Stratford-on-Avon District Council

# Data Protection Policy

| | |
|---|---|
| **Title** | Data Protection Policy |
| **Author** | Information Governance Manager |
| **Date** | 16 July 2018 |
| **Version No.** | 1 |
| **Status** | Final |
| **Protective Marking** | OFFICIAL |
| **Review Date** | Annually |
| **Distribution** | Internal |

# Contents


1. Document Control ..... 2
2. Introduction ..... 3
3. Policy Statement ..... 4
4. Key Roles and Responsibilities ..... 5
   Leader and Cabinet ..... 5
   Executive Directors and Senior Management Team ..... 5
   Senior Information Risk Owner ("SIRO") ..... 5
   Information Risk Owners ("IRO") ..... 5
   Information Governance Manager ..... 6
   Information Governance Special Interest Group ("IG SIG") ..... 6
   Service Management Teams and Service Managers ..... 6
   Other key responsibilities ..... 7
5. The Data Protection Principles ..... 8
   The Lawfulness, Fairness and Transparency Principle ..... 8
   The Purpose Limitation Principle ..... 8
   The Data Minimisation Principle ..... 8
   The Accuracy Principle ..... 8
   The Storage Principle ..... 8
   The Integrity and Confidentiality Principle ..... 8
6. "Personal Data" and "Special Personal Data" ..... 9
   What are Personal Data and Special Personal Data? ..... 9
   When can we use Personal Data and Special Personal Data? ..... 9
   What is consent? ..... 10
   What is a legitimate interest? ..... 10
   What is the public interest? ..... 11
7. Privacy Notices ..... 12
8. Data Protection Impact Assessments ("DPIAs") ..... 14
   What is a DPIA? ..... 14
   When is a DPIA required? ..... 14
   How to conduct a DPIA? ..... 14
9. Records Management ..... 16
   The Register of Processing Activities ("ROPA") ..... 16
   Information held on third party servers outside of the EEA ..... 16
   Information held in Microsoft Outlook and electronic filing systems ..... 16
   Information not held in electronic filing systems ..... 17
   Protective marking ..... 17
10. Information Rights ..... 19
   Freedom of Information requests ..... 19
   Requests for somebody else's personal data ..... 19
   Requests to *access* personal data ("Subject Access Request") ..... 20
   Requests to *rectify* personal data ..... 21
   Requests for the *erasure* of personal data ("the Right to be Forgotten") ..... 21
   Requests to *restrict* the processing of personal data ..... 23
   Requests for the *portability* of personal data ..... 23
   Responding to *objections* to the processing of personal data ..... 24
   Requests *not to be subject to automated decision-making* ..... 24
11. Exemptions ..... 26
   Crime and taxation exemption ..... 26
12. Training and Guidance ..... 27
13. Data Incidents and Breaches ..... 28
14. Retention and Destruction ..... 29
Appendix 1 – The Records Lifecycle ..... 30

# 1. Document Control

1.1 This policy sets out the Council's requirements in relation to officers' roles and responsibilities, the use of personal and private information, access to information and the exercise of other information rights, protecting information that needs to be retained, secure and confidential, compliance with the law on freedom of information and data protection, being transparent and proactive by making information accessible whenever it can, disclosing and sharing information when necessary, records management, training, data incidents, how we provide people with details of how we use their information ("privacy notices"), when and how we obtain consent from individuals to use their information, protective marking, phishing and fraud.

1.2 This policy applies to all employees, all workers who are not employees (e.g. individuals supplied through an agency or other company or partner or subsidiary organisations, contractors, individuals seconded to the Council or otherwise engaged on Council business), all volunteers, any individuals on work experience at the Council and all councillors. Any reference in this document to an "employee" is deemed to be a reference to any of the above.

1.3 This document is for internal use only. Any requests for copies of this document should be directed to the Information Governance Manager.

1.4 This policy will be reviewed annually in line with legislation and official guidance. Details of updates made to this document are set out in the table below.

| **Version No.** | **Date of edits** | **Description of edits** | **Editor** |
|---|---|---|---|
| 1 | 16 July 2018 | Original version | Phil Grafton |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

*Table 1*

# 2. Introduction

2.1 The Council accumulates information from both individuals and external organisations. The Council also generates a wide range of information, which is collected into records. Information is a vital asset for the provision of services to the public and for the efficient management of the Council's services and resources.

2.2 "Information" is used here as a collective term to cover terms such as data, documents, records, web content, images and biometric data. The Council's documents and records are in several different formats e.g. communications such as letters, emails and attendance notes; financial information including invoices, statements and reports; legal documents such as contracts and deeds; and information relating to various types of applications, including forms, plans, drawings, photographs and tape recordings.

2.3 Some of this personal information is shared with other organisations (including contractors and government bodies) in the interests of the individuals concerned or in the public interest.

2.4 Information governance is concerned with how information is held, obtained, recorded, used and shared by the organisation. Information governance plays a key part in service planning, performance management, protecting confidentiality and ensuring rights of access to information. It is essential that the Council has a robust system of information governance in place to ensure that information is effectively managed.

