Tamworth Borough Council

Technology & Information Services

DATA PROTECTION POLICY

Document Hierarchy: Tier 1 Policy

Document Status: FINAL

TISMS Document Ref: TISDPP0105

Originator: Data Protection Officer (Information Governance Manager)

Updated: Data Protection Officer (Information Governance Manager)

Owner: Assistant Director People

Version: 01.05

Date: November 2023
Review Date: November 2026

Approved by
Technology & Information Services Management Team
ELT/CMT

Document Location

This document is held by Tamworth Borough Council, and the document owner is Information Governance Manager

Printed documents may be obsolete an electronic copy will be available on Tamworth Borough Councils Intranet. Please check for current version before using.

Revision History

Revision Date	Version Control	Summary of changes
July 2020	01.01	Initial Draft
July 2020	01.02	Draft
September 2020	01.03	Final for approval
March 2023	01.04	Minor changes in respect of: • lead officer details • principle details updated
November 2023	01.05	Review

Key Signatories

Approvals Creation and Major Change

Name	Title	Approved
T&IS MT	Technology & Information Services - Management Team	September 2020
TU	Trade Union	October 2020
CMT	Corporate Management Team	November 2020
CAB	Cabinet	December 2020

Approvals Minor Change and Scheduled Review

Name	Title	Approved
T&IS MT	Technology & Information Services - Management Team	
CMT	Corporate Management Team	

Approval Path

Major Change	**Action**
Originator	T&IS
Owner	Head of T&IS
TULG	Consultative Group
CMT	Corporate Approval

Minor Change	**Action**
T&IS	Submission

T&IS Mgmt Team	Approval

Document Review Plans

This document is subject to a scheduled 3 yearly review, or sooner where legislation or contract changes previse.
Updates shall be made in accordance with business requirements and changes and will be with agreement with the document owner.

Distribution

The document will be distributed through Astute as a **MANDATORY** policy where applicable and will also be available on the Intranet.

Security Classification

This document is classified as Official

CONTENTS PAGE

Contents

Policy on a Page

You **must** comply with the whole policy, but in summary:

- The Council will adhere to the Data Protection Principles and promote good practice in respect of obtaining, using and holding personal data.

- The Council will only disclose personal data in-line with its statutory responsibilities to undertake its functions/services for employees and service users. No voluntary release of data will be undertaken beyond the normal business requirements. In exceptional emergency circumstances data will be released where it is deemed appropriate.

- The Council will hold minimum personal data necessary to enable it to perform its functions. Every effort will be made to ensure that information is accurate and up to date and that inaccuracies are corrected without unnecessary delay. Only matters of fact will be recorded and which can be substantiated at a later date. Any opinions expressed will be based on reliable information and in a professional manner.

- The Council will retain personal data only far as long as is necessary in order to comply with legal, statutory or legitimate business function purposes. It will be the responsibility of each Assistant Director or Head of Service to inform the Corporate Management Team of this retention period for each class of data under their control and to arrange, in conjunction with Information Services, secure destruction of expired data.

- The Council will respond to and assist every request for access to personal data from those subject to the personal data processed about them. In most circumstances a fee cannot be charged, but the Council may charge for access to personal data where permitted by the UK -GDPR and DPA 2018 provisions.

- Personal data will be kept in an appropriately controlled and secure environment.

- Data Sharing/Data Use with external organisations will be the subject of a written agreement covering the scope of data to be used, controls to protect personal data and where necessary the reasons permitting the sharing/use of the data.

The Council will ensure all employees, elected Members and temporary/contract staff receives the appropriate training/guidance regarding their individual responsibilities under the UK-GDPR and DPA's provisions.

Any member of staff knowingly or recklessly breaching the Council's Data Protection Policy will be subject to the internal disciplinary procedure. Matters relating to Elected Member non-compliance will be reported the Standards Committee for review.

1 Introduction

This Data Protection Policy provides a framework within which Tamworth Borough Council will strive to ensure compliance with the requirements of the Data Protection Act 2018 (DPA 2018) and any other related legisaltion, and will underpin any operational procedures and activities connected with the implementation the DPA 2018.

