of value and/or retained for a limited period where classification is not required or necessary
2. **Public** - information that is freely obtained from the public and as such, is not classified as being personal or confidential
3. **Internal** - physical or information assets that are solely for internal use and do not process external information or permit external access
4. **Personal** - information or a system that processes information that belongs to an individual and is classed as personal under the data protection laws
5. **Confidential** - private information or systems that must be secured at the highest level and are afforded access restrictions and high user authentication

When each asset is obtained, they are added to the IAR and are assessed and classified by the owner according to their content. The classification is then used to decide what access restriction need to be applied and the level of protection afforded to the asset. The classification along with the asset type, content and

description are then used to assess the risk level associated with the information and mitigating action can then be applied.

17.14 Non-Disclosure & Confidentiality Agreements

The Council uses a robust and predefined non-disclosure agreement with all employees as part of their employment contract. We also use such agreements for visitors to the Council building, during audits and where contracts, business relationship or supplier connections are formed. The non-disclosure agreement template is altered on a case by case basis to ensure that information seen, disclosed or shared during any relationship with the Council, is secure and protected.

Due to the nature of our business, the Council often shares personal and confidential information with other service providers and clients and as such, relies on clauses and stipulations in our confidentiality agreements. Alongside encryptions and secure transfers, the Council always assess the risk of disclosing any information against the purpose and reason for doing so.

Where information must be shared for business interests or legal reasons, on-disclosure agreements are signed by the third-party prior to any information being disclosed and reviews are conducted to ensure that they have adequate safeguards in place for information transfers.

17.15 Information Labelling, Handling and Disposal

The Council employs a labelling system that categorises the content of systems, files, applications and documents, without the necessity of disclosing the actual contents. This enables our employees to understand what content or information resides on a system or in a location, without accessing or seeing the personal content. Labelling allows us to document and control information, whilst still respecting access restriction.

17.15.1 Disposal of Assets

How we dispose of assets is of paramount importance due to the nature of our business and services. We handle large volumes or personal data and utilise systems that retain and process such data daily. Please refer to our ***Retention & Erasure section*** which details how we dispose of all data, hardware, devices and records.

Reformatting of systems and hardware is our default position, however great care is always exercised when disposing of any equipment which has been used in the processing of information, as there is always a possibility that some information may remain.

17.16 Section Responsibilities

The Council will ensure that all staff are provided with the time, training and support to learn, understand and implement the Asset Management Policy and that direct asset owners are trained and supported in their role. Asset Management at the Council is a top-down approach and every employee understands the importance of the information and assets in our possession.

17.17 Information Asset Owners (IAO)

IAO's act as the nominated owner of specific assets within the Council and are responsible for maintaining the correct information on the IAR and for documenting and understanding how the asset is used, access and of value to the council. Any process or function that affects an asset must first be authorised by the IAO.

17.17.1 Managers and Supervisors

Line managers are held responsible for ensuring that any employee who reports to them is aware of this policy and has been provided with adequate time and resources to understand its contents and meaning.

Any documented manual, handbook, policy or procedures that is related to asset management must be accessible to all employees and managers must be approachable and available should employees have questions regarding assets or their management. Line managers are also responsible for liaising with the IAO(s) to ensure that effective and adequate training is provided to new starts and existing staff on a rolling basis regarding assets, with emphasis on information assets.

18 Information Security

18.1 Section Introduction

The Council has an extensive and robust Information Security Program that consists of a vast array of policies, procedures, controls and measures. This section is the foundation of this program and ties together all other sections as they relate to information security and data protection.

This section covers all aspects of how we identify, secure, manage, use and dispose of information and physical assets as well as acceptable use protocols, remote access, password and encryptions. To ensure that the importance of each information security area is not missed or vague, we use separate sections for each information security area and where applicable, reference external policies in this document.

All information security policies and sections should be read and referred to in conjunction with each other, as their meaning, controls and measures often overlap. The policies, sections and documents that form part of the Council ***Information Security Program are: -***

- Information Security
- Risk Assessment
- Business Continuity Plan
- Remote Access & Bring Your Own Device (BYOD)
- Access Control & Password
- Clear Desk & Screen
- Third Party/Outsourcing
- Supplier Due Diligence & Questionnaire
- Data Retention & Erasure
- Data Protection
- Asset Management

18.2 SECTION STATEMENT

Information and physical security is the protection of the information and data that the Council creates, handles and processes in terms of its confidentiality, integrity and availability from an ever-growing number and wider variety of threats, internally and externally. Information security is extremely important as an enabling mechanism for information sharing between other parties.

The Council are committed to preserving Information Security of all physical, electronic and intangible information assets across the Council, including, but not limited to all operations and activities.

We aim to provide information and physical security to: -

- Protect customer, 3rd party and client data
- Preserve the integrity of The Council and our reputation

- Comply with legal, statutory, regulatory and contractual compliance
- Ensure business continuity and minimum disruption
- Minimise and mitigate against business risk

18.3 Section Purpose

The purpose of this section is to provide the Council's statement of intent on how it provides information security and to reassure all parties involved with the Council that their information is protected and secure from risk at all times.

The information the Council manages will be appropriately secured to protect against the consequences of breaches of confidentiality, failures of integrity, or interruptions to the availability of that information.

18.4 Section Objectives

The Council have adopted the below set of principles and objectives to outline and underpin this section and any associated information security procedures: -

- Information will be protected in line with all our data protection and security policies and the associated regulations and legislation, notably those relating to data protection, human rights and the Freedom of Information Act
- All information assets will be documented on an Information Asset Register (IAR) by the IT Service Manager and will be assigned a nominated owner who will be responsible for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect it
- All information will be classified according to an appropriate level of security and will only be made available solely to those who have a legitimate need for access and who are authorised to do so
- It is the responsibility of all individuals who have been granted access to any personal or confidential information, to handle it appropriately in accordance with its classification and the data protection principles
- Information will be protected against unauthorised access and we will use encryption methods as set out in the above objectives in this policy
- Compliance with this Information Security and associated sections & policies will be enforced and failure to follow either this policy or its associated procedures will result in disciplinary action

The IT Service Manager has the overall responsibility for the governance and maintenance of this document and its associated procedures and will review this policy at least annually to ensure that it is still fit for purpose and compliant with all legal, statutory and regulatory requirements and rules. It is the sole responsibility of the IT Service Manager to ensure that these reviews take place

and to ensure that the policy set is and remains internally consistent.

18.5 Section Procedures & Guidelines

18.5.1 Security Classification

Each information asset will be assigned a security classification by the asset owner or Information Security Officer, which will reflect the sensitivity of the asset. Classifications will be listed on the Information Asset Register.

18.5.2 Access to Information

Users at The Council will only be granted access to the information that they need to fulfil their role within the organisation. Users who have been granted access must not pass on information to others unless they have also been granted access through appropriate authorisation.

18.5.3 Secure Disposal of Information

Care needs to be taken to ensure that information assets are disposed of safety and securely and confidential paper waste must be disposed of in accordance with relevant procedures on secure waste disposal. Where an external shredding service provider is employed, secure paper disposal bins are in each office and used in all instances of confidential paper disposal.

Electronic information must be securely erased or otherwise rendered inaccessible prior to leaving the possession of the Council, unless the disposal is undertaken under contract by an approved disposal contractor.

In cases where a storage system *(for example a computer disc)* is required to be returned to a supplier it should be securely erased before being returned unless contractual arrangements are in place with the supplier which guarantee the secure handling of the returned equipment.

18.5.4 Information on Desks, Screens and Printers

Users who handle confidential paper documents should take the appropriate measures to protect against unauthorised disclosure, particularly when they are away from their desks. Confidential documents should be locked away overnight, at weekends and at other unattended times.

Care should also be taken when printing confidential documents to prevent unauthorised disclosure.

Computer screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons and all computers should be locked while unattended.

18.5.5 DATA ENCRYPTION

Encryption methods are always used to protect confidential and personal information within the Council and when transmitted across data networks. We also use encryption methods when accessing The Council's network services, which requires authentication of valid credentials *(usernames and passwords)*.

Where confidential data is stored on or accessed from mobile devices *(for example, laptops, tablets, smartphones, external hard drives, USB sticks, digital recorders)* the devices themselves are be encrypted (*using "full disk" encryption*), irrespective of ownership. Where strictly confidential data is stored in public, cloud-based storage facilities the data must be encrypted prior to storing to ensure that it is not possible for the cloud service provider to decrypt the data.

Where data is subject to an agreement with an external organisation, the data should be handled *(stored, transmitted or processed)* in accordance with the organisation's specified encryption requirements.

Where there is a requirement to remove or transfer personal information outside of The Council, it is always kept in an encrypted format. Encryption is used whenever appropriate on all remote access connections to the council's network and resources. The Council also has documented protocols for the management and use of electronic keys, with a view to controlling both the encryption and decryption of confidential and sensitive information.

All confidential and restricted information transmitted via email is encrypted. Where a secret key is provided to decrypt, this is done so in a separate format to the original email.

18.5.5.1 Encryption Keys

Definitions

Encryption: This is the process of locking up (*encrypting*) information using cryptography. Such information appears illegible if access, unless a corresponding key is used to decrypt the data.

Decryption: The process of unlocking the encrypted information via a key.

The Council utilise both asymmetric and symmetric key encryption algorithms, dependant on the systems, purpose and information. The type of encryption is

decided by the IT Service Manager after assessing the requirements of the information and transfer.

Asymmetric Key Encryption Algorithms: A type of encryption algorithm whereby two different keys are used. One key is for encrypting the information and the other for decrypting. This type is also known as public-key encryption.

Symmetric Algorithms: These are also referred to as *"secret key encryption"* and use the same key for both encryption and decryption.

18.5.5.2 Approved Encryption Algorithms and Protocols

The Council use a variety of encryption methods dependant on the nature of the information being stored or transferred, its location and its use. Below are the standard and acceptable forms of encryption used by The Council.

Symmetric Key Encryption Algorithms

- Triple Data Encryption Standard (3DES)- Minimum encryption key length of 168 bits
- Advanced Encryption Standard (AES)- Minimum encryption key length of 256 bits

Asymmetric Key Encryption Algorithms

- Digital Signature Standard (DSS)
- Elliptic Curve Digital Signature Algorithm (ECDSA)

Encryption Protocols

- IPSec *(IP Security)*
- SSL (*Secure Socket Layer)*
- SSH (*Secure Shell)*
- TLS (*Transport Layer Security)*

18.5.5.3 Key Use & Protocols

Encryption key management is fully automated, and all private keys are kept secure, restricted and confidential. Whilst keys are in transit and/or storage, they are always encrypted.

Due to their nature, when the Council use symmetric encryption key algorithms, there is a requirement to share the secret key with the recipient. Protecting and securing the key for sharing is paramount to protecting the information the key encrypts, and so encrypting the key itself is a mandatory requirement. During distribution and transfer, the symmetric encryption keys are always encrypted

using a stronger algorithm with a key of the longest key length for that algorithm.

The Council's aim when encrypting secret keys is to afford them a higher, more stringent level of protection than the encryption used to protect the data. When keys are at rest, they are again secured with encryption methods, equal to or higher than the existing encryption level.

Where asymmetric algorithms are used, the public key is passed to the certificate authority to be included in the digital certificate that will be issued to the end user. Once the digital certificate is issued, it is then made available to all relevant parties. The corresponding private key is only made available to the end user who is in receipt of the corresponding digital certificate.

18.5.6 REMOTE ACCESS

It is the responsibility of all the Council's users with remote access privileges to the council network, to ensure that their remote access connection is given the same consideration as the user's on-site connection to The Council. ***Refer to our Remote Access & BYOD Policy for protocols and more information.***

- Secure remote access must be strictly controlled
- Control will be enforced via one-time password authentication or public/private keys with strong passphrases
- At no time, should any the Council employee provide their login or email password to anyone else
- The Council's users with remote access privileges must ensure that their The Council owned or personal computer or workstation, which is remotely connected the council network, is not connected to any other network at the same time, except for personal networks that are under the complete control of the user.
- All hosts that are connected to The Council internal networks via remote access must use the most up-to-date anti-virus software

18.5.7 FIREWALLS & MALWARE

The Council understands that adequate and effective firewalls, anti-malware and protected gateways are one of the main and first lines of defence against breaches via the internet and our networks.