2.5 The General Data Protection Regulation, together with other data protection legislation, strikes a balance between the privacy rights of individuals and the interests of other parties who access their personal information. The legislation requires the Council to handle personal information relating to living identifiable individuals in a fair, safe, responsible and secure manner.

2.6 The law on data protection is affected by other regulatory regimes including the Privacy and Electronic Communications Regulations, the common law on confidentiality and the Freedom of Information Act.

2.7 The effect of a breach of the legislation can be very distressing and damaging to the individual concerned, and can also be damaging for the party responsible for the breach. The law does not create unreasonable barriers to the use of personal or private information, but it does subject individuals and organisations to significant sanctions for unfair, unlawful, disproportionate, or reckless use of personal data.

2.8 The Council expects everyone who works on its behalf to recognise their responsibility for treating personal and private information with the care and respect it deserves. The same applies to those bodies with which the Council shares personal information.

# 3. Policy Statement

3.1 The Council regards the lawful and correct treatment of personal information as very important to successful operations and to maintaining public confidence. The Council will always do its utmost to ensure that it treats all information lawfully and correctly.

3.2 The Council fully endorses the requirements of the General Data Protection Regulation (GDPR) and the other data protection legislation.

3.3 The Council recognises that information rights are important in ensuring that the Council operates in a transparent and accountable way, and that they give power to the individual to control the use of their personal information.

3.4 The Council recognises that its records are valuable assets and vital to the delivery of high quality public services. Effective records management is also essential in enabling the Council to comply with its legal and regulatory obligations. This policy sets out the Council's requirements.

3.5 The Council is committed to meet its obligations in law and in spirit by ensuring that it –

(a) values the personal information entrusted to it and make sure that it respects that trust (there should be no surprises for the data subject in the way that personal information is processed, used and shared);

(b) goes further than just the letter of the law when it comes to handling personal information and adopts good practice standards ensuring transparency and accountability;

(c) addresses privacy risks first when planning to process personal information in new ways, such as when introducing new systems;

(d) informs individuals when information will be shared and why, and ensures that the organisations with whom information is shared are fully compliant with information law;

(e) gives access to data subject's information when they request it, as well as processing updates and corrections in a timely manner;

(f) keeps personal information to the minimum extent necessary and deletes it when no longer needed;

(g) has effective safeguards in place to make sure personal information is kept securely and does not fall into the wrong hands;

(h) provides awareness training to all staff who handle personal information;

(i) puts appropriate financial and human resources into looking after personal information; and

(j) regularly checks compliance with this policy and legislative requirements.

# 4. Key Roles and Responsibilities

4.1 Every employee and other person to whom this policy applies is responsible for the appropriate use and protection of personal information which is in their possession or use. Everyone is also responsible for familiarising themselves with their obligations under this policy and related ones, for ensuring their own compliance and for seeking guidance where they need it.

## Leader and Cabinet

4.2 The Cabinet is the lead councillor body responsible for information governance. The Cabinet is responsible for ensuring that sufficient resources are made available to support the Council and its employees in meeting the obligations under this policy.

4.3 The Leader is Portfolio Holder for Strategic Leadership. The Governance and Democracy Portfolio Holder is responsible for Information Governance, which includes data protection.

## Executive Directors and Senior Management Team

4.4 The two Executive Directors are the Head of Paid Service and the s151 Officer respectively. Together with the Heads of Service they form the Council's Senior Management Team which will ensure delivery of an effective council-wide information governance approach.

4.5 The Executive Directors will ensure a co-ordinated response from the Council and its employees to this policy and keep under review the Council's approach to personal information, data protection and privacy.

4.6 The Senior Management Team will ensure that information governance policies, standards, procedures and systems are in place and operating effectively throughout the Council.

## Senior Information Risk Owner ("SIRO")

4.7 The SIRO is the Head of Governance and Democracy (and Monitoring Officer). As Head of Governance and Democracy, the SIRO is a Head of Service and member of the Senior Management Team.

4.8 The SIRO has overall responsibility for managing information risk in the Council, and will in particular, ensure compliance with legislation and policies relating to information governance, provide a focal point for managing information risks and incidents and foster a culture for protecting and using information within the Council.

## Information Risk Owners ("IRO")

4.9 Heads of Service are designated IROs in respect of their individual Services.

4.10 IROs will understand how the information assets are held, used and shared; and they will be responsible for identification, access, security, and privacy of personal information. IROs will be responsible for ensuring (in accordance with this Policy) that their records management arrangements are fit for purpose.

4.11 IROs are responsible for the management of information risk for their service's information assets. This includes ensuring that their information assets are properly recorded in the Council's ROPA,

and that the ROPA is reviewed and updated as required (see **The Register of Processing Activities ("ROPA")** below).