As part of the authority's obligations and duties relating to the reporting of Data Breaches, Tamworth Borough Council is obliged to protect data using all means necessary, ensuring that any incident which could cause damage to the Councils reputation and assets is prevented and/or reduced.

Tamworth Borough Council collects and uses different types of information about people with whom it deals and communicates with in order to operate, including information on current, past and prospective employees, suppliers, clients, customers, and service users. In addition the Council is required by law to collect and use certain types of information to fulfil its statutory duties and also to comply with the legislative requirements. This personal information must be dealt with properly whether it is collected, recorded and used on paper, computer or other material.

The Council is committed to ensuring that personal information is handled in a secure and confidential manner in accordance with its Data Protection obligations.

This policy outlines Tamworth Borough Councils approach to Data Protection, and its best practice approach to Data Breach reporting. In additon there are a number of supporting policies that must be read in conjunction with this policy, these being;

- Information Security Policy
- Data Breach Notification Policy
- Data Protection Impact Assessment - Policy (and procedure)
- Records Management Policy
- Retention Schedule

This is not an exhaustive list and maybe subject to change.

2 Overview of Data Protection Act 2018

The Data Protection Act 2018 is the UK's implementation of the UK General Data Protection Regulation (GDPR).

The Data Protection Act 2018 governs the handling of personal information that identifies living individuals directly or indirectly and covers both manual and computerised information. It provides a mechanism by which individuals (data subjects) can have a certain amount of control over their personal data and the way in which it is handled.

Some of the main features of the Act are:

1. All data covered by the Act must be handled in accordance with the seven principles
2. The Data Subject has various rights under the Act including the right to be informed about what personal data is being processed.
3. Processing of data, including special categories of data, must be done under a lawful basis
4. The Data Protection Act 2018 deals with criminal offence data in a similar way to special category data and sets out specific conditions providing lawful authority for processing it.
5. There is a principle of accountability of data controllers to implement appropriate technical and organisational measures that include internal data protection policies, staff training and awareness of the requirements of the Act, internal audits of processing activities, maintaining relevant documentation on processing activities, appointing a data protection officer, and implementing measures that meet the principles of data protection by design and data. Protection by default, including data minimisation, transparency, and creating and improving security features on an on-going basis.
6. Data protection impact assessments (DPIA's) are carried out as part of the design and planning of projects, systems and programmes.
7. Data controllers must have written contracts in place with all data processors and ensure that processors are only appointed if they can provide 'sufficient guarantees 'that the requirements of the Act will be met and the rights of data subjects protected.
8. Data breaches that are likely to result in a risk to the rights and freedoms of individuals must be reported to the Information Commissioner's Office within 72 hours of the Council becoming aware of the breach. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the council will notify those individuals concerned directly.

The Information Commissioner is responsible for regulation and issue notices to organisations where they are not complying with the requirements of the Act. The Information Commissioner can prosecute those who commit offences under the Act and to issue fines.

3 Scope

The Policy applies to all employees and Elected Members of the organisation, both permanent and temporary. It also applies to contractors, partners and visitors who are engaged to work with, or have access to, council information.

This policy applies to all personal data held by Tamworth Borough Council and covers all formats, including but not exclusive to: electronic, paper, magnetic, digital and video.

Some of the responsibilities within this policy extend to employees of the Council beyond their period of employment or to Elected Members beyond their period of office. This paragraph refers specifically to their continued responsibility to keep secure and not publicly disclose the personal data of any third party (particularly any sensitive personal information) to which they may have had privileged access by virtue of their period of employment or office.

4 Definitions

Under UK General Data Protection Regulations (UK-GDPR) and Data Protection Act 2018 (DPA 2018), certain words have specific meanings:

Data Controller
This is the organisation or individual(s) who hold and use (process) personal information. Data controllers are responsible for ensuring that data is processed within the principles of the UK-GDPR. The UK-GDPR places additional emphasis on meeting contractual obligations with the processor to ensure they also comply with UK-GDPR.

Data Processor
Data processor means any organisation or person, other than an employee of the Council, who processes data on behalf of the data controller. For example, someone contracted to the Council to undertake work on its behalf. As a processor, the UK-GDPR requires them to maintain records of all processing activities and personal data use, which increases the legal liability for processors in the event of a breach.