We utilise configured firewalls and have daily anti-virus applications running on all computers, networks and servers. The IT Service manager is responsible for checking the log of all scans and for keeping these applications updated and compliant.

Systems are regularly scanned and assessed for unused and outdated software with the aim of reducing potential vulnerabilities and we routinely remove such software and services from our devices where applicable.

The IT Service manager also has full responsibility for ensuring that the latest application and software updates and/or patches are downloaded and installed, keeping our security tools current and effective. Security software is reviewed and updated monthly, or sooner where updates or patches have been released.

18.6 Security Breach Management

18.6.1 Introduction

The Council's definition of a breach for the purposes of this and related documents, is a divergence from any standard operating procedure (SOP), which causes a failure to meet the required compliance standards as laid out by our own compliance program objectives and/or those of any regulatory body.

Compliance in this document means any area of business that is subject to rules, laws or guidelines set out by a third party which are to be followed and which, when breached, could cause emotional, reputational or financial damage to a third party.

18.6.2 Breach Management Approach

The Council has robust objectives and controls in place for preventing security breaches and for managing them if they do occur. Due to the nature of our business, the Council processed and stores a vast amount of personal information and confidential client data and as such, require a structured and documented breach incident program to mitigate the impact of any breaches. Whilst we take every care with our systems, security and information, risks still exist when using technology and being reliant on human intervention, necessitating defined measures and protocols for handling any breaches.

We carry out frequent risk assessments and gap analysis reports to ensure that our compliance processes, functions and procedures are fit for purpose and that mitigating actions are in place where necessary, however should there be any compliance breaches, we are fully prepared to identify, investigate manage and mitigate with immediate effect and to reduce risks and impact.

The Council have the below objectives with regards to Breach Management: -

- To maintain a robust set of compliance procedures which aim to mitigate against any risk and provide a compliant environment for trading and

business activities

- To develop and implement strict compliance breach and risk assessment procedures that all staff are aware of and can follow
- To ensure that any compliance breaches are reported to the correct regulatory bodies within the timeframes as set out in their code of practice or handbooks
- To use breach investigations and logs to assess the root cause of any breaches and to implement a full review to prevent further incidents from occurring
- To use the Compliance Breach Incident Form for all breaches, regardless of severity so that any patterns in causes can be identified and corrected
- To comply with regulating bodies and laws on compliance breach methods, procedures and controls
- To protect consumers, clients and staff – including their data, information and identity

18.7 PCI DSS Compliance

As the Council take, use or store cardholder data, we choose to comply with the industry leading Payment Card Industry Security Standards Councils regulations and guidance and take full responsibility for managing the security standards and our approach to compliance in this area. We understand the payment card brands directly (*Visa, MasterCard etc*.) enforce compliance with the PCI Data Security Standards (PCI DSS) and remain updated with any regulations and codes of conduct as they apply to us.

The Council confirms that we are PCI compliant and have a valid certification which covers our payment system. Our staff are fully trained on the requirement under the PCI DSS and have prompt reminders on screen or in hard copy format when taking payments. Any call recordings are automatically switched off during the relay of card and/or payment information and our card processing activities and associated systems and technologies comply with the PCI-DSS standard.

18.7.1 Definitions

Credit Card Data - Full magnetic strip or the PAN (Primary Account Number) plus any of the following:

- Cardholder name
- Expiration date

- Service Code (CVS)

PCI-DSS - Payment Card Industry Data Security Standard

PCI Security Standards Council - The security standards council defines credentials and qualifications for assessors and vendors as well as maintaining the PCI-DSS.

Self-Assessment - The PCI Self-Assessment Questionnaire (SAQ) is a validation tool that is primarily used by merchants to demonstrate compliance to the PCI DSS.

PAN - Primary Account Number is the payment card number (credit or debit) that identifies the issuer and the particular cardholder account. It is also called Account Number.

18.7.2 PCI DSS Approach & Protocols

The Council takes PCI compliance very seriously and understands our obligations to protect cardholder data. The Council aims to meet the below policy objectives, which have been created in accordance with the actual PCI standards as set out for vendors.

- Create PA-DSS compliant Payment Applications that facilitate and do not prevent our customers PCI DSS compliance
- Follow the best practices of the PCI DSS Requirements whenever we process or transmits cardholder
- Educate staff, customers, integrators, and resellers on how to install and configure the Payment Applications in a PCI DSS-compliant manner
- Ensure that our Payment Applications meet PA-DSS Requirements by successfully passing a PADSS
- Assessment as specified in PCI PA-DSS Requirements and Security Assessment Procedures
- Comply with the Vendor Release Agreement (ROV) including the adoption and implementation of Vulnerability Handling Policies consistent with industry best practices
- Create a PA-DSS Implementation Guide, specific to each application, in accordance with the requirements in the PA-DSS
- Adhere to our own defined software versioning methodology as validated and documented in the ROV1.
- Install and maintain a firewall configuration to protect data and never use vendor-supplied defaults for system passwords and other security

parameters

- Protect stored data by using encryption methods, restricted access and login authentication
- Encrypt transmission of cardholder data and sensitive information across public networks
- Use and regularly update anti-virus software and develop and maintain secure systems and applications
- Restrict access to data by business need-to-know and assign a unique ID to each person with computer access
- Track and monitor all access to network resources and cardholder data and regularly test security systems and processes
- Ensure that all payments transactions are compliant and that any stored personal or card details are done so in accordance with the PCI-DSS
- Ensure that all staff are fully trained on the PCI requirements and using any PCI compliant payment software and/or systems
- Ensure that staff have regular training on PCI compliance to ensure adherence to the standards and our own business objectives
- Ensure that all customers are informed of any rights that they have under the PCI compliance standards

18.7.3 CARD STORAGE & DISPOSAL

The Council complies with all PCI-DSS requirements when it comes to the storage and disposal of any personal and/or card information. We ensure that each of the below objectives are achieved through our PCI, compliance, secure waste disposal, retention and information security procedures: -

- Credit card information is not entered onto or stored on any of the Council's network servers, workstations, or laptops
- Credit card information is never transmitted via email and we advise all customers and clients to adhere to this rule as well
- Web payments are always processed using a PCI-compliant service provider and credit/debit card numbers are not entered into a web page of a server hosted on our own personal network
- Electronic storage of credit/debit card data is prohibited by this policy and our relevant officers carry our regular and routine checks and audits to ensure that these policy objectives is not being violated

- All hard-copy, paper documents containing credit/debit card information are limited to instances specifically required by the transactions and if there is a need to retain such information, it is kept in a secure and safe location, only accessible by authorised staff.
- Where hard-copy card details have been retained, the Council follows it secure waste disposal policy and procedures for destroying the documents via approved methods once business needs no longer require retention

18.8 Section Responsibilities

All information users within the Council are responsible for protecting and ensuring the security of the information to which they have access. Managers and staff are responsible for ensuring that all information in their direct work area is managed in conformance with this policy and any subsequent procedures or documents. Users who act in breach of this policy, or who do not act to implement it, may be subject to disciplinary procedures.

The Council will ensure that staff do not attempt to gain access to information that is not necessary to hold, know or process and that restrictions and/or encryptions are in place for specific roles within the organisation relating to personal and/or sensitive information.

19 Publication Scheme & Freedom of Information Policy

19.1 Section Introduction

Newquay Town Council, as the first tier of local government for the town, has a range of powers and provides a growing number of local services. It believes in openness and working closely with all of its communities of place and interest. It is also determined to involve as many of its citizens as possible in its decision making processes. It has based this, it's Publication Scheme on the statutory Model Publication Scheme for local councils and hopes it will help to develop a greater culture of transparency, awareness and understanding. It will be supplemented with an Information Guide which will give greater detail of what the Council will make available and hopefully make it easier for people to access it.

19.2 Scope of this Section

The purpose of the scheme is to be a means by which the Council can make a significant amount of information available routinely, without waiting for someone to specifically request it. The scheme is intended to encourage local

people to take an interest in the work of the Council and its role within the community. In accordance with the provisions of the Freedom of Information Act 2000, this Scheme specifies the classes of information which the Council publishes or intends to publish.

19.3 Model Publication Scheme

This model publication scheme has been prepared and approved by the Information Commissioner. It may be adopted without modification by any public authority without further approval and will be valid until further notice.

This publication scheme commits an authority to make information available to the public as part of its normal business activities. The information covered is included in the classes of information mentioned below, where this information is held by the authority. Additional assistance is provided to the definition of these classes in sector specific guidance manuals issued by the Information Commissioner.

- To proactively publish or otherwise make available as a matter of routine, information, including environmental information, which is held by the authority and falls within the classifications below.

- To specify the information which is held by the authority and falls within the classifications below.

- To proactively publish or otherwise make available as a matter of routine, information in line with the statements contained within this scheme.

- To produce and publish the methods by which the specific information is made routinely available so that it can be easily identified and accessed by members of the public.

- To review and update on a regular basis the information the authority makes available under this scheme.

- To produce a schedule of any fees charged for access to information which is made proactively available.

- To make this publication scheme available to the public.

19.4 Classes of Information

Who we are and what we do: Organisational information, locations and contacts, constitutional and legal governance.

What we spend and how we spend it: Financial information relating to projected and actual income and expenditure, tendering, procurement and contracts.

What our priorities are and how we are doing: Strategy and performance information, plans, assessments, inspections and reviews.

How we make decisions: Policy, proposals and decisions. Decision making processes, internal criteria and procedures, consultations.

Our policies and procedures. Current written protocols for delivering our functions and responsibilities.

Lists and Registers. Information held in registers required by law and other lists and registers relating to the functions of the authority.

The Services we Offer. Advice and guidance, booklets and leaflets, transactions and media releases. A description of the services offered.

The classes of information will not generally include:

- Information the disclosure of which is prevented by law, or exempt under the Freedom of Information Act, or is otherwise properly considered to be protected from disclosure.

- Information in draft form.

- Information that is no longer readily available as it is contained in files that have been placed in archive storage, or is difficult to access for similar reasons.

19.5 Methodology Statement

The authority will indicate clearly to the public what information is covered by this scheme and how it can be obtained. Where it is within the capability of a public authority, information will be provided on a website.

Where it is impracticable to make information available on a website or when an individual does not wish to access the information by the website, a public authority will indicate how information can be obtained by other means and provide it by those means.

In exceptional circumstances some information may be available only by viewing in person. Where this manner is specified, contact details will be provided. An appointment to view the information will be arranged within a reasonable timescale. Information will be provided in the language in which it is held or in such other language that is legally required. Where an authority is legally required to translate any information, it will do so. Obligations under disability and discrimination legislation and any other legislation to provide information in other forms and formats will be adhered to when providing information in accordance with this scheme.

19.6 Potential Charges for Information

The purpose of this scheme is to make the maximum amount of information

readily available at minimum inconvenience and cost to the public. Charges made by the authority for routinely published material will be justified and transparent and kept to a minimum. Material which is published and accessed on a website will be provided free of charge. Charges may be made for information subject to a charging regime specified by Parliament. Charges may be made for actual disbursements incurred such as:

• Photocopying

• Postage and packaging

• The costs directly incurred as a result of viewing information

Charges may also be made for information provided under this scheme where they are legally authorised, they are in all the circumstances, including the general principles of the right of access to information held by public authorities, justified and are in accordance with a published schedule or schedules of fees which is readily available to the public. If a charge is to be made, confirmation of the payment due will be given before the information is provided. Payment may be requested prior to provision of the information.

19.7 Data in alternative Formats

Equality Act 2010 – copies of this document in large print (A3 Format) or larger font size can be made available for those with sight impairment on request from the Council Office or by telephoning 01637 878388 or e-mailing the Town Clerk's Office.

19.8 Freedom of Information

In accordance with the Freedom of Information Act 2000, this Document will be posted on the
Council's Website www.newquaycouncil.uk.

20 Risk Management

20.1 Section Statement

The council are committed to ensuring that we understand and adhere to all regulatory and legal requirements regarding our risk management obligations. Whilst we accept that not all risks can be eliminated, we are committed to ensuring robust and effective controls, measures and processes to identify gaps and risks, have proportionate oversight functions and mitigate risk where possible.