4.12 IROs will address risks to the information including by incorporating an assessment of data protection and privacy risk into their risk management arrangements and by ensuring that action is taken where necessary to reduce the Council's information risk exposure.

4.13 IROs will make sure that employees who access or handle personal information are suitably trained in order to understand their obligations under this policy.

4.14 IROs must ensure that any new or amended systems for processing personal data are screened for the possible need to produce a full Data Protection Impact Assessment ("DPIA") (see **Data Protection Impact Assessments ("DPIAs")** below).

4.15 Heads of Service may delegate the operational aspect of these functions to one or more officers within their service area.

## Information Governance Manager

4.16 The Information Governance Manager is the Data Protection Officer for the Council for the purposes of the General Data Protection Regulation and the Data Protection Act 2018.

4.17 The Information Governance Manager is responsible for reporting on data protection compliance, advising on Data Protection Impact Assessments and liaising with the Information Commissioner over data breaches, data protection notifications and other issues as appropriate.

4.18 The Information Governance Manager will advise on information legislation and records management best practice and will record, issue, track and report on all information and data subject requests.

4.19 The Information Governance Manager will provide expert advice and guidance to all staff on all elements of information governance. The Information Governance Manager is responsible for developing information governance policies and procedures, and for working with the SIRO and IROs (and their representatives) to establish protocols on how information is to be used and shared.

4.20 The Information Governance Manager will develop information governance awareness and training modules for staff, and remind staff of their obligations. The Information Governance Manager will raise awareness of official guidance, policies and codes of practice.

## Information Governance Special Interest Group ("IG SIG")

4.21 The IG SIG shall meet regularly and consist of the Information Governance Manager (chair), the SIRO and all IROs or their nominated representatives.

4.22 The terms of reference for the IG SIG will be kept alongside this document.

## Service Management Teams and Service Managers

4.23 A Service Management Team comprises the Head of Service and all Service Managers for a Service.

4.24 Service Management Teams and individual Service Managers are accountable for the effective management of information risk and information governance compliance, as well as the

implementation of, and adherence to, this policy and any associated standards and procedures within their team.

4.25 Service Managers are responsible for implementing measures that ensure compliance with this policy including conducting new staff inductions, arranging compliant local procedures and systems, and providing appropriate communications and awareness-raising of data protection requirements (both among employees and contractors with whom the deal).

4.26 Service Managers must ensure that their teams receive sufficient guidance to ensure that record systems are actively maintained, and to foster an awareness of the full record life cycle.

## Other key responsibilities

4.27 ICT services will provide technical security management of the infrastructure and technical security advice, including areas such as PSN Code of Connection, PCIDSS and device policy. ICT is responsible for advising on digital security and use of network drives.

4.28 Legal Services will provide expert legal opinion on all information governance matters to all service teams.

4.29 There will be identified roles in the Services whose role includes some aspects of information governance and ensuring compliance. These will vary according to the Service.

4.30 Disregard for information governance policies by employees may be regarded as misconduct to which the Council's Dismissal and Disciplinary Procedure applies and a serious breach of any policy may be treated as gross misconduct and may lead to dismissal.

4.31 Disregard by contractors and agents working for the Council will be regarded as a contractual breach. Disregard by volunteers and work experience students working for the Council may lead to terminating their work agreement.

# 5. The Data Protection Principles

5.1 All employees must comply with the six data protection principles. The Council's policies and guidelines underpin these principles.

## The Lawfulness, Fairness and Transparency Principle

5.2 Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

## The Purpose Limitation Principle

5.3 Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

## The Data Minimisation Principle

5.4 Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

## The Accuracy Principle

5.5 Personal data shall be 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.

## The Storage Principle

5.6 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.

## The Integrity and Confidentiality Principle

5.7 Personal data shall be 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.

# 6. "Personal Data" and "Special Personal Data"

## What are Personal Data and Special Personal Data?

6.1 "Personal data" means any information relating to an identified or identifiable natural person.

6.2 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.

6.3 "Special personal data" is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a person's sex life or sexual orientation.

6.4 There are also specific requirements for the handling of criminal conviction details and the personal information of children.

6.5 All those handling personal information must be aware of the extra sensitivity of these categories of personal data and be aware that any data protection breaches involving these will have correspondingly more serious consequences for the data subject and the Council.

## When can we use Personal Data and Special Personal Data?

6.6 Your collection and use of personal data must not exceed what is necessary to enable you to perform your job; and you may only collect, process and share personal data where you are able to identify a specific purpose for doing so.

6.7 Personal data must not be processed in any manner which is incompatible with the purpose for which it was originally collected.

6.8 Furthermore, you must only collect, process and share Personal Data where you can point to a "lawful basis". The lawful bases are that the use of the information is –

(a) on the basis of the individual's consent (see **What is consent?** below);

(b) necessary for the performance of a contract with the individual;

(c) necessary to meet one of our legal obligations;

(d) necessary to protect somebody's "vital interests" i.e. an interest which is essential to life;

(e) necessary for the purposes of our legitimate interests (see **What is a legitimate interest?** below); or

(f) necessary for the performance of a task carried out in the public interest or in the exercise of our official authority (see **What is the public interest?** below).