Data Subject
Data subject is the individual about whom personal data is held. Data subjects have certain legal rights in relation to how, if at all, their personal data is processed.

Identifiable Natural Person
An Identifiable Natural Person is anyone 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 one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Anonymisation
Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person.

Personal Data
The UK-GDPR makes a distinction between Personal Data and 'Special Category data. Personal data is any information, which relates to an identified or Identifiable Natural Person. In addition, it includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. The definition of personal data has been expanded to reflect the importance of the online element of many individuals' and includes online identifiers, device identifiers, cookie IDs and IP addresses.

Processing
Processing means obtaining, recording or holding the information or data, or carrying out any operation on the data (whether or not by automated means). This includes organisation, adaptation or alteration, retrieval, disclosure and destruction of the data.

Relevant Filing System
Relevant filing system means any filing system which is structured and refers to identifiable individuals; the information relating to those individuals being readily accessible.

Special Category Data
Special Category data is subject to stricter conditions of processing. The scope of special category data has been expanded to keep up with advances in medical technology, therefore special category data means personal data consisting of information in any of the following categories:

• Genetic data;
• Biometric data;
• Racial or ethnic origin;
• Political opinion;
• Religious or other beliefs;
• Trade union membership;
• Physical or mental health or condition;
• Sexual life;
• Criminal proceedings or convictions.

Information Commissioner (ICO)
The ICO is the supervisory authority for data protection in the UK. They offer advice and guidance, promote good practice, monitor breach reports, conduct audits and advisory visits, consider complaints, monitor compliance and take enforcement action where appropriate.

5 Data Protection Principles

The Data Protection Act defines the key principles we must follow when processing data.

The Information Commissioner who oversees compliance and promotes good practice requires all data controllers and data processors, who process personal information, to be responsible for their processing activities and comply with the seven data protection principles detailed below.

- processed lawfully, fairly and in a transparent manner in relation to individuals **('lawfulness, fairness and transparency')**

- The Council must have lawful authority for processing personal information and the purpose of the processing must be explained to the data subject.

- 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 not be considered to be incompatible with the initial purposes **('purpose limitation')**

    - Processing must fall strictly within the purposes for which the data were obtained. Where the Council is obliged to obtain personal data for a statutory purpose, the data may not be processed for any other statutory purpose unless it directly relates to the original purpose.

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

    - Personal information must be adequate, relevant and limited to only what is needed to get the job done given the purposes for which it is held. Care should be taken to ensure that information is not collected 'just in case' and that files are checked regularly to ensure that unnecessary information is removed.

- 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')**

    - Where it is discovered that information held by the Council is inaccurate, the error must be rectified immediately.

- 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals **('storage limitation')**

    - Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purpose for which it was collected. The Council's Retention Schedule must be applied at all times.

    - Personal data may be stored for longer periods, if it will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR and the DPA 2018 in order to safeguard the rights and freedoms of individuals.

- 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')**

    - This principle protects the integrity and privacy of data by making sure it is secure (which extend to IT systems, paper records and physical security). The Council, when collecting and processing data, is responsible for implementing appropriate security measures that are proportionate to the risks and rights of data subjects. Further information on how the Council works to achieve this is detailed in the Council's Information Security Policy

In additon to the six principles detailed above, there is an overarching princple of accountabilty which means the Authority **MUST** not only comply with the above six princples, they **MUST** be able to demonsrate compliance if inspected by reglatory bodies, such as the ICO.

- The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 **('accountability').**

    - This focuses on compliance and for the Council to be able to demonstrate compliance with the principles.

6 Roles and Responsibilities

Organisational Responsibilities
Tamworth Borough Council is a data controller under the Data Protection Act 2018. The Council as an organisation is responsible for compliance with the Data Protection Act 2018.

Lead Officer
The lead officer for Data Protection is the Assistant Director – People.

Data Protection Officer
The responsibility for incident management is delegated to The Head of Technology and Information Services and the Information Governance Manager.

The responsibility for compliance with the Data Protection Act 2018 is delegated to the Data Protection Officer (DPO).

The Data Protection Officer must be independent, an expert in data protection, adequately resourced, and report to the highest management level (CMT).