Operational managers are tasked with risk mitigation and we utilise the ***Three Lines of Defence*** model in our approach, ensuring that effective management control, adequate risk control and compliance oversight functions and internal independent audits are established within our risk management framework. Effective lines of communication and collaboration across the Council, ensures that gaps are easily, and quickly identified and duplicated functions are removed.

This document states our risk management objectives and lays out our approach to managing and mitigating risks, as well as providing defined and detailed

procedures for identification, assessment, mitigation and correction actions. We are dedicated to ensuring that all employees are fully trained and understand the implications of risk and know that our structured procedures, systems and controls have been put into place to identify the risks, mitigate where possible and prevent unnecessary harm or damage to any individual or entity.

20.2 PURPOSE

The purpose of this policy is to provide our objectives, intent, approach and procedures for risk management and assessment, and to act as a guidance and reference document for all users. Effective risk management requires a robust and defined framework, detailing the functions, actions and controls used to identify, assess and prevent risks.

In addition to standard business risks and those associated with our business type and industry, we also recognise the risks that result from processing personal data and understand our obligation to protect and secure personal data by identifying and mitigating the risks posed.

The Council are committed to ensuring a risk-based approach towards personal data and the protection of individual's rights and freedoms and utilise such an approach as an effective tool for securing personal data and mitigating associated risks. Such measures and tools better enable us to provide funding, allocate resources and ensure that preventative measures are implemented in any areas where risks or potential harm towards individuals is identified.

20.2.1 WHAT IS RISK?

The Council's definition of a ***'risk'*** is: -

An event, action or cause leading to uncertainty in the outcome of the Council's operations. This risk may be financial, reputational, regulatory, legal or ethical and can affect one to many persons associated with the Council.

With regards to privacy and the protection of data, we define ***'risk'*** in terms of the severity, impact and/or probability a breach, function or processing activity would have to individuals. When referring to personal data risks, we consider varying factors, including if the rights and freedoms of individuals will be affected or compromised, severity of any impact (*i.e. loss, threat, unauthorised disclosure*) and whether mitigating controls and measures already in place (*or able to be implemented*) would reduce impact, severity and/or probability.

The stages in risk assessment are to: -

- identify the main risks to your objectives, business and customers
- assess/measure the importance, impact and likelihood of the risk

- mitigate the risks through corrective actions, controls and operational measures
- reassess the risk importance, impact and likelihood
- ongoing monitoring of the risk and mitigating controls

20.3 OBJECTIVES

The Council have developed several objectives for identifying, assessing, mitigating and monitoring risks.

The Council ensures that we: -

- Identify and assess all risks and where necessary, treat/address them in a timely manner
- Have effective processes to identify, manage, monitor and report the risks we are *(or might be)* exposed to
- Established, implement and maintain adequate risk management and security policies and procedures, including effective controls for risk assessment, identifying the risks relating to our activities, processes and systems, and where appropriate, set the level of risk tolerated by us
- Apply adequate and effective controls to mitigate the identified risks within the agreed parameters and regularly test these controls to ensure that they remain effective and appropriate
- Review risks (*frequency determined by risk score)* and related procedures for adequacy and relevance, as well as re-assessing new risks that we might me exposed to
- Conduct reverse stress testing to ensure that the controls, systems and procedures put into place for risk management are effective and mitigate the risks of business failure
- Have compliant and robust remuneration policy and procedure in place to prevent internal risks associated with unfair business practices through competitive sales and/or advice
- Provide staff with sufficient training and support to manage our risk management obligations and objectives
- Conduct risk assessments on all new business ventures, systems, functions to ensure that they are aligned with the goals and objectives in this policy
- Assign responsibilities for risk management, security and data protection and ensure an unbiased, support role for each
- Ensure there are processes in place to analyse and log any identified threats, vulnerabilities, and potential impacts associated with our business activities and information (*risk register)*
- Utilise a risk matrix for rating and scoring the impact and likelihood of nay

identified risk and using this score for the frequency of monitoring, migration requirements and for making informed decision about the risk(s)

- Identify and analyse the GDPR requirements for risks relating to personal data, with emphasis on any high-risk processing activities and processing special categories of personal data
- Review all processing activities on a frequent basis to assess their risk rating and to identify any gaps or new risks associated with the processing of personal data
- Define procedures and reporting mechanisms for data protection impact assessments (DPIA) where mandatory under the data protection laws

20.4 Data Protection Risks

Where the Council processes personal information as part of our business functions, we have risk assessment measures in place with the specific purpose of assessing the risk posed to individual's when their data is processed and the risk of the processing activity itself.

Recital 74 of the GDPR states that: *"the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should consider the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons."*

Whilst the risk measures and management around data protection and privacy are within the scope of this risk assessment document, any activity identified as high-risk or meeting the Article 35 requirements are subject to our separate ***Data Protection Impact Assessment (DPIA) Procedures.***

20.4.1 Data Protection Impact Assessment (DPIA)

This risk policy and procedures document is for assessing the risks to our business, personal data, function and customers and does not extend to the risks associated with the GDPR's Article 35 Data Protection Impact Assessment requirements. We have a specific procedure document and recording templates for carrying out DPIA's which is specific to personal data, data protection and high-risk processing

20.4.2 Data Protection Officer (DPO's)

The DPO's responsibility and obligation to be part of any advice on any ***Data Protection Impact Assessments (DPIAs)*** is detailed in our DPIA Policy & Procedures. However, where any risk *(high or low)* involves personal data, data

subjects and/or processing activities, the Council involve the DPO in all risk assessments and subsequent advice and decisions. in the organisation.

Where others within the organisation carry out all or part of the risk assessment process, they escalate personal data matters to the DPO, who then decides if there is sufficient risk to apply the DPIA screening questions assessment.

20.5 Approach to Risk Management

In relation to IT Security, the Council utilises the Three Lines of Defence approach in our risk management, which provides an effective framework for our 3-tiered method of identifying, assessing and managing risk. It is essential to the functioning and compliance of our business that all risks are identified and managed and that reporting lines and communication is effective and efficient. Using an ownership, oversight and audit framework allows a multi-faceted approach to risk, preventing gaps and removing duplications.

Our Three Lines of Defence framework is: -

1) Operational and line managers are responsible for identifying, assessing, managing and owning risk in their defined area and are tasked with developing and implementing corrective actions where applicable. Managers are responsible for the employees in their department and for supervising procedures and tasks associated with any defined risks. Risk controls, measures and the day-to-day monitoring fall within the managers remit. Operational managers are also responsible for training employees on risk management and the Council's defined approach.
2) The Town Clerk / Deputy Town Clerk are responsible for the oversight of the managers and their approach to risk, ensuring that a second line of defence is in place. This second level monitors and assesses the controls, measures and corrective actions that are in place and report directly to the Finance & Policy Committee. The Town Clerk & Deputy Town Clerk are responsible for the quality management of the risk functions of all managers and are tasked with ensuring the appropriate, adequate and effective operation of those functions. They are also responsible for providing training and support to the operational managers.
3) The Council operate a Finance & Policy Committee who acts as the third line of defence and provides independent monitoring and analysis of the overall risk management functions and approach. The auditor reports directly to this committee and provides management information reporting to the committee on any issues and/or areas for improvement. Having an independent audit role enables the Council to assess, review and improve our risk management function and to ensure that we take an encompassing approach to assessing and managing risk. The auditor is also responsible for assessing the functions and processes against regulations and legislation and ensuring their compliance and

adequacy.

20.5.1 RESPONSE TO RISK

The Council employs 4 main options in response to any risks: -

- **Tolerate** – if we cannot reduce the risk in a specific area, we can decide to tolerate the risk *i.e*. do nothing further to reduce the risk. Tolerated risks are to be noted on the Risk Assessment Register, without any intended further actions. If the risk is shown as ***'green'*** after existing mitigating actions are taken, it is usually okay to tolerate it. Tolerated risks are those with no impact effect and no future probability of future recurrence.
- **Treat –** if we can reduce the risk in a sensible way by identifying mitigating actions and implementing them, we should do so. For most risks on the Risk Assessment Register, this is the action that is/will be taken. If there is any probability of the risk occurring again, it must be treated, and the necessary mitigating actions put into place to prevent further occurrence.
- **Transfer –** in this case, some risk can be transferred to other organisations i.e. by way of using insurance or outsourcing certain tasks/services.
- **Terminate –** this applies to risks we cannot mitigate other than by no longer carrying out work in that area. i.e. if a planned project is deemed too high risk and the risks cannot be mitigated, we may decide to cancel the project.

20.6 FIRST LINE PROCEDURES

20.6.1 IDENTIFY THE RISK

All first line procedures are the responsibility of the operational managers. All areas of a manager's department are reviewed to identify risk, ***including: -***

- All staff, including due diligence, background checks, referencing and further checks not listed here
- All tasks and activities carried out within the business as part of its functioning
- Systems and controls
- Existing procedures relating to legal and regulatory obligations, rules and requirements
- Suppliers and other 3rd party associations
- Customers and clients
- Compliant logs
- Previous insurance claims

Identified risks are recorded on the risk register, regardless of rating, impact or likelihood. The identification stage includes: -

- Defining the risk in a clear and simply statement
- Recording the risk on the risk register
- Deciding who has overall responsibility for the risk

20.6.2 ASSESS THE RISK

A risk assessment is carried out on all risks, regardless of impact or likelihood. Risks are recorded on the register and the assessment also rates the risk in terms of the probability and impact.

During the risk assessment stage, we: -

- Define the risk in a clear statement
- Identifying if the risk does/could adversely affect the function or delivery of the project that the risk relates to
- Record the objectives and benefits of the function/project to enable risk acceptance decision
- Assess the importance, probability and the impact of each risk
- Decide whether the level of risk is acceptable
- Identify possible mitigating or corrective actions that can be taken to eliminate or reduce the risk impact and/or likelihood
- Review whether any existing control measures are effective
- Decide what action should be taken to control or mitigate the risk
- Decide how urgently the action needs to be taken

20.6.2.1 Risk Rating

Part of the risk assessment is to rate the risk in terms of impact and likelihood (*probability of the risk occurring)*. We use a predefined Risk Matrix to give each risk a rating score, which assists in manging the risk and deciding on further actions. The rating provides a colour code for how severe the risk is and therefore the necessity of putting mitigating/corrective actions into place.

Risks will usually fall into one of three categories: -

- ***Risks to Individuals*** - Any risk that affects an individual (*data subject, employee, client etc*). The main risks to individuals are posed by data protection risks and information processing.
- ***Compliance Risks*** - These can arise where the assessment response indicates that a breach of laws, legislation and/or regulations will occur if the processing goes ahead. This can also include breaching codes of

conduct as relevant to a council's business type or the services/products offered

- ***Corporate Risks*** - Risks that will affect the business, including reputation, revenue, fines and sanctions.

The risk rating table below uses the common *'Red, Amber, Green (RAG)'* matrix, where each risk is given a RAG score based on the likelihood versus the impact. This rating is also provided in more detail in our ***Risk Matrix***.

LIKELIHOOD	IMPACT					
		Trivial (1)	**Minor (2)**	**Moderate (3)**	**Major (4)**	**Severe (5)**
	Certain (5)	**Low Med**	**Medium**	**High**	**Very High**	**Very High**
	Likely (4)	**Low**	**Low Med**	**Med High**	**High**	**Very High**
	Possible (3)	**Low**	**Low Med**	**Medium**	**Med High**	**High**
	Unlikely (2)	**Low**	**Low Med**	**Low Med**	**Medium**	**Med High**
	Rare (1)	**Low**	**Low**	**Low Med**	**Medium**	**Medium**
Impact Score x Likelihood Score = Risk Rating						

- **GREEN** - Where an assessment outcome is Green, we still work to see if we can develop and implement any solutions or mitigating actions that can be applied to reduce the risk impact down as far as possible. However, most green rated risks are acceptable and so focus should be placed on those with higher ratings. Even where a green RAG rating has been given at the risk/privacy identification stage, this risk will still be added to the mitigating actions template for continuity and to ensure that all risks have been recorded and assessed.