6.9 Additionally, you will only collect and use special personal data where one of the following applies –

(a) the individual has given their explicit consent (see **What is consent?** below);

(b) it is necessary for the purposes of employment, social security and social protection law;

(c) it is necessary to protect somebody's "vital interests" i.e. an interest which is essential to life;

(d) the information has been manifestly made public by the individual;

(e) it is necessary for the establishment, exercise or defence of legal claims;

(f) it is necessary for reasons of substantial public interest (see **What is the public interest?** below);

(g) it is necessary for the purposes of preventative or occupational medicine;

(h) it is necessary in the area of public health; or

(i) it is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

6.10 These restrictions are not intended to prevent processing, but to ensure that we process personal data fairly and without adversely affecting the individual concerned.

## What is consent?

6.11 Where consent is required to obtain personal information, because there is no other lawful basis for collecting it, consent must be positively and unambiguously affirmed. No reliance can be placed on consent obtained by default (e.g. pre-ticked boxes), implied consent or inferred consent, and a record must be held of the consent.

6.12 It is not permissible to use consent as a lawful basis for holding and using information where another lawful basis exists or in any situation where the data subject has no effective choice.

6.13 The Information Commissioner's Office has issued guidance that public bodies (such as the Council) will not ordinarily be able to rely on consent as a lawful basis to process data. The reason for this is that there is an imbalance of power between the public body and the individual.

6.14 Consent may still be the appropriate lawful basis in limited circumstances e.g. where the Council is obtaining addresses for a newsletter, or email addresses for planning updates or job alerts, etc..

6.15 Where personal data is being used on the basis of the individual's consent – the individual may (and must be informed that they may) at any time, withdraw that consent.

6.16 This approach must be taken to all existing and new uses of personal information involving consent.

## What is a legitimate interest?

6.17 The Council is prohibited from relying on its 'legitimate interests' as a lawful basis for processing data when it is performing its tasks as a public authority. This limits the Council's ability to rely on this lawful basis to instances when (i) no other lawful bases are applicable, and (ii) the Council is acting outside of the scope of its tasks as a public authority (e.g. personnel functions, etc.).

6.18 In order to rely on this lawful basis it is necessary to identify the legitimate interest, show that the processing is necessary to achieve it, and balance it against the individual's interests, rights and freedoms.

## What is the public interest?

6.19 This is the lawful basis under which the Council will process the majority of the personal data that it holds.

6.20 This lawful basis will apply in circumstances including where the processing of personal data is necessary for the exercise of a statutory function or the administration of justice.

# 7. Privacy Notices

7.1 We must provide detailed, specific information to individuals about how their information is used.

7.2 This information must be provided through privacy notices which must be concise, transparent, intelligible, easily accessible, and written in clear and plain language.

7.3 Whenever we collect personal data directly from an individual, we must provide them with the required information through a privacy notice which must be presented when the individual first provides the personal data i.e. on the form that they complete, in our initial acknowledgment letter to them, etc..

7.4 When personal data is collected indirectly e.g. from a third party or publicly available source, we must provide the individual with the required information as soon as possible after collecting or receiving the data.

7.5 The details that must be provided include –

(a) the identity and the contact details of the data controller;

(b) the contact details of the data controller's data protection officer (see **Information Governance Manager** above);

(c) the purposes of the processing for which the personal data are intended as well as the lawful basis for the processing (see **"Personal Data" and "Special Personal Data"** above);

(d) where the lawful basis for the processing is the data controller's legitimate interests – details of those legitimate interests (see **What is a legitimate interest?** above);

(e) where the lawful basis for the processing is the individual's consent – details of their right to withdraw consent (see **What is consent?** above);

(f) the recipients of the personal data, or categories of recipients;

(g) where applicable, details of the transfer of the information outside of the EEA and the personal data safeguards that would apply to such transfer (see **Information held on third party servers outside of the EEA** below);

(h) the period for which the personal data will be stored, or the criteria used to determine that period;

(i) the existence of the right to request from the controller access to, and rectification or erasure of, personal data, or restriction of processing concerning the individual, or to object to processing, as well as the right to data portability where applicable (see **Information Rights** below);

(j) the right to lodge a complaint with the Information Commissioner's Office;

(k) the existence of any statutory or contractual obligation to provide the information, and the consequences of failing to do so;

(l) the existence of automated decision making or profiling as well as the significance and consequences for the data subject;

(m) details of any further or secondary processing; and

(n) (in cases where the personal data has been obtained otherwise than from the individual concerned) the origin of the personal data and the categories of personal data held.

7.6 The Information Commissioner's Office has issued guidance on how these details can be provided without causing "information overload" – it is recommended that these details are provided in a 'tiered' format that provides the most appropriate details at the most appropriate time.