The council must provide the Data Protection Officer with the necessary resources and access to personal data and processing operations to enable them to perform the tasks outlined below and to maintain their expert knowledge of data protection law and practice.

The Data Protection Officer for Tamworth Borough Council is the Information Governance Manager, and is responsible for the following tasks:

- To inform and advise the Council and its employees about their obligations to comply with the Data Protection Act 2018 and other data protection laws.
- To monitor compliance with the Data Protection Act 2018 and other data protection laws, including the assignment of responsibilities, raising awareness, and training of staff involved in the processing operations and related audits.
- To provide advice regarding Data Protection Impact Assessments (DPIAs)
- Being the first point of contact for Subject Access Requests, and queries from data subjects
- Working closely with ICT to ensure all systems, services and equipment used for storing personal data meet acceptable security standards and UK-GPDR responsibilities
- Co-operating wherever necessary with the relevant supervisory authority.

The DPO for Tamworth Borough Council will attend the Councils Statutory Officers group on a quarterly basis and reports to the Assistant Director – People for matters pertaining to Data Protection.

CMT
CMT has overall responsibility and accountability for ensuring that all staff and associated third parties comply with data protection legislation, this policy and associated policies and procedures

Heads of Service and Managers
Heads of Service and Managers, as data controllers for their Department and Teams, will retain a service responsibility for ensuring compliance with the provisions of the Data Protection Act 2018. Their main roles will be:

- Monitor compliance within their Service Area/Team
- Monitor compliance by external service providers who are processing personal data
- Ensure their Service Area/Team process and extract data in relation to subject access requests
- Assign ownership to information assets
- Ensure their Service Area/Team complies when there is a suspected data protection breach/incident management breach.

All Employees and Elected Members
Every employee and elected Member must comply with this Policy when using personal data controlled by the Council. All employees and elected Members are individually responsible for ensuring that their collection, storage, processing and destruction of data are in accordance with the Data Protection Act 2018.

All employees should ensure paper files and other records or documents containing personal, confidential and sensitive data are kept in a secure environment. All employees are responsible for being aware of, and complying with, the disposal of confidential waste in the area in which they work. For further information on disposal of confidential waste, please see the Council's Confidential Waste Policy.

Personal data held on computers and computer systems are protected by the use of secure passwords and individual passwords should be such that they are not easily compromised. It is a criminal offence to access personal data held by the Council for other than Council business, or to procure the disclosure of personal data to a third party. It is a further offence to sell such data.

Employees who experience or discover a data loss are responsible for reporting it as soon as possible to the Data Protection Officer. All relevant employees will be responsible for assisting the Data Protection Officer during this investigation. Relevant employees play an important role in providing information about the data which has been lost. Further information is detailed in the Councils Breach Notification Policy.

Contractors/Partners
All contractors, partners and other agents of the Council must ensure that they and their employees who have access to personal data held or processed for or on behalf of the Council are aware of this Policy and are fully trained in and are aware of their duties and responsibilities under the Data Protection legislation.

Ownership of data
Each department is responsible for the personal data it holds. The responsibility also extends to personal data that is processed by a third party on behalf of Tamworth Borough Council. The departments will hold a record of all their processing activities containing personal information, irrespective of format. Where required each department will provide the necessary information to Data Protection Officer to demonstrate Accountability under Data Protection Legislation.

Legal Services
Legal Services, provided through South Staffs will provide advice and assistance on matters relating to the Data Protection Act as required.

7 Information Sharing

Information sharing is the sharing of sensitive and/or personal information in a closed way, between or within organisations. In instances of sharing, in order to comply with the DPA 2018 and other relevant legislation, the Council are responsible for giving individuals' clear and adequate information about how their information will be protected.

The Council will give thought to the following before sharing personal data with third parties:

- Does the Council have the power to share the information, for example, if consent is the lawful basis for sharing, how is the consent obtained and recorded?
- Is the sharing justified;
- Is the sharing to be carried out on an ad hoc or systematic basis;
- Is an information sharing agreement to be created; and
- how to ensure the security of information being shared

Any sharing of personal information between the Council and other organisations will be subject to an information sharing protocol that commits the partners to an agreed data transfer process that meets the requirements of the Data Protection Act, and as specified by an overarching Information Sharing Protocol.