- **AMBER** - Where an assessment outcome is Amber, mitigating actions are always proposed and outcomes envisaged, before processing is approved. The aim is to reduce all risks down to a green (*acceptable)* level, however there will be occasions when processing must take place for legal/best interest reasons and so some processing with risks will go ahead and must be accepted into the project. All solutions and mitigating actions must first be considered, tried and applied if possible. ***If the risk is associated with the processing of personal data, the risk should be escalated***

to the Data Impact Assessment screening questions to ascertain if a complete DPIA is required.

- **RED** - Where an assessment outcome is Red, it indicates that either or both impact and/or likelihood scores are unacceptable, and that complete solutions and mitigating actions would be required to bring both indicators down to an acceptable level. Some activities are eliminated at this point as the impact is considered to high risk to proceed.

  However, in instances where the activity or project is essential or is a legal requirement, the proposed solutions and mitigating actions are applied, and a further risk assessment carried out to see if the risk score can be reduced to an acceptable. ***If the risk is associated with the processing of personal data, the risk should be escalated to the Data Impact Assessment screening questions to ascertain if a complete DPIA is required.***

Once the risk assessment has been carried out, we use the overall risk rating to make the decision whether to: -

- **PREVENT:** High-probability/high-impact risk (*we actively work to mitigate these)*
- **ACCEPT:** Low-probability/low-impact risks *(maintain vigilance)*
- **CONTAIN**: High-probability/low-impact risk (*minimize likelihood of occurrence)*
- **PLAN**: Low-probability/high-impact risks *plan steps to take if this occurs)*

20.6.3 MANAGE THE RISK

Managing risks involves: -

- Eliminating them so far as is reasonably practicable
- If it is not possible/practical to eliminate a risk, we aim to minimise it as far as is reasonably practicable
- Applying corrective actions to mitigate a risk where possible

Where a risk or its affects can be managed, or controlled, we operate a hierarchy system based on the risk matrix rating. We prioritize those risks with the highest rating *(therefore most likely to occur and/or could have the most impact)* as those that should have controls put into place to immediately to eliminate/minimise them. We then work through the risk register putting controls into place based on a descending rating order.

To control or eliminate the assessed risk, we use a hierarchy of control. Where possible, we always aim to eliminate a risk, as we recognise that this is the most effective form of control. However, where elimination is not an option, we aim to minimise the risk by working through the alternatives in our hierarchy system.

Level 1 Risk Mitigation Measures	**RISK REMOVAL**
The most effective control measure involves eliminating the risk altogether along with any associated affects. Where possible, we will either opt to not introduce the risk into the business in the first place, or if already in place and the risk has been assessed as an elimination option, we will take steps to remove the risk altogether.	
Level 2 Risk Mitigation Measures	**RISK SUBSTITUTION/ISOLATION**
If total removal of the risk is not possible due to business or external factors, we will aim to substitute the risk object/situation with an appropriate alternative that produces less of or no risk. ***Level 2 measures include: -*** • Using different systems • Altering the existing procedures of a function or activity • Using alternate suppliers • Isolating tasks/systems from certain staff and/or departments • Outsourcing the risk to a 3rd party	
Level 3 Risk Mitigation Measures	**RISK REDUCTION**
Where the impact and/or probability of a risk is medium to low and where possible, we try to reduce the likelihood of the risk occurring and/or the effects and impact that the risk might have. This is done through mitigating and correction actions, including: - • Quality control measures and procedures • Frequent monitoring and audits • Continuous compliance with legal, regulatory and business obligations • Staff training and assessments • Changes to procedures • Off-site back-ups and Business Continuity Plan	
Level 4 Risk Mitigation Measures	**ACCEPT THE RISK**
Where the impact and/or probability of a risk is low and where we are unable to apply any of the measures for levels 1-3, we accept the risk and its	

implications. Level 4 is only applied where a risk in unlikely to cause any measured damage or harm to the business, its customers and/r its clients.

Where a risk is accepted, we still have an incident response plan and business continuity plan in place to ensure that if a low-probability risk occurs, we have the procedures, resources and controls in place to handle it.

20.6.3.1 Risk Mitigating Actions

When risks are identified and assessed as being acceptable to the functioning of the business and cannot be eliminated, we develop and implement mitigating actions where possible, to reduce the impact and/or likelihood of the risk. Managers use the **IT *Risk Mitigating Action Plan*** for each risk, detailing what actions, processes and controls can be used to reduce the risk.

20.6.3.2 Risk Corrective Actions

Corrective actions are defined as those required where there has been an issue or breach. A new or first identified risk is given mitigating actions to reduce the impact and likelihood, however where those actions fail to prevent the risk from occurring, managers are required to carry out a reassessment of the risk and any failing processes or functions that contributed to it occurring. Some risks are expected during the Council's business and cannot be eliminated, however as time, resources and technology develops, it is possible to put new actions into place to mitigate risks.

Managers use the below ***Risk Management Corrective Action Plan*** for assessing a risk that has occurred and to put new corrective actions into place.

RISK MANAGEMENT CORRECTIVE ACTION PLAN			
Assessor Name:	**Date:**	**Risk:**	
Did the risk occur due to it not being previously identified?			**YES/NO**
Had the risk previously been assessed and had mitigating actions implemented?			**YES/NO**
Cause/s Identified:			
Cause/s to be Corrected:			

New Mitigating Strategies	**Indicators of Success**	**Monitoring Methods**
e.g. 2 persons check team prior to data upload	*e.g. zero upload errors*	*e.g. audits*
	e.g. consistent data results from both team checkers	*e.g. 3rd person check prior to upload*

20.7 Risk Register

The Council uses an **IT *Risk Register*** to record the details of all the risks identified within the business relating to IT. These include internal and external risks, ongoing risks and those defined at the beginning and during the life of a project. All risks are scored based on their impact and probability ratings and then this risk is assigned to the register and used to make decisions on mitigating and corrective actions. Managers are responsible for adding each identified risk to the register and for reviewing the risks monthly.

Our Risk Register includes: -

- A unique identifier for each risk
- A description of the risk
- Risk Score/Rating
- Assessment of probability and/or impact
- Who is responsible for managing the risk?
- Summary of proposed corrective and/or preventative actions

20.8 Second Line Procedures

20.8.1 Review & Monitor the Risks

The controls and procedures that operational managers put in place to identify, assess and manage the risks associated with our business, are monitored and reviewed regularly to make sure they work as planned and are adequate and effective. Set officers are responsible for monitoring and auditing the risks and their corrective actions, as well as the support and training provided by the managers to employees in their respective departments.

Officers are tasked with ensuring the effective risk management functions and practices by operational management and to support and assist those managers in setting targets, defining the risks and reporting requirements. Quality monitoring forms a large part of the second line of defence approach, which aims to remove gaps and duplicated functions.

The Compliance Officer establishes processes and functions to ensure that managers and the first line of defence is adequate, effective and is operating as intended. This level is essential to the Council for ensuring an added oversight function and reducing the human error element that is present in all processes and actions.

Officers will use several methods and controls in their oversight capacity, including (*but not limited to*): -

- Carrying out audits and tests to ensure that the controls in place work and are effective
- Disaster Recovery tests to ensure that back-ups and controls are effective and appropriate
- Manager and team meetings are held each month to keep the staff informed of any changes to the risk management program and to ensure that staff know and understand their risk management responsibilities
- Scenario testing is carried out on staff and systems so that any gaps can be identified and rectified
- Identifying and communicating known and new issues and gaps
- Assisting management in developing and implementing effective risk controls and measures
- Supporting and training managers in their risk management functions and duties
- Reporting to the Town Clerk & Deputy Town Clerk

20.9 THIRD LINE PROCEDURES

20.9.1 AUDITS

To ensure a complete and effective approach to risk management, The Council uses the Three Lines of Defence model, which incorporates an independent auditor/audit committee who review, audit and report to the Finance & Policy Committee**.**

The auditor(s) is provided with the budget, tools and resources to carry out independent, unbiased and objective audits of all risks, their identifications, assessment, classification and management as well as assessing and auditing

the Senior Management functions and approach. This third level of defence enables us to objectively review our risk management processes and ensure that all areas are operating effectively, adequately and proportionately.

The auditor(s) uses multiple methods to assess and review the functions and employees to ensure the effectiveness of governance, risk management and internal controls. Their remit includes: -

- Reporting to the Finance & Policy Committee
- Assessing all elements and facets of the risk management framework
- Reviewing the support and training provided by the managers to employees and the Senior Managers/Compliance Officer to the Managers
- Reviewing the Risk Register and Mitigating/Corrective Action plans and assessing their ratings and outcomes
- Auditing the functions and processes in place to reduce/mitigate risk and ensure they are appropriate, effective and adequate
- Ensuring the reliability and integrity of the management reporting processes
- Reviewing and ensuring compliance with regulations and laws

20.10 Documenting Risk Assessments

The Council details throughout this document how and when the stages of risk assessment are recorded. We understand the need and requirement to document all identification, mitigating actions, risk rating, reviews and audits and maintain effective and adequate documents for evaluation, pattern analysis and compliance.

It is our aim to fully evidence and demonstrate all aspects of our risk assessments *(including DPIA's for which the documentation requirements are stated in our **DPIA Procedures**)*, which are documented in all cases, regardless of the size, scope, nature or rating the risk carries. Ensuring accurate and adequate records enables effective breach management, risk analysis and compliance with our regulatory and legal obligations; as well as being able to provide such evidence to supervising authorities or bodies on request.

20.11 Section Responsibilities

The Council will ensure that all staff are provided with the time, resources and support to learn, understand and implement all Risk Assessment and Management documents and related procedures and that departmental managers are supported in completing the Risk Assessment Register.

Where the risk involves personal data; the Data Protection Officer is consulted and involved in all decisions and mitigating actions, including making the decision as to whether a risk should be escalated to the Data Protection Impact Assessment screening question stage.

20.11.1 Associated Documents with this section

The Council has a robust and defined document control system with sections, policies, controls, procedures and measures for all business, contractual, legal, statutory and regulatory requirements. Some sections / policies overlap in other function or activity areas, with the below documents needing to be read and used in conjunction with our Risk Management section: -

- Data Protection
    - Privacy by Design
    - Security of Processing
- Data Protection Impact Assessment (DPIA)
- Breach Management & Incident Reporting
- Information Security
- Access Control
- Audit & Monitoring
- Business Continuity Plan

21 Data Breach

21.1 Section Statement

The Council are committed to our obligations under the regulatory system and in accordance with the GDPR and maintain a robust and structured program for compliance and monitoring. We carry out frequent risk assessments and gap analysis reports to ensure that our compliance processes, functions and procedures are fit for purpose and that mitigating actions are in place where necessary. However, we recognise that breaches can occur, hence this policy states our intent and objectives for dealing with such incidents.

Although we understand that not all risks can be mitigated, we operate a robust and structured system of controls, measures and processes to help protect data subjects and their personal information from any risks associated with processing data. The protection and security of the personal data that we process is of paramount importance to us and we have developed data specific protocols for any breaches relating to the GDPR and the data protection laws.

21.2 Section Purpose

The purpose of this section is to provide the Council's intent, objectives and procedures regarding data breaches involving personal information. As we have obligations under the GDPR, we also have a requirement to ensure that adequate procedures, controls and measures are in place and are disseminated to all employees; ensuring that they are aware of the protocols and reporting lines for data breaches. This policy details our processes for reporting, communicating and investigating such breaches and incidents.

21.3 Data Security & Breach Requirements

The Council's definition of a personal data breach is any incident of security, lack of controls, system or human failure, error or issue that leads to, or results in, the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Alongside our *'Privacy be Design'* approach to protecting data, we also have a legal, regulatory and business obligation to ensure that personal information is protected whilst being processed by the Council. Our technical and organisational measures are detailed in our Data Protection Policy & Procedures and Information Security Policies.