7.7 The details must be provided for all existing and new uses of personal information.

7.8 The information must be provided unless an exemption applies (see **Exemptions** below).

# 8. Data Protection Impact Assessments ("DPIAs")

## What is a DPIA?

8.1 DPIAs are a formal procedure through which an organisation can assess the impact of data processing activities on the protection of personal data. It is a form of "privacy by design" activity intended to demonstrate an organisation's compliance with its accountability obligations under data protection laws.

8.2 DPIAs are assessments of the impact of anticipated processing operations on the protection of personal data. This is done by evaluating processing practices, assessing the necessity and proportionality of processing, and managing risks to data subjects.

## When is a DPIA required?

8.3 A DPIA must be carried out when processing personal data is "likely to result in a high risk to the rights and freedoms of natural persons". If it is unclear whether processing is high risk, it is recommended that a DPIA be carried out regardless.

8.4 In particular, a DPIA must be carried out in circumstances where there is –

(a) a 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;

(b) processing on a large scale of special personal data or personal data relating to criminal convictions and offences (see **What are Personal Data and Special Personal Data?** above).

(c) a systematic monitoring of a publicly accessible area on a large scale; or

(d) large-scale processing operations that aim at processing considerable amounts of data and could affect a large number of individuals.

8.5 In addition to the above, the Information Commissioner's Office will publish a list of circumstances where a DPIA is required.

8.6 A DPIA should be commenced as early as practical, even where aspects of the processing operation remain unknown. The consequence of commencing a DPIA in advance may mean that DPIAs will frequently require revision once processing has started – however, this is no excuse for postponing or failing to engage in a DPIA.

## How to conduct a DPIA?

8.7 The Information Governance Manager should be consulted immediately whenever a DPIA is conducted so that they can advise on the procedure to be followed and provide template documents.

8.8 The procedure to conduct a DPIA should be broadly as follows –

(a) Prepare a description of the intended processing operations and the purposes of the processing.

(b) Assess the necessity and proportionality of the processing.

(c) Assess the risks to the rights and freedoms of data subjects.

(d) Consider the measures to address the identified risks and thereby demonstrate compliance.

8.9 If the processing is "wholly or partly" performed by a third party processor, the processor should provide assistance and any necessary information in the conduct of the DPIA.

8.10 The individuals concerned should be consulted during the conduct of the DPIA where appropriate. If the individuals are not consulted, then the DPIA should set out the reasons for this. If the final decision is different to the views of the individuals, then the reasons for the decision should be documented.

8.11 Obtaining the individuals' consent (see **What is consent?** above) does not constitute consulting them for the purposes of conducting a DPIA.

8.12 All DPIAs must be conducted in accordance with the official guidance at the time.

8.13 If the outcome of the DPIA indicates a high risk which cannot be mitigated or reduced (even after protective measures have been introduced) – the Information Commissioner's Office must be formally consulted. This consultation will be undertaken by the Information Governance Manager.

8.14 A record of the DPIA should be retained for the lifetime of the system or project. If it is determined that a DPIA does not need to be carried out, a record should also be kept of the reasons why a DPIA was not considered necessary.

# 9. Records Management

## The Register of Processing Activities ("ROPA")

9.1 The General Data Protection Regulation ("GDPR") requires the Council to keep a register of all activities where it processes personal data ("the ROPA"). The ROPA contains essential details about the lawful basis, use, security, sharing and retention of personal information.

9.2 All significant information and record systems will be recorded in the ROPA.

9.3 The ROPA is held by the Information Governance Manager and all IROs must ensure that it is kept up to date.

## Information held on third party servers outside of the EEA

9.4 Information held by the Council should ordinarily be held on its own servers. In some circumstances, information may be held on third party servers located outside of the EEA e.g. where the Council is using a web-based service to send surveys (e.g. Survey Monkey) or newsletters (e.g. Mail Chimp) to its service users.

9.5 Information will only be held on third party servers outside of the EEA where either –

(a) the European Commission has made a decision that the destination ensures an adequate level of protection for personal data ("an Adequacy Decision"); or

(b) in the absence of an Adequacy Decision, the Council (if applicable) is able to provide appropriate safeguards and ensure that enforceable data subject rights and effective legal remedies for data subjects are available.

9.6 The Information Governance Manager should be consulted for further information as to what Adequacy Decisions have been made and what safeguards are required to be in place.

## Information held in Microsoft Outlook and electronic filing systems

9.7 When circulating documents internally, wherever possible, a link to the document in a shared drive should be circulated in preference to the document itself being circulated as an attachment. This is to reduce duplication of documents on the Council's systems.

9.8 Microsoft Outlook should not be used as a filing system.

9.9 Emails should either be stored within a specific business application system or EDMS. If this is not possible records should held in folders in a structure that allows active management in accordance with the record lifecycle (see **Appendix 1 – The Records Lifecycle**) including deletion when required by the Retention and Destruction Policy.

9.10 For some records that might form evidence for court proceedings or investigations it can be important that secure storage with appropriate rights access can be demonstrated as well as a supporting change log or history. The possible need to maintain evidential integrity should be considered when record systems are set up.