A review and log of Information Sharing Agreements involving Council services will be maintained by the DPO.

Lawful basis for processing

The lawful basis for processing personal data is set out in the UK-GDPR and DPA 2018. At least one of these must apply whenever the Council processes personal information:

- **Consent:**
  The data subject has given clear and unambiguous consent for the Council to process his/her personal data for a specific purpose.

- **Contract:**
  The processing is necessary for a contract that the Council has with the data subject, or because the data subject has asked the Council to take specific steps before entering into a contract.

- **Legal Obligation:**
  The processing is necessary for the Council to comply with the law (not including contractual obligations).

- **Vital interests:**
  The processing is necessary to protect someone's life. If you can reasonably protect the person's vital interests in another less intrusive way, this basis will not apply.

- **Public interest:**
  The processing is necessary for the Council to perform a task in the public interest or in the exercise of official authority vested in the Council.

- **Legitimate interests:**
  The processing is necessary for the purposes of legitimate interests pursued by the Council or a third party except where such interests are overridden by the interests of the data subject. This requires balancing the Council's interests against the individual's interests. However, this basis is not available to processing carried out by the Council in the performance of its official tasks.

Consent

UK-GDPR now places a higher threshold for using consent as a lawful basis for processing person or special category data.
The correct use of consent should put individuals in control of their personal data, build customer trust and engagement, and enhance the Council's reputation.

Where the Council has another lawful basis for processing personal data this should be relied upon instead of consent, as consent must only be used where the data subject has a true choice in the processing of their personal data

Any data collection forms used in order to record personal information MUST contain a 'fair processing' statement. This should be clearly visible and placed appropriately on the form detailing our duties under the Data Protection Act. The statement should also contain the following information:

- The identity of the data controller; contact for submitting subject access requests.
- The purpose or purposes for which the information is intended to be processed.
- Any foreseeable third parties that the information is intended to be disclosed to.
- Any further information in order to make the processing fair.

When collecting information over the telephone, or face to face, the above information should also be made clear to the data subject **before** any processing of their personal data takes place.

Recording and using data

Data **MUST** only be used for the purposes it was collected and **MUST** not be used for any additional purposes without the consent of the data subject.

Tamworth Borough Council has a duty to inform all individuals of why their personal data is being collected. **Principle 1** stipulates that all personal data collected should be fair and lawful and processed in line with the purpose it was given. The Council may need to hold and process the information in order to carry out its statutory obligations, where this process takes place it will also be processed fairly and lawfully.

Processing Sensitive Data

When processing sensitive data, the Council **MUST** be able to demonstrate that the processing is strictly necessary and satisfies one of the conditions in Schedule 8 of the DPA or is based on consent.

8 Rights of Individuals

The Data Protection Act provides individuals the following rights:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

Note: Not all rights are absolute and will depend on the lawful basis on which the Council are relying to process the personal data.

Right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under Data protection legislation.

The Council must provide privacy information to individuals at the time their personal data is collected from them. The information provided to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language. This is done in a Privacy Notice, made available on the Councils website.

The information you must supply is determined by whether you obtained the personal data directly from the data subject, or from a 3rd party.

Information that must be contained within the Privacy Notice can be found in Appendix A

A review and log of Privacy Notices will be maintained by the DPO

Right of subject access

Data Subjects have the right to request access to their personal information upon written application to the data controller for information which they believe may be held by them.

If the Council does hold the requested information, then subject to any exemptions, will provide a legible copy to the applicant or their authorised recipient within one month (prescribed period) of receipt of the subject access request.

Alternatively, the applicant or their authorised recipient may wish to view only the files. The files will be prepared in such a way to comply with the DPA 2018 and arrangements made to allow privacy whilst inspecting. An appropriate officer must be in attendance at all times whilst this process is being carried out to maintain security of the documentation, this again must be carried out within the prescribed period.

The Council will be diligent in providing the information within the prescribed period. Where this period is insufficient then the applicant must be informed at the earliest possible time and within one calendar month giving good reasons for the delay (resource shortage will not be considered a good reason). Where the period will be exceeded it is good practice to disclose any available information immediately and not wait until the package is complete.