We carry out information audits to ensure that all personal data processed by us is adequately and accurately identified, assessed, classified and recorded. We carry out risk assessments that assess the scope and impact of any potential data breach; both on the processing activity and the data subject. We have implemented adequate, effective and appropriate technical and organisational measures to ensure a level of security appropriate to the risks, including *(but not limited to*): -

- Pseudonymisation and encryption of personal data
- Restricted access and biometric measures
- Reviewing, auditing and improvement plans for the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Disaster Recovery and Business Continuity Plan to ensure up-to-date and secure backups and the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Audit procedures and stress testing on a regularly basis to test, assess, review and evaluate the effectiveness of all measures in compliance with the data protection regulations
- Frequent and ongoing data protection training programs for all employees
- Staff assessments and regular knowledge testing to ensure a high level of

competency, knowledge and understanding of the data protection regulations and the measures we have in place to protect personal information

- Reviewing internal processes to ensure that where personal information is transferred, disclosed, shared or is due for disposal; it is rechecked and authorised by the Data Protection Officer

21.3.1 OBJECTIVES

- To adhere to the GDPR and UK Data Protection Act 2018 and to have robust and adequate procedures and controls in place for identifying, investigating, reporting and recording any data breaches
- To develop and implement adequate, effective and appropriate technical and organisational measures to ensure a high level of security with regards to personal information
- To utilise information audits and risk assessments for mapping data and to reduce the risk of breaches
- To have adequate and effective risk management procedures for assessing any risks presented by processing personal information
- To ensure that any data breaches are reported to the correct regulatory bodies within the timeframes set out in any regulations, codes of practice or handbooks
- To use breach investigations and logs to assess the root cause of any breaches and to implement a full review to prevent further incidents from occurring
- To use the Data Breach Incident Form for all data breaches, regardless of severity so that any patterns in causes can be identified and corrected
- To protect consumers, clients and employees, including their information and identity
- To ensure that where applicable, the Data Protection Officer is involved in and notified about all data breaches and risk issues
- To ensure that the Supervisory Authority is notified of any data breach (*where applicable*) with immediate effect and at the latest, within 72 hours of the Council having become aware of the breach

21.4 DATA BREACH PROCEDURES & GUIDELINES

The Council has robust objectives and controls in place for preventing data breaches and for managing them in the rare event that they do occur. Our procedures and guidelines for identifying, investigating and notification of breaches are detailed below. Our documented breach incident policy aims to

mitigate the impact of any data breaches and to ensure that the correct notifications are made.

21.4.1 BREACH MONITORING & REPORTING

The Council has appointed a Data Protection Officer who is responsible for the review and investigation of any data breach involving personal information, regardless of the severity, impact or containment. All data breaches are reported to this person with immediate effect, whereby the procedures detailed in this policy are followed.

All data breaches will be investigated, even in instances where notifications and reporting are not required, and we retain a full record of all data breaches to ensure that gap and pattern analysis are available and used. Where a system or process failure has given rise to a data breach, revision to any such process is recorded in the Change Management and Document Control records.

21.4.2 BREACH INCIDENT PROCEDURES

21.4.2.1 Identification of an Incident

As soon as a data breach has been identified, it is reported to the direct line manager and the Data Protection Officer immediately so that breach procedures can be initiated and followed without delay.

Reporting incidents in full and with immediate effect is essential to the compliant functioning of the Council and is not about apportioning blame. These procedures are for the protection of the Council, its staff, customers, clients and third parties and are of the utmost importance for legal regulatory compliance.

As soon as an incident has been reported, measures must be taken to contain the breach. Such measures are not in the scope of this document due to the vast nature of breaches and the variety of measures to be taken; however, the aim of any such measures should be to stop any further risk/breach to the organisation, customer, client, third-party, system or data prior to investigation and reporting. The measures taken are noted on the incident form in all cases.

21.4.2.2 Breach Recording

The Council utilises a Breach Incident Form for all incidents, which is completed for any data breach, regardless of severity or outcome. Completed forms are logged in the Breach Incident Folder *(electronic or hard copy)* and reviewed against existing records to ascertain patterns or reoccurrences.

In cases of data breaches, the Data Protection Officer is responsible for carrying out a full investigation, appointing the relevant staff to contain the breach, recording the incident on the breach form and making any relevant and legal

notifications. The completing of the Breach Incident Form is only to be actioned after containment has been achieved.

A full investigation is conducted and recorded on the incident form, with the outcome being communicated to all staff involved in the breach, in addition to senior management. A copy of the completed incident form is filed for audit and documentation purposes.

If applicable, the Supervisory Authority and the data subject(s) are notified in accordance with the GDPR requirements (*refer to item 5 of this section*). The Supervisory Authority protocols are to be followed and their '***Security Breach Notification Form'*** should be completed and submitted. In addition, any individual whose data or personal information has been compromised is notified if required, and kept informed throughout the investigation, with a full report being provided of all outcomes and actions.

21.4.3 BREACH RISK ASSESSMENT

21.4.3.1 Human Error

Where the data breach is the result of human error, an investigation into the root cause is to be conducted and a formal interview with the employee(s) held.

A review of the procedure(s) associated with the breach is conducted and a full risk assessment completed in accordance with the Council's Risk Assessment Procedures. Any identified gaps that are found to have caused/contributed to the breach are revised and risk assessed to mitigate any future occurrence of the same root cause.

Resultant employee outcomes of such an investigation can include, but are not limited to: -

- Re-training in specific/all compliance areas
- Re-assessment of compliance knowledge and understanding
- Suspension from compliance related tasks
- Formal warning *(in-line with the Council's disciplinary procedures)*

21.4.3.2 System Error

Where the data breach is the result of a system error/failure, the IT Service are to work in conjunction with the Data Protection Officer to assess the risk and investigate the root cause of the breach. A gap analysis is to be completed on the system/s involved and a full review and report to be added to the Breach Incident Form.

Any identified gaps that are found to have caused/contributed to the breach are to be revised and risk assessed to mitigate and prevent any future occurrence of the same root cause. Full details of the incident should be determined and mitigating action such as the following should be taken to limit the impact of the incident: -

- Attempting to recover any lost equipment or personal information
- Shutting down an IT system
- Removing an employee from their tasks
- The use of back-ups to restore lost, damaged or stolen information
- Making the building secure
- If the incident involves any entry codes or passwords, then these codes must be changed immediately, and members of staff informed

21.4.3.3 Assessment of Risk and Investigation

The Data Protection Officer should ascertain what information was involved in the data breach and what subsequent steps are required to remedy the situation and mitigate any further breaches.

The lead investigator should look at: -

- The type of information involved
- It's sensitivity or personal content
- What protections are in place (e.*g. encryption*)?
- What happened to the information/Where is it now?
- Whether there are any wider consequences/implications to the incident

The appointed lead should keep an ongoing log and clear report detailing the nature of the incident, steps taken to preserve any evidence, notes of any interviews or statements, the assessment of risk/investigation and any recommendations for future work/actions.

21.5 Breach Notifications

The Council recognises our obligation and duty to report data breaches in certain instances. All users have been made aware of the Council's responsibilities and we have developed strict internal reporting lines to ensure that data breaches falling within the notification criteria are identified and reported without delay.

21.5.1 SUPERVISORY AUTHORITY NOTIFICATION

The Supervisory Authority is to be notified of any breach where it is likely to result in a risk to the rights and freedoms of individuals. These are situations which if the breach was ignored, would lead to significant detrimental effects on the individual.

Where applicable, the Supervisory Authority is notified of the breach no later than 72 hours after the Council becoming aware of it and are kept notified throughout any breach investigation, being provided with a full report, including outcomes and mitigating actions as soon as possible, and always within any specified timeframes.

If for any reason it is not possible to notify the Supervisory Authority of the breach within 72 hours, the notification will be made as soon as is feasible, accompanied by reasons for any delay. Where a breach is assessed by the DPO and deemed to be ***unlikely*** to result in a risk to the rights and freedoms of natural persons, we reserve the right not to inform the Supervisory Authority in accordance with Article 33 of the GDPR.

The notification to the Supervisory Authority will contain: -

- A description of the nature of the personal data breach
- The categories and approximate number of data subjects affected
- The categories and approximate number of personal data records concerned
- The name and contact details of our Data Protection Officer and/or any other relevant point of contact (*for obtaining further information)*
- A description of the likely consequences of the personal data breach
- A description of the measures taken or proposed to be taken to address the personal data breach *(including measures to mitigate its possible adverse effects)*

Breach incident procedures are always followed, and an investigation carried out, regardless of our notification obligations and outcomes, with reports being retained and made available to the Supervisory Authority if requested.

Where the Council acts in the capacity of a processor, we will ensure that controller is notified of the breach without undue delay. In instances where we act in the capacity of a controller using an external processor, we have a written agreement in place to state that the processor is obligated to notify us without delay after becoming aware of a personal data breach.

21.5.2 Data Subject Notification

When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, we will always communicate the personal data breach to the data subject without undue delay, in a written, clear and legible format.

The notification to the Data Subject shall include: -

- The nature of the personal data breach
- The name and contact details of our Data Protection Officer and/or any other relevant point of contact (*for obtaining further information)*
- A description of the likely consequences of the personal data breach
- A description of the measures taken or proposed to be taken to address the personal data breach *(including measures to mitigate its possible adverse effects)*

We reserve the right not to inform the data subject of any personal data breach where we have implemented the appropriate technical and organisational measures which render the data unintelligible to any person who is not authorised to access it *(i.e. encryption, data masking etc*) or where we have taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise.

If informing the data subject of the breach involves disproportionate effort, we reserve the right to instead make a public communication whereby the data subject(s) are informed in an equally effective manner.

21.6 Record Keeping

All records and notes taking during the identification, assessment and investigation of the data breach are recorded and authorised by the Data Protection Officer and are retained for a period of 6 years from the date of the incident. Incident forms are to be reviewed monthly to assess for patterns or breach reoccurrences and actions taken to prevent further incidents from occurring.

21.7 Responsibilities

The Council will ensure that all staff are provided with the time, resources and support to learn, understand and implement all procedures within this document, as well as understanding their responsibilities and the breach incident reporting lines.

The Data Protection Officer is responsible for regular compliance audits and gap analysis monitoring and the subsequent reviews and action follow ups. There is a continuous audit trail of all compliance reviews and procedural amendments and feedback to ensure continuity through each process and task.

22 Clear Desk Policy

23 Section Statement

As a council obligated under the Data Protection laws as well as having legal and contractual responsibilities for information security, Newquay Town Council protects and secures all forms of personal data pertaining to natural and legal persons.

It is the Council's policy to operate a clear desk approach with regards to paper and confidential materials and users are aware that they should never leave personal or sensitive information on their desks or in any area that it may be seen or access by an unauthorised person.

23.1 Section Purpose

The purpose of this section is to ensure that users are aware of the reasons for operating a clear desk environment and to protect any personal information held or processed by the Council. The Council occasionally has external visitors to its offices, such as clients, suppliers and regulators and it is therefore important to prevent personal or confidential information from lying around unattended.

We also adhere to our Environmental Policy which restricts the printing of materials to only those that are necessary. Having a clear desk provides a professional outlook and helps to maintain a safe environment for our employees, buy reducing clutter and preventing accidents

We are committed to the protection of personal information, including that of customers, clients and employees and as such utilise electronic systems for data reading and access where possible. Due to the nature of Council's duties, it necessary for the Council to retain some sensitive information and a large amount of personal information relating to customers. Our Data Protection Policy provide exact controls and measures for securing this type of information.

23.2 Section Objectives

The Council is committed to ensuring compliance with the rules, standards and regulations as laid out by its regulating and governing bodies and our own council objectives. Having a Clear Desk Policy enables is to maintain efficiency

and an effective workplace and secures the personal information that we must hold owing to the nature of our business. As a council, we have a full understanding of the requirements to protect personal information and we believe that having a clear desk environment is pivotal to this end.

The Council's objectives regarding clear desks are to: -

- Improve information security and the protection of personal data
- Abide by GDPR requirements and Principles
- Ensure that personal and/or confidential information is locked away where there is a requirement to print it or where it has been received in a paper format
- Redact paper information as far as possible when it pertains to personal information that exceeds our requirements and needs
- Demonstrate an effective and efficient workplace to visitors, clients and regulators
- Protect employee information and employee rights
- Prevent accidents resulting from clutter and an untidy workplace
- Create a stress-free, clean and tidy environment for our employees
- Reduce paper use and recycle where possible
- Reduce the use of toner inks for the printer
- Reduce the storage space for paper information and archiving resources

23.3 Measures and Controls

Users are continuously reminded that personal information should not be printed unless necessary, however, due to the nature of the Council's business and services, paper formats of confidential information are received on occasion. In such instances, where they are required to be on a desk for any duration of time (*i.e. for administration or data entry purposes*), we can provide secured, locked A4 boxes that paper can be stored in should the user be away from their desk. Users are aware that clear desks are always in operation and when leaving the office for any period of time, paper information is either locked away or destroyed.