## Information not held in electronic filing systems

9.11 Where records are not entered on a specific business application or an Electronic Document and Records System ("EDMS"), the Council's standard "record metadata set" should be applied whenever possible. This metadata set appears as follows –

| | |
|---|---|
| **Title** | |
| **Author** | |
| **Date** | |
| **Version No.** | |
| **Status** | |
| **Protective Marking** | |
| **Review Date** | |
| **Distribution** | |

*Table 2*

9.12 Records with protective marking should always be handled and stored with caution.

## Protective marking

9.13 The Council has adopted a systematic approach to the classification of the information that it holds. This approach takes into account the potential impact of the loss or disclosure of different types of information. The Council's approach is based upon that of central government which was introduced in April 2014 and is set out in the Cabinet Office's Government Security Classifications Scheme ("GSCS").

9.14 The protective markings attached to the Council's information do not, in and of themselves, impose any particular requirements in relation to data protection or freedom of information law. They are simply an indication of the sensitivity of the information e.g. that it may contain personal data or special personal data.

9.15 A protective marking should be attached to all information for internal use. An explanation of the different protective markings available is set out below.

| Protective Marking | Explanation |
|---|---|
| Unclassified | Information should be marked as Unclassified where it does not relate to the Council's work e.g. internal emails about Christmas parties, staff socials, appraisals, etc.. |
| OFFICIAL | OFFICIAL is the default protective marking for all information relating to the Council's work and will apply to the majority of information held by the Council. |
| OFFICIAL – PERSONAL | Any OFFICIAL information which contains personal data should be protectively marked as OFFICIAL – PERSONAL. |

| | |
|---|---|
| OFFICIAL – SENSITIVE | Any OFFICIAL or OFFICIAL – PERSONAL information which contains special personal data should be protectively marked as OFFICIAL – SENSITIVE.<br><br>(see **"Personal Data" and "Special Personal Data"** above)<br><br>This protective marking should also be applied to any information which is sensitive for another reason e.g. it contains details of criminal convictions, it contains private financial information, it has been imparted in confidence, it is commercially sensitive, etc. |
| SECRET and TOP SECRET | SECRET and TOP SECRET are the highest levels of protective marking and will apply rarely (if at all) to information held by the Council. Any information protectively marked as SECRET or TOP SECRET should be handled in accordance with the GSCS.<br><br>Information which should be protectively marked as SECRET or TOP SECRET includes information which, if compromised, could cause widespread loss of life or seriously damage military capabilities, national security, economic wellbeing, international relations or the investigation of serious organised crime. |

*Table 3*

# 10. Information Rights

10.1 Guidance must be available to persons wanting to access either the Council's information or the personal information that we hold about them. This will be on the Council's website with links to and from the Council's top level Privacy Notice and Publication Scheme.

10.2 All requests to exercise these information rights should be notified to the Information Governance Manager for record keeping purposes.

## Freedom of Information requests

10.3 Requests for information under Freedom of Information Act (FOIA) or Environmental Information Regulations (EIR) must be correctly identified. The request does not have to name the Act or Regulation specifically and conversely the requestor may name the FOIA or EIR mistakenly when the request is for personal data.

10.4 Requests for publically available information should be dealt with as routine requests unless the information is more difficult to locate, complex in nature, or subject to possible restrictions.

10.5 A self-service approach is encouraged for FOIA and EIR requests whereby public information that is regularly requested can be made available on the Council's website using search facilities or by reference to the Publication Scheme.

## Requests for somebody else's personal data

10.6 Requests for access to personal data will be treated formally and include the necessary safeguards to prevent inappropriate disclosure. Everyone must however be aware that there are situations where personal information is disclosable e.g. for the prevention, detection and prosecution of crime, or where there is a risk of significant harm to an individual.

10.7 Particular caution should be exercised in relation to records and information which has been protectively marked. Be aware that the protective marking is a broad indication of the content and handling required (see **Protective marking** above). A more detailed examination of the document content may be required for FOI and DPA request purposes.

10.8 Not all requests for personal or confidential information will be genuine. Employees must be alert to the possibility that the person requesting the information may not be genuine. Fraudsters and phishers can be very credible. Anyone routinely applying for information in an official capacity must follow an established sharing protocol. There must be a sharing protocol in place for any routine sharing of personal or confidential information. For ad hoc confidential information sharing identity and authorisation checks must be carried out.

10.9 Information security issues are covered in the ICT Code of Practice. Where an incident is likely to result in a high risk to the 'rights and freedoms' of a person the Council shall notify the data subject without undue delay unless action has already been taken to address those potential concerns. This is partly to ensure that affected individuals can take timely action where this is needed.

10.10 Services must make sure that their information systems whether manual, network and email folder based, Electronic Records Management or Business Application enable the Council to fulfil those requests fully and reliably where they are found to be correctly invoked.