If the applicant subject believes that Tamworth Borough Council has not responded correctly and are dissatisfied with the Council's response, they are entitled to lodge a complaint with the Information Commissioners Office, who may carry out an investigation and can result in a fine being levied.

Further information on Subject Access Requests (SAR) is detailed in the Councils Subject Access Guide

Right of rectification

Individuals have the right to have inaccurate personal data rectified. An individual may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing.

On receipt of a request for rectification Tamworth Borough Council should take reasonable steps to ensure that the data is accurate and to rectify the data if necessary, within the prescribed period (one calendar month)

The Council can refuse to comply with a request for rectification if the request is manifestly unfounded or excessive. The individual must be informed of the decision within one calendar month of receiving the request.

Right of erasure

Individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

The Council must respond to a request within one calendar month.

Right to restrict processing

Individuals have the right to request the restriction or suppression of their personal data. It is not an absolute right and only applies in certain circumstances. The Council has one calendar month to respond to the request.

When processing is restricted, the Council is permitted to store the personal data, but not use it.

Right of data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.

This right only applies to information an individual has provided to a controller (the Council).

Right to object

Individuals have the right to object to the processing of their personal data in certain circumstances.

They have an absolute right to stop their data being used for direct marketing. However, in other cases where the right to object applies Tamworth Borough Council may be able to continue processing if they can show that they have a compelling reason for doing so.

The Council must respond to an objection within one calendar month of receiving it.

Rights related to automated decision-making including profiling

Solely automated individual decision-making, including profiling with legal or similarly significant effects is restricted.

Tamworth Borough Council is required to give individuals specific information about automated individual decision-making, including profiling. There are additional restrictions on using special category and children's personal data.

There are grounds for this type of processing that lift the restriction, but the Council is required to introduce additional safeguards to protect data subjects where one of these grounds applies.

9 Training

All employees of Tamworth Borough Council that hold, have access to, or process personal information will receive appropriate training to comply with Data Protection legislation.

Data Protection awareness is essential for all personnel that carry out these functions, and the Council will provide this awareness through e-learning, to ensure that compliance with the DPA 2018 is known and understood and how DPA relates to their duties.

It is the responsibility of all Heads of Service / Managers to ensure that the appropriate level of training has been received by their staff.

Records will be held on the employees' electronic file within the iTrent HR& payroll system

10 Data Breach Notification

A data breach could be defined as the unintentional release of personal or special category information (as defined under the Data Protection Act 2018) to an unauthorised person, either through accidental disclosure or loss/theft. However, non-compliance with any of the Principles referred to in Section 5 could be classed as a breach, particularly if there is a possibility that the data subject could be put at risk or suffer substantial damage or distress.

A security incident is defined as a breach of council security which may result in a risk of loss, access to or corruption of council information or assets, whether personal or not.

The Councils Breach Notification procedure is described in more detail in the Councils Breach Notification procedure

11 Breach of policy

The document will be distributed through Astute as a **MANDATORY** policy where applicable and will also be available on the Infozone and staff will be reminded to refresh their knowledge and understanding of the policy on an annual basis.

If any user is found to have breached this Policy, they could be subject to the organisation's Conduct and Capability Policy. The policy can be found on Infozone

End of Document

Appendix A

What information do we need to provide?	**Personal data collected from individuals**	**Personal data obtained from other sources**
The name and contact details of your organisation	✓	✓
The name and contact details of your representative	✓	✓
The contact details of your data protection officer	✓	✓
The purposes of the processing	✓	✓
The lawful basis for the processing	✓	✓
The legitimate interests for the processing	✓	✓
The categories of personal data obtained		✓

The recipients or categories of recipients of the personal data	✓	✓
The details of transfers of the personal data to any third countries or international organisations	✓	✓
The retention periods for the personal data	✓	✓
The rights available to individuals in respect of the processing	✓	✓
The right to withdraw consent	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source of the personal data		✓
The details of whether individuals are under a statutory or contractual obligation to provide the personal data	✓	

The details of the existence of automated decision-making, including profiling	✓	✓