At the end of the working day, all users are expected to tidy their desk and to tidy away all office papers into locked desk drawers and filing cabinets. The line manager should also do an office walk round to ensure that paper data has been locked away or destroyed before leaving the office. We have a ***Retention &***

***Erasure* Policy** that outlines how paper information is destroyed and records our retention periods for all information.

It is not just personal information relating to customer or employees that are bound by the clear desk approach. All paper formats, including those used to write information down can be considered private or personal information and are subject to the same policy governance rules. Such documents can include, ***but are not limited to: -***

- Telephone notes
- Printed emails
- Notices and minutes of meetings
- Disciplinary letters
- References
- Accounting paperwork
- Draft letters
- Report and Management Information
- Polices & Procedures
- Corrective Action Plans
- Registers and Visitor Sign-in Books
- Publications
- Manuals
- Training Handbooks

23.3.1 SECTION GUIDELINES

Users are provided with guidelines for keeping their workspace and office clean, tidy and paper free. They understand their obligations under the data protection law and do not keep personal information for longer than is necessary. The Council uses in house shredding facilities and confidential shredding bags where paper information is no longer required. Paper waiting to be shredded is secured in a locked cabinet until destruction.

Users should be afforded regular timeslots to clear their desks of unnecessary clutter such as old diaries, notebooks and filing paperwork that is no longer needed and are each provided with secure A4 lock boxes for securing personal information in paper formats that must be retained on their desk for any period or whilst they are absent from the office.

23.4 Section Responsibilities

The Council will ensure that all users are provided with the time, training and support to learn, understand and implement the Clear Desk Policy and subsequent or associated procedures. Management are responsible for a top down approach and in ensuring that all staff are included and have the support needed to meet the regulatory requirements in this area.

24 Secure Disposal

24.1 Section Statement

Newquay Town Council confirms that it is committed to the secure and safe disposal of any confidential waste and information assets in accordance with our contractual and legal obligations and that we do so in an ethical and compliant manner.

We have specific measures for deleting and erasing personal information documented in our Data Retention & Erasure Policy to ensure compliance with the General Data Protection Regulation (GDPR) and UK's Data Protection Act.

24.2 Purpose

The purpose of this document is to provide the Council's statement of intent on how it disposes of secure information and confidential data in accordance with our legal, statutory and regulatory obligations. ***The Council ensures that we have: -***

- a standardised and established approach to handling the disposal of confidential waste and information assets
- procedures in place for the disposal of secure waste, both hard copies and electronic formats and information assets
- a dedicated Retention & Erasure Policy to comply with our data protection obligations
- guidance for staff on dealing with disposal and/or destruction
- controls and measures in place to comply with any regulatory or legal requirements as they relate to disposal and destruction

24.3 Objectives

The Council have put into place numerous principles and processes for handling the disposal of confidential waste material and information assets (*information and physical*), as below. ***The Council ensures that: -***

- We have a standardised and established approach to handling the disposal of confidential waste and information assets
- We have procedures in place for the disposal of secure waste, both hard copies and electronic formats and information assets
- We provide guidance for staff on dealing with disposal and/or destruction
- We have robust controls and measures in place to comply with any regulatory or legal requirements as they relate to disposal and destruction
- Secure waste bins are used for sensitive and/or confidential wastepaper
- Confidential paper is never used a scrap or re-printed onto
- Confidential wastepaper is never placed into the general waste bin or outside disposal receptacle unless it has been securely shredded
- Waste will be stored in accordance with the waste disposal procedures if not collected immediately, that includes being locked away securely if left overnight, or in an unoccupied building
- Physical and IT assets are encrypted and/or reformatted prior to disposal
- The IT Manager must provide authorisation for assets removal and disposal
- Assets are disposed of in accordance with the manufacturer's guidelines
- Assets, equipment and information are disposed of in an authorised, appropriate, legal and environmentally sound manner adhering to appropriate standards or codes of conduct

25 GUIDELINES & PROCEDURES

Once a record, document or data has reached its designated retention period date, the designated owner should refer to the retention register for the action to be taken. Not all data or records are expected to be deleted upon expiration; sometimes it is sufficient to anonymise the data in accordance with the GDPR requirements or to archive records for a further period.

25.1.1 DESTRUCTION AND DISPOSAL OF RECORDS & DATA

All information of a confidential or sensitive nature on paper, card, microfiche or electronic media must be securely destroyed when it is no longer required. This ensures compliance with the Data Protection laws and the duty of confidentiality we owe to our employees, clients and customers.

The Council is committed to the secure and safe disposal of any confidential waste and information assets in accordance with our contractual and legal obligations and that we do so in an ethical and compliant manner. We confirm that our approach and procedures comply with the laws and provisions made in

the General Data Protection Regulation (GDPR) and that staff are trained and advised accordingly on the procedures and controls in place.

25.1.1.1 Paper Records

Due to the nature of our business, the Council retains paper based personal information and as such, has a duty to ensure that it is disposed of in a secure, confidential and compliant manner. The Council utilise onsite shredding to dispose of all paper materials.

Shredding machines and confidential waste sacks are made available throughout the building and where we use a service provider for large disposals, regular collections take place to ensure that confidential data is disposed of appropriately.

25.1.1.2 Electronic & IT Records and Systems

The Council uses numerous systems, computers and technology equipment in the running of our business. From time to time, such assets must be disposed of and due to the information held on these whilst they are active, this disposal is handled in an ethical and secure manner.

The deletion of electronic records must be organised in conjunction with the IT Service who will ensure the removal of all data from the medium so that it cannot be reconstructed. When records or data files are identified for disposal, their details must be provided to the designated owner to maintain an effective and up to date a register of destroyed records.

Only the IT Service can authorise the disposal of any IT equipment and they must accept and authorise such assets from the department personally. Where possible, information is wiped from the equipment through use of software and formatting, however this can still leave imprints or personal information that is accessible and so we also comply with the secure disposal of all assets.

In all disposal instances, the IT Department must complete a disposal form and confirm successful deletion and destruction of each asset. This must also include a valid certificate of disposal from the service provider removing the formatted or shredded asset. Once disposal has occurred, the IT Service is responsible for liaising with the information Asset Owner and updating the Information Asset Register for the asset that has been removed.

It is the explicit responsibility of the asset owner and IT Service to ensure that all relevant data has been sufficiently removed from the IT device and backed up before requesting disposal and/or prior to the scheduled pickup.

25.1.1.3 Disposing of Removable Media Devices

When the Council no longer has use for any removable media devices or where they are no longer functioning due to damage or corruption, they are securely disposed of to protect any remaining information and prevent data leakage or unauthorised access. All types of removable media are given to the IT Service Manager for disposal and no employee is permitted to carry out this process themselves.

The IT Service Manger formats all media types and ensures that information and materials have been fully removed from the device prior to disposal. However, as technology advances, the Council are aware that methods exist to retrieve partial data or imprints from removable media and as such, secure disposal methods are still used as well as encryption techniques. The IT Service Manager has access to specialist software and tools for the erasure, formatting and disposal of removable media types or where this is not possible, the Council employs a professional service provider to carry out this task.

25.2 Responsibilities

The Council will ensure that all staff are provided with the time, training and support to learn, understand and implement this Secure Disposal Policy and subsequent procedures. Management are responsible for a top down approach and in ensuring that all staff are included and have the support needed to meet the regulatory requirements in this area.

26 Data Retention & Erasure

26.1 Section Statement

The Council recognises that the efficient management of its data and records is necessary to support its core business functions, to comply with its legal, statutory and regulatory obligations, to ensure the protection of personal information and to enable the effective management of the organisation.

This policy and related documents meet the standards and expectations set out by contractual and legal requirements and has been developed to meet the best practices of business records management, with the aim of ensuring a structured approach to document control.

Effective and adequate records and data management is necessary to: -

- Ensure that the business conducts itself in a structured, efficient and accountable manner

- Ensure that the business realises best value through improvements in the quality and flow of information and greater coordination of records and storage systems
- Support core business functions and provide evidence of conduct and the appropriate maintenance of systems, tools, resources and processes
- Meet legislative, statutory and regulatory requirements
- Deliver services to, and protect the interests of, employees, clients and Councillors in a consistent and equitable manner
- Assist in document policy formation and managerial decision making
- Provide continuity in the event of a disaster or security breach
- Protection personal information and data subject rights
- Avoid inaccurate or misleading data and minimise risks to personal information
- Erase data in accordance with the legislative and regulatory requirements

Information held for longer than is necessary carries additional risk and cost and can breach data protection rules and principles. The Council only ever retains records and information for legitimate or legal business reasons and always comply fully with the data protection laws, guidance and best practice.

26.2 Purpose

The purpose of this document is to provide the Council's statement of intent on how it provides a structured and compliant data and records management system. We define ***'records'*** as all documents, regardless of the format, which facilitate business activities, and are thereafter retained to provide evidence of transactions and functions.

Such records may be created, received or maintained in hard copy or in an electronic format with the overall definition of records management being a field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use, distribution, storage and disposal of records.

26.3 Personal Information and Data Protection

The Council needs to collect personal information about the people we employ, work with have a business relationship with, to effectively and compliantly carry out our everyday business functions and activities, and to provide the products and services defined by our business type. This information can include *(but is not limited to),* name, address, email address, data of birth, IP address,

identification number, private and confidential information, sensitive information and bank details.

In addition, we may occasionally be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however we are committed to collecting, processing, storing and destroying all information in accordance with the ***General Data Protection Regulation (GDPR)***, the ***Data Protection Act 2018 (DPA18)*** and any other associated legal or regulatory body rules or codes of conduct that apply to our business and/or the information we process and store.

Our Data Retention Policy and processes comply fully with the GDPR's fifth Article 5 principle: -

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ***('storage limitation').***

26.4 OBJECTIVES

A record is information, regardless of media, created, received, and maintained which evidences the development of, and compliance with, regulatory requirements, business practices, legal policies, financial transactions, administrative activities, business decisions or agreed actions. It is the Council's objective to implement the necessary records management procedures and systems which assess and manage the following processes: -

- The creation and capture of records
- Compliance with legal, regulatory and contractual requirements
- The storage of records
- The protection of record integrity and authenticity
- The use of records and the information contained therein
- The security of records
- Access to and disposal of records

Records contain information that are a unique and invaluable resource to the Council and are an important operational asset. A systematic approach to the management of our records is essential to protect and preserve the information

contained in them, as well as the individuals such information refers to. Records are also pivotal in the documentation and evidence of all business functions and activities.

The Council's objectives and principles in relation to Data Retention are to: -

- Ensure that the Council conducts itself in an orderly, efficient and accountable manner
- Support core business functions and providing evidence of compliant retention, erasure and destruction
- To develop and maintain an effective and adequate records management program to ensure effective archiving, review and destruction of information
- To only retain personal information for as long as is necessary
- Comply with the relevant data protection regulation, legislation and any contractual obligations
- Ensure the safe and secure disposal of confidential data and information assets
- Ensure that records and documents are retained for the legal, contractual and regulatory period stated in accordance with each bodies rules or terms.
- Ensure that no document is retained for longer than is legally or contractually allowed
- Mitigate against risks or breaches in relation to confidential information

26.5 GUIDELINES & PROCEDURES

The Council manage records efficiently and systematically, in a manner consistent with the GDPR requirements, ISO15489 and regulatory Codes of Practice on Records Management. Records management training is mandatory for all staff as part of the Council's statutory and compliance training programme and this policy is widely disseminated to ensure a standardised approach to data retention and records management.

Records will be created, maintained and retained to provide information about, and evidence of the council's transactions, customers, employment and activities. Retention schedules will govern the period that records will be retained and can be found in the ***Record Retention Periods*** table at the end of this document.

It is our intention to ensure that all records and the information contained therein is: -

- **Accurate** - records are always reviewed to ensure that they are a full and accurate representation of the transactions, activities or practices that they document
- **Accessible** - records are always made available and accessible when required (*with additional security permissions for select staff where applicable to the document content*)
- **Complete** - records have the content, context and structure required to allow the reconstruction of the activities, practices and transactions that they document
- **Compliant** - records always comply with any record keeping legal and regulatory requirements
- **Monitored** – staff, council and system compliance with this Data Retention Policy is regularly monitored to ensure that the objectives and principles are being complied with at all times and that all legal and regulatory requirements are being adhered to.