## Requests to *access* personal data ("Subject Access Request")

10.11 Data subjects have the right to request access to their personal data processed by us. Such requests are called subject access requests (SARs). When a data subject makes an SAR we shall take the following steps –

(a) log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met);

(b) confirm the identity of the data subject who is the subject of the personal data. For example, we may request additional information from the data subject to confirm their identity;

(c) search databases, systems, applications and other places where the personal data which are the subject of the request may be held; and

(d) confirm to the data subject whether or not personal data of the data subject making the SAR are being processed.

10.12 If personal data of the data subject are being processed, we shall provide the data subject with the following information in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in writing or by other (including electronic) means –

(a) the purposes of the processing;

(b) the categories of personal data concerned (for example, contact details, bank account information and details of sales activity);

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients overseas (e.g. US-based service providers);

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data or to object to such processing;

(f) the right to lodge a complaint with the Information Commissioner's Office (ICO);

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; and

(i) where personal data are transferred outside the EU, details of the appropriate safeguards to protect the personal data.

10.13 We shall also, unless there is an exemption (see **Exemptions** below), provide the data subject with a copy of the personal data processed by us in a commonly used electronic form (unless the data subject either did not make the request by electronic means or has specifically requested not to be provided with the copy in electronic form) within one month of receipt of the request. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for responding we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay.

10.14 Before providing the personal data to the data subject making the SAR, we shall review the personal data requested to see if they contain the personal data of other data subjects. If they do, we may redact the personal data of those other data subjects prior to providing the data subject with their personal data, unless those other data subjects have consented to the disclosure of their personal data.

10.15 If the SAR is manifestly unfounded or excessive e.g. because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of providing the personal data, or refuse to act on the request.

10.16 If we are not going to respond to the SAR we shall inform the data subject of the reason(s) for not taking action and of the possibility of lodging a complaint with the ICO.

## Requests to *rectify* personal data

10.17 Data subjects have the right to have their inaccurate personal data rectified. Rectification can include having incomplete personal data completed, for example, by a data subject providing a supplementary statement regarding the data. Where such a request is made, we shall, unless there is an exemption (see **Exemptions** below), rectify the personal data without undue delay.

10.18 We shall also communicate the rectification of the personal data to each recipient to whom the personal data have been disclosed (for example, our third party service providers who process the data on our behalf), unless this is impossible or involves disproportionate effort. We shall also inform the data subject about those recipients if the data subject requests it.

## Requests for the *erasure* of personal data ("the Right to be Forgotten")

10.19 Data subjects have the right, in certain circumstances, to request that we erase their personal data. Where such a request is made, we shall, unless there is an exemption (see **Exemptions** and paragraph 10.23 below), erase the personal data without undue delay if –

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws their consent to the processing of their personal data and consent was the basis on which the personal data were processed and there is no other legal basis for the processing (see **What is consent?** above);

(c) the data subject objects to the processing of their personal data on the basis of our performance of a task carried out in the public interest (see **What is the public interest?** above), or on the basis of our legitimate interests (see **What is a legitimate interest?** above), unless we either can show compelling legitimate grounds for the processing which override those interests, rights and freedoms, or we are processing the data for the establishment, exercise or defence of legal claims;

(d) the data subject objects to the processing of their personal data for direct marketing purposes;

(e) the personal data have been unlawfully processed;

(f) the personal data have to be erased for compliance with a legal obligation to which we are subject; or

(g) the personal data have been collected in relation to the offer of e-commerce or other online services.

10.20 When a data subject makes a request for erasure in the circumstances set out above, we shall, unless there is an exemption (see **Exemptions** and paragraph 10.23 below), take the following steps –

(a) log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met);

(b) confirm the identity of the data subject who is the subject of the personal data. We may request additional information from the data subject to do this;

(c) search databases, systems, applications and other places where the personal data which are the subject of the request may be held and erase such data within one month of receipt of the request. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for responding we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay;

(d) where we have made the personal data public, we must, taking reasonable steps, including technical measures, inform those who are processing the personal data that the data subject has requested the erasure by them of any links to, or copies or replications of, those personal data; and

(e) communicate the erasure of the personal data to each recipient to whom the personal data have been disclosed unless this is impossible or involves disproportionate effort. We shall also inform the data subject about those recipients if the data subject requests it.

10.21 If the request is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of erasure, or refuse to act on the request.

10.22 If we are not going to respond to the request we shall inform the data subject of the reasons for not taking action and of the possibility of lodging a complaint with the ICO.

10.23 In addition to the main exemptions (see **Exemptions** below), we can also refuse to erase the personal data to the extent processing is necessary –

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by law and to which we are subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in us;

(c) for reasons of public interest in the area of public health;

(d) 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; or

(e) for the establishment, exercise or defence of legal claims.

## Requests to *restrict* the processing of personal data

10.24 Data subjects have the right, unless there is an exemption (see **Exemptions** below), to restrict the processing of their personal data if –

(a) the data subject contests the accuracy of the personal data, for a period to allow us to verify the accuracy of the personal data;

(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c) we no longer need the personal data for the purposes we collected them, but they are required by the data subject for the establishment, exercise or defence of legal claims; and

(d) the data subject has objected to the processing, pending verification of whether we have legitimate grounds to override the data subject's objection.

10.25 Where processing has been restricted, we shall only process the personal data (excluding storing them) –

(a) with the data subject's consent (see **What is consent?** above);

(b) for the establishment, exercise or defence of legal claims;

(c) for the protection of the rights of another person; or

(d) for reasons of important public interest (see **What is the public interest?** above).

10.26 Prior to lifting the restriction, we shall inform the data subject of the lifting of the restriction.

10.27 We shall communicate the restriction of processing of the personal data to each recipient to whom the personal data have been disclosed, unless this is impossible or involves disproportionate effort. We shall also inform the data subject about those recipients if the data subject requests it.

## Requests for the *portability* of personal data

10.28 Data subjects have the right, in certain circumstances, to receive their personal data that they have provided to us in a structured, commonly used and machine-readable format that they can then transmit to another organisation. Where such a request is made, we shall, unless there is an exemption (see **Exemptions** below), provide the personal data without undue delay if –

(a) the legal basis for the processing of the personal data is consent (see **What is consent?** above) or pursuant to a contract; and

(b) our processing of those data is automated.

10.29 When a data subject makes a request for portability in the circumstances set out above, we shall take the following steps –

(a) log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met);

(b) confirm the identity of the data subject who is the subject of the personal data. We may request additional information from the data subject to confirm their identity; and

(c) search databases, systems, applications and other places where the personal data which are the subject of the request may be held and provide the data subject with such data (or, at the data subject's request, transmit the personal data directly to another company, where technically feasible) within one month of receipt of the request. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for responding we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay.

10.30 If the request is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of providing or transmitting the personal data, or refuse to act on the request.

10.31 If we are not going to respond to the request we shall inform the data subject of the reasons for not taking action and of the possibility of lodging a complaint with the ICO.

## Responding to *objections* to the processing of personal data

10.32 Data subjects have the right to object to the processing of their personal data where such processing is on the basis of our performance of a task carried out in the public interest or in the exercise of official authority vested in us, or on the basis of our legitimate interests which override the data subject's interests or fundamental rights and freedoms, unless we either –

(a) can show compelling legitimate grounds for the processing which override those interests, rights and freedoms; or

(b) are processing the personal data for the establishment, exercise or defence of legal claims.

10.33 Data subjects also have the right to object to the processing of their personal data for scientific or historical research purposes, or statistical purposes, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

10.34 Where such an objection is made, we shall, unless there is an exemption (see **Exemptions** below), no longer process a data subject's personal data.

10.35 Where personal data are processed for direct marketing purposes, data subjects have the right to object at any time to the processing of their personal data for such marketing. If a data subject makes such a request, we shall stop processing the personal data for such purposes.

## Requests *not to be subject to automated decision-making*

10.36 Data subjects have the right, in certain circumstances, not to be subject to a decision based solely on the automated processing of their personal data, if such decision produces legal effects concerning them or similarly significantly affects them. Where such a request is made, we shall, unless there is an exemption (see **Exemptions** below), no longer make such a decision unless it –

(a) is necessary for entering into, or the performance of, a contract between us and the data subject;

(b) is authorised by applicable law which lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

10.37 If the decision falls within sub-paragraph (a) or (c), we shall implement suitable measures to safeguard the data subject's rights, freedoms and legitimate interests, including the right to obtain human intervention, to express their point of view and to contest the decision.

# 11. Exemptions

11.1 Before responding to any request or providing any privacy notice we shall check whether there are any exemptions that apply to the relevant personal data.

11.2 Exemptions may apply where it is necessary and proportionate not to comply with a request or provide a privacy notice to safeguard –

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security (see **Crime and taxation exemption** below);

(e) other important objectives of general national public interest, in particular an important national economic or financial interest, including monetary, budgetary and taxation matters, public health and social security;

(f) the protection of judicial independence and judicial proceedings;

(g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in sub-paragraphs (a) and (g) above;

(i) the protection of the data subject or the rights and freedoms of others; or

(j) the enforcement of civil law claims.

## Crime and taxation exemption

11.3 The requirements to provide a privacy notice (see **Privacy Notices** above) and to respond to requests to exercise information rights, with the exception of the right to request not to be subject to automated decision-making (see **Information Rights** above) do not apply where personal data is processed for any of the following purposes –

(a) the prevention or detection of crime;

(b) the apprehension or prosecution of offenders; or

(c) the assessment or collection of a tax or duty or an imposition of a similar nature.

11.4 The exemption only applies to the extent that failure to rely on the exemption would be likely to prejudice any of the matters mentioned above.

# 12. Training and Guidance

12.1 Information governance training for all employees will be mandatory as part of inductions (including for the avoidance of doubt, for all employees, seconded persons, agency