26.5.1 RETENTION PERIOD PROTOCOLS

All records retained during their specified periods are traceable and retrievable. Any file movement, use or access is tracked and logged, including inter-departmental changes. All council and employee information are retained, stored and destroyed in line with legislative and regulatory guidelines.

For all data and records obtained, used and stored within the Council, we: -

- Carry out periodical reviews of the data retained, checking purpose, continued validity, accuracy and requirement to retain
- Establish periodical reviews of data retained
- Establish and verify retention periods for the data, with special consideration given in the below areas: -
    - the requirements of the Council
    - the type of personal data
    - the purpose of processing
    - lawful basis for processing
    - the categories of data subjects

- Where it is not possible to define a statutory or legal retention period, as per the GDPR requirement, the Council will identify the criteria by which the period can be determined and provide this to the data subject on request and as part of our standard information disclosures and privacy notices
- Have processes in place to ensure that records pending audit, litigation or investigation are not destroyed or altered
- Transfer paper-based records and data to an alternative media format in instances of long retention periods (*with the lifespan of the media and the ability to migrate data where necessary always being considered*)

26.5.2 Designated Owners

All systems and records have designated owners (IAO) throughout their lifecycle to ensure accountability and a tiered approach to data retention and destruction. Owners are assigned based on role, business area and level of access to the data required. The designated owner is recorded on the Retention Register and is fully accessible to all employees. Data and records are never reviewed, removed, accessed or destroyed with the prior authorisation and knowledge of the designated owner.

26.5.3 Document Classification

The Council have detailed Asset Management protocols for identifying, classifying, managing, recording and coordinating the Council's assets (*including information*) to ensure their security and the continued protection of any confidential data they store or give access to. We utilise an ***Information Asset Register (IAR)*** to document and categorise the assets under our remit and carry out regular Information Audits to identify, review and document all flows of data within the Council.

We also carry out regular Information Audits which enable us to identify, categorise and record all personal information obtained, processed and shared by our council in our capacity as a controller and processor and has been compiled on a central register which includes: -

- What personal data we hold
- Where it came from
- Who we share it with
- Legal basis for processing it
- What format(s) is it in
- Who is responsible for it?

- Retention periods
- Access level (*i.e. full, partial, restricted etc*)

Our information audits and registers enable us to assign classifications to all records and data, thus ensuring that we are aware of the purpose, risks, regulations and requirements for all data types.

We utilise 5 main classification types: -

6. **Unclassified** - information not of value and/or retained for a limited period where classification is not required or necessary
7. **Public** - information that is freely obtained from the public and as such, is not classified as being personal or confidential
8. **Internal** - information that is solely for internal use and does not process external information or permit external access
9. **Personal** - information or a system that processes information that belongs to an individual and is classed as personal under the data protection laws
10. **Confidential** - private information or systems that must be secured at the highest level and are afforded access restrictions and high user authentication

The classification is used to decide what access restriction needs to be applied and the level of protection afforded to the record or data. The classification along with the asset type, content and description are then used to assess the risk level associated with the information and mitigating action can then be applied.

26.5.4 Suspension of Record Disposal for Litigation or Claims

If the Council is served with any legal request for records or information, any employee becomes the subject of an audit or investigation or we are notified of the commencement of any litigation against our firm, we will suspend the disposal of any relevant scheduled records until we are able to determine the requirement for any such records as part of a legal requirement.

26.5.5 Storage & Access of Records and Data

Documents are grouped together by category and then in clear date order when stored and/or archived. Documents are always retained in a secure location, with authorised personnel being the only ones to have access. Once the retention period has elapsed, the documents are either reviewed, archived or confidentially destroyed dependant on their purpose, classification and action type.

26.6 Expiration of Retention Period

Once a record or data has reached its designated retention period date, the designated owner should refer to the retention register for the action to be taken. Not all data or records are expected to be deleted upon expiration; sometimes it is sufficient to anonymise the data in accordance with the GDPR requirements or to archive records for a further period.

26.6.1 Destruction and Disposal Of Records & Data

All information of a confidential or sensitive nature on paper, card, microfiche or electronic media must be securely destroyed when it is no longer required. This ensures compliance with the Data Protection laws and the duty of confidentiality we owe to our employees, clients and customers.

The Council is committed to the secure and safe disposal of any confidential waste and information assets in accordance with our contractual and legal obligations and that we do so in an ethical and compliant manner. We confirm that our approach and procedures comply with the laws and provisions made in the General Data Protection Regulation (GDPR) and that staff are trained and advised accordingly on the procedures and controls in place.

26.6.1.1 Paper Records

Due to the nature of our business, the council retains paper based personal information and as such, has a duty to ensure that it is disposed of in a secure, confidential and compliant manner. The Council utilise onsite shredding and have a contract with a professional shredding service provider to dispose of all paper materials.

Shredding machines and confidential waste sacks are made available throughout the building and where we use a service provider for large disposals, regular collections take place to ensure that confidential data is disposed of appropriately.

26.6.1.2 Electronic & IT Records and Systems

The Council uses numerous systems, computers and technology equipment in the running of our business. From time to time, such assets must be disposed of and due to the information held on these whilst they are active, this disposal is handled in an ethical and secure manner.

The deletion of electronic records must be organised in conjunction with the IT Service who will ensure the removal of all data from the medium so that it cannot be reconstructed. When records or data files are identified for disposal, their details must be provided to the designated owner to maintain an effective and up to date a register of destroyed records.

Only the IT Service can authorise the disposal of any IT equipment and they must accept and authorise such assets from the department personally. Where possible, information is wiped from the equipment through use of software and formatting, however this can still leave imprints or personal information that is accessible and so we also comply with the secure disposal of all assets.

In all disposal instances, the IT Service must complete a disposal form and confirm successful deletion and destruction of each asset. This must also include a valid certificate of disposal from the service provider removing the formatted or shredded asset. Once disposal has occurred, the IT Service is responsible for liaising with the information Asset Owner and updating the Information Asset Register for the asset that has been removed.

It is the explicit responsibility of the asset owner and IT Department to ensure that all relevant data has been sufficiently removed from the IT device and backed up before requesting disposal and/or prior to the scheduled pickup.

26.6.1.3 Internal Correspondence and General Memoranda

Unless otherwise stated in this policy or the retention periods register, correspondence and internal memoranda should be retained for the same period as the document to which they pertain or support *(i.e. where a memo pertains to a contract or personal file, the relevant retention period and filing should be observed*).

Where correspondence or memoranda that do not pertain to any documents having already be assigned a retention period, they should be deleted or shredded once the purpose and usefulness of the content ceases or at a maximum, 2 years.

Examples of correspondence and routine memoranda include (but are not limited to): -

- Internal emails
- Meeting notes and agendas
- General inquiries and replies
- Letter, notes or emails of inconsequential subject matter

26.7 ERASURE

In specific circumstances, data subjects' have the right to request that their personal data is erased, however the Council recognise that this is not an absolute *'right to be forgotten'*. Data subjects only have a right to have personal data erased and to prevent processing if one of the *below conditions applies: -*

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data must be erased to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

Where one of the above conditions applies and the Council received a request to erase data, we first ensure that no other legal obligation or legitimate interest applies. If we are confident that the data subject has the right to have their data erased, this is carried out by the Data Protection Officer in conjunction with any department manager and the IT Service to ensure that all data relating to that individual has been erased.

These measures enable us to comply with a data subjects right to erasure, whereby an individual can request the deletion or removal of personal data where there is no compelling reason for its continued processing. Whilst our standard procedures already remove data that is no longer necessary, we still follow a dedicated process for erasure requests to ensure that all rights are complied with and that no data has been retained for longer than is needed.

Where we receive a request to erase and/or remove personal information from a data subject, the below process is followed: -

1. The request is allocated to the Data Protection Officer and recorded on the Erasure Request Register
2. The DPO locates all personal information relating to the data subject and reviews it to see if it is still being processed and is still necessary for the legal basis and purpose it was originally intended
3. The request is reviewed to ensure it complies with one or more of the grounds for erasure: -
    a. the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed
    b. the data subject has withdrawn consent on which the processing is based and where there is no other legal ground for the processing
    c. the data subject objects to the processing and there are no overriding legitimate grounds for the processing

   d. the personal data has been unlawfully processed
   e. the personal data must be erased for compliance with a legal obligation
   f. the personal data has been collected in relation to the offer of information society services to a child
4. If the erasure request complies with one of the above grounds, it is erased within 30 days of the request being received
5. The DPO writes to the data subject and notifies them in writing that the right to erasure has been granted and provides details of the information erased and the date of erasure
6. Where the Council has made any of the personal data public and erasure is granted, we will take every reasonable step and measure to remove public references, links and copies of data and to contact related controllers and/or processors and inform them of the data subjects request to erase such personal data

If for any reason, we are unable to act in response to a request for erasure, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy. ***Such refusals to erase data include: -***

- Exercising the right of freedom of expression and information
- Compliance with a legal obligation for the performance of a task carried out in the public interest
- For reasons of public interest around public health
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing
- For the establishment, exercise or defence of legal claims

26.7.1 SPECIAL CATEGORY DATA

In accordance with GDPR requirements and Schedule 1 Part 4 of The Data Protection Act 2018, organisations are required to have and maintain appropriate policy documents and safeguarding measures for the retention and erasure of special categories of personal data and criminal convictions etc.

Our methods and measures for destroying and erasing data are noted in this policy and apply to all forms of records and personal data, as noted on our retention register schedule.

26.8 Compliance and Monitoring

The Council are committed to ensuring the continued compliance with this policy and any associated legislation and undertake regular audits and monitoring of our records, their management, archiving and retention. Information asset owners are tasked with ensuring the continued compliance and review of records and data within their remit.

26.9 Responsibilities

Heads of services and information asset owners have overall responsibility for the management of records and data generated by their departments' activities, namely to ensure that the records created, received and controlled within the purview of their department, and the systems (*electronic or otherwise*) and procedures they adopt, are managed in a way which meets the aims of this policy.

The DPO must be involved in any data retention processes and records or all archiving and destructions must be retained. Individual employees must ensure that the records for which they are responsible are complete and accurate records of their activities, and that they are maintained and disposed of in accordance with the Council's protocols.

26.10 Retention Periods

Section 12 of this policy contains our regulatory, statutory and business retention periods and the subsequent actions upon reaching those dates. Where no defined or legal period exists for a record, the default standard retention period is 6 years plus the current year (*referred to as 6 years + 1*).

27 E-mail Usage & Archiving

27.1 Section Introduction

Newquay Town Council utilises and makes available corporate email for our employees in the functioning of our business activities but recognise the risks to security and personal data posed by such use. This section outlines our acceptable email usage, restrictions and rules for governing use of email throughout the Council and serves as a guidance document in the correct use and behaviour of users, employees and third parties when accessing and using email.

This section should be read in conjunction with our other information security sections and data protection protocols and measures for a complete approach to securing and protecting personal information.

27.2 Section Statement

The council recognises that email is a necessary and standard way to communicate in business and makes up an essential part of the Council's communication with other users, employees, third parties and our customers.

Like all forms of technology used by the Council, email can pose security or business risks if used or set-up incorrectly or inappropriately. This email policy sets out our approach and expectations for safe and secure use of email throughout the Council and provides guidelines on good email etiquette for those using and accessing email.

27.3 Section Purpose

The purpose of this policy is to provide the Council's statement of intent on how it sets-up, secures, uses and monitors email use within the business. It provides users & employees with their obligations and expectations when using email and helps to reduce the risk associated with corporate email use.

A portion of the information sent and received by email in the Council constitutes personal information and as such, this section should be read in conjunction with our other information security and data protection policies.

27.4 Email Use and Guidelines

The Council has set out guidance for users & employees on how to use email for best practice, acceptable use and any actions deemed unacceptable when using or accessing the Council email.

27.4.1 Acceptable Use

The Council have adopted the below set of acceptable use guidelines for users & employees to follow when using the Council's email: -

- Email must be used in accordance with current legislation and regulations
- Employees must always adhere to this policy when using corporate email
- The Council email should only be accessed outside of the business premises or hours with the explicit authorisation of a manager and the IT Service
- Users & employees must only access their own business email and must not share or disclose logins or passwords

- Users & employees must report any unusual or flagged email messages to the IT Service immediately
- The Council email should only be used for legitimate business use

27.4.2 PROHIBITED USE

In addition to the acceptable use of the Council email system, the below actions and forms of use are unacceptable and must be adhered to by all employees.
The Council email must not be used: -

- To send or receive inappropriate content or attachments, including distributing, disseminating or storing images, text or materials that might be considered indecent, racist, sexist, abusive, offensive, pornographic, obscene or illegal
- For personal use, to disseminate personal views or opinions or to access personal emails
- For sending confidential messages to any unauthorised person or location
- To sign-up to personal, inappropriate or non-business internet sites
- For sending or forwarding *'chain letters'* or social content
- forwarding of council confidential messages to external locations
- To send, receive or access any copyrighted information in a way that violates or breaches that copyright
- To send unsolicited corporate, marketing or advertising material
- In a way that restricts the sending or receive of files by other employees *(i.e. sending large files without pre-authorisation)* or for undertaking deliberate activities that waste any networked resources
- In a way that could introduce any form of computer virus or malware into the Council network

27.4.3 BEST PRACTICE

As email is used so often to communicate with other people, the Council have set out the best email etiquette that should be followed by all employees or third parties using the business email. Appropriate use of the email system and message structure is essential to the Council's reputation and for best practice when contacting customers or other entities.

The Council suggests that when using corporate email, Users & employees should: -

- Ensure that the *'to'* field is correctly populated before sending the email
- Not use the email system for sending personal employee content, discussions or opinions such as jokes, outside work events etc

- Always ensure that the *'Subject'* line is meaningful and appropriate
- Keep the email content brief and to the point – do not clog other employees email system up with length emails if a meeting or phone call would serve better
- Only use the 'flag' or 'urgent' options when the message is urgent or needs a time sensitive response
- Not add a *'read receipt'* request onto email as they can become overwhelming when someone receives a lot of email and some servers do not support them
- Do not type in all 'CAPS' to get a message across or in the subject lines as in email terms it is seem as shouting and is not polite

27.5 Personal Email

The Council understands that email forms a large part of individuals daily life and is an integral communication tool used by most people. As such, we allow the accessing of personal email, with the below stipulations: -

- Personal email can only be used or accessed on personal devices such as smartphones and must never be accessed via corporate computers or devices
- Use and access to personal email is restricted to non-working periods such a prior to, and after work and lunch, break times
- Employees must never use personal email to send or receive material or information relating to or owned by the Council or for business purposes
- Personal email must never be used to send or receive inappropriate content, whether for personal or business purposes

27.6 Email Security

The IT Service are responsible for ensuring that the network and email system is adequately protected from viruses and malware. However, employees and users can also help in avoiding security issues by complying with the below responsibilities. ***Users of the email system must not: -***

- Send or open any attachment that is not recognised, authorised or has come from an unknown source
- Disable or change any of the security settings applied by default to the Council email system and network
- Alter any of the security settings on the device being used to access the email system
- Submit any personal devices being used to access the Council email system to the IT Service for security software installation and checks
- Send any personal or confidential information by standard software. Speak to the IT Service who will advise on the correct secure transfer tool or system for the file type

- Disclose your email login or password or attempt to access another user's email system
- Leave email systems open, unattended and unlocked when leaving a desk or the room

27.7 Email Archiving & Retention

Under the ***General Data Protection Regulation (GDPR),*** all personal data, including that stored as a message or in an email system is subject to the GDPR's data minimisation and storage limitation principles, which the Council strictly adheres to.

Our general retention periods and destruction and archiving methods are detailed in our Retention & Erasure Policy, to which all emails and archives messages are subject. To ensure that the Council is prepared for a compliant with the new data protection legislation, ***we have: -***

- Reviewed this email policy to ensure that security and confidentiality are paramount when accessing, sending and receiving messages containing personal information
- Assessed our existing archived message and email database for all devices, documenting any messages or attachments relating to personal information
- Utilised our Information Audit to identify the legal basis for storing or processing personal information emails and applying our retention and destruction processes to any that are no longer required or where we do not have a legal obligation to retain the message
- Created parameters for filtering, categorising and the destruction of emails that we are not obligated or lawfully allowed to retain

Emails that we have a lawful obligation or basis to retain are archived and become the responsibility of the IT Service / Data Protection Officer for review on retention periods and setting accurate destruction dates.

Where any email contains personal information in the form of an attachment (*i.e. medical invoices, passports copies, birth certificates etc),* these attachments are removed from the email and stored in accordance with our personal information protocols as detailed in our data protection and information security policies.

27.8 Monitoring Email

The email system and software are provided to users & employees and relevant third parties for legitimate business use and as such will always be subject to being monitored . The IT Service can access corporate emails, including sent,

received and archived messages and have the right to remove messages or access to email as they deem appropriate.

In compliance with our legal business obligations, any emails sent or received through the corporate email system form part of our business records and must be retained in accordance with our Retention Periods schedule.

27.9 Section Responsibilities

All email users within the Council are responsible for adhering to this policy and for the correct and proper use of email and ensuring the security of the information sent and received. Where any user has or is believed to have breached the standards or requirements set out in this policy, they may face disciplinary action.

The disciplinary penalty will be proportionate to the level of misuse of email but can range from a verbal warning through to dismissal, dependant on the factors involved in the policy breach. Knowingly using email in a manner that does not comply with legal obligations or this policy is a serious matter and the Council will monitor and review all email use to ensure the correct procedures are being followed and adhered to.

28 Artificial Intelligence in the Workplace

28.1 Section Introduction

AI systems, including Large Language Models (LLMs), can now be utilised by staff. This policy defines appropriate use cases.

A clear distinction is made between creating new Generative AI systems, which is strongly discouraged and requires approval from the Data Protection Officer due to potential unforeseen consequences, and using readily available proprietary LLMs, which is permissible for streamlining workflows and administrative tasks.

The following section outlines reasonable use guidelines for staff leveraging LLMs.

28.2 Acceptable Use

Council staff often face high workloads with administrative tasks comprising a significant portion of their responsibilities. Large Language Models (LLMs) can alleviate some of this burden by assisting with day-to-day tasks.

LLMs excel at reducing duplicative work by creating templates for and aiding in the drafting of common documents such as business cases, proposals, reports, communications, policies, agendas, and more. Additionally, they can summarise lengthy documents, research topics, and provide concise overviews to expedite information gathering.

Moreover, LLMs can facilitate procurement processes by reviewing bids, conducting supplier research, and comparing offerings. They can also assist in drafting requests for proposals (RFPs), evaluating responses, and providing insights to support decision-making.

LLMs can help streamline meeting preparation by suggesting relevant agenda items, generating meeting minutes, and drafting follow-up actions and correspondence based on discussions.

Furthermore, LLMs can support staff in drafting and editing public-facing communications, such as newsletters, website content, social media posts, and press releases, ensuring clarity and consistency in messaging.

It is important to note that while LLMs can significantly enhance productivity, their outputs should be carefully reviewed and fact-checked, as they may occasionally produce inaccurate or biased information, especially when dealing with sensitive or confidential topics.

28.3 Unacceptable Use & Potential Risks

Privacy and Data Protection: LLMs should not be used to process or generate content containing personal or sensitive information of individuals, as this could lead to privacy violations and breaches of data protection regulations.

Biased or Discriminatory Content: LLMs may perpetuate societal biases present in their training data. Outputs should be carefully reviewed and edited to ensure they do not contain discriminatory language or viewpoints based on race, gender, age, or other protected characteristics.

Misinformation and Inaccuracies: LLMs can generate convincing but false information (hallucinations). Their outputs should not be treated as authoritative sources, especially for critical decisions or public-facing communications without thorough fact-checking and verification.

Misuse of Public Data: LLMs should not be used to generate content that could reveal confidential or sensitive public data, such as details about ongoing legal cases, law enforcement investigations, or unreleased policy decisions.

Automated Decision-Making: LLMs should not be used for high-stakes decision-making processes, such as determining eligibility for services or benefits, without human oversight and the ability to explain the rationale behind the decisions.

28.4 Mitigating Risk & Promoting Responsible Use

28.4.1 Mitigation

Human Oversight and Review: LLM outputs should always be carefully reviewed and edited by human staff to ensure accuracy, appropriateness, and alignment with the Council's values and objectives.

Fact-Checking and Verification: Information generated by LLMs should be cross-checked against authoritative sources and verified for accuracy before being used or disseminated.

Bias Monitoring and Correction: Outputs should be regularly monitored for potential biases, and appropriate measures should be taken to correct or mitigate any identified issues.

Training and Guidance: Staff should receive proper training on the responsible use of LLMs, including best practices for prompt engineering, output evaluation, and ethical considerations.

Transparency and Accountability: Clear policies and procedures should be established to ensure transparency and accountability in the use of LLMs, including logging and auditing of their interactions and outputs.

By implementing these mitigation strategies and adhering to strict guidelines, the Council can harness the benefits of LLMs while minimizing potential risks and ensuring responsible and ethical use within the workplace.

28.4.2 Prompt Engineering Best Practice

The quality and accuracy of LLM outputs heavily rely on the prompts provided. Staff should follow these best practices when using LLMs:

- Clearly define the task or desired output in the prompt, using specific and unambiguous language.
- Provide relevant context or background information to guide the LLM's understanding of the topic.
- Specify any constraints or requirements, such as output length, formatting, or tone.
- Use examples or illustrations to clarify the desired output style or structure.
- Incorporate instructions to avoid generating harmful, biased, or illegal content.
- Iteratively refine prompts based on the LLM's responses and feedback from human reviewers.
- In the prompt, the inputter could ask the AI to return to the inputter, questions to ensure it understands the prompt fully and the output therefore becomes more accurate.

28.4.3 Intellectual Property and Copyright

The use of LLMs may raise intellectual property and copyright concerns. To mitigate these risks, staff should adhere to the following guidelines:

- Properly attribute any sources used by the LLM in generating content, including direct quotes or paraphrased material.
- Ensure compliance with licensing agreements and terms of use for any data or models used by the LLM.
- Avoid reproducing or distributing copyrighted material without obtaining necessary permissions.
- Exercise caution when using LLM-generated content for commercial purposes or in publicly available materials to prevent potential infringement claims.

28.4.4 Ethical AI Principles

The Council is committed to upholding the highest standards of ethics and responsible AI use. When leveraging LLMs, staff should adhere to the following ethical principles:

- Transparency: Ensure transparency by clearly communicating when content has been generated or assisted by an LLM, and provide appropriate context or disclaimers.
- Accountability: Maintain human accountability and oversight for all decisions and actions informed by LLM outputs, without abdicating responsibility to the AI system.

- Fairness and Non-Discrimination: Monitor LLM outputs for potential biases or discriminatory language, and take appropriate measures to correct or mitigate these issues.
- Respect for Human Rights: Ensure that the use of LLMs does not infringe upon fundamental human rights, such as privacy, freedom of expression, or due process.
- Beneficence: Prioritize the well-being and best interests of the Council's constituents, ensuring that LLM use does not cause harm or negative impacts.

28.5 Data Access Security in the Context of AI

An AI assistant may be utilised within the organisation's Microsoft tenant environment. However, strict access control measures must be enforced to ensure the AI system cannot inadvertently access or process any confidential or sensitive data. The AI assistant will only be able to interact with data and systems explicitly permitted by its configured access permissions. Robust governance of user/system permissions is critical to mitigate potential data privacy risks associated with AI system interactions.

~~28~~29 ADDITIONAL INFORMATION & RELEVANT CONTACT INFORMATION

Chief Executive & Town Clerk

Newquay Town Council
Municipal Offices
Marcus Hill
Newquay
TR7 1AF

ceo@newquay.gov.uk

01637 878388

Data Protection Officer
Newquay Town Council
Municipal Offices
Marcus Hill
Newquay
TR7 1AF

dpo@newquay.gov.uk

01637 878388

IT Service Manager
Newquay Town Council
Municipal Offices
Marcus Hill
Newquay
TR7 1AF

it@newquay.town

01637 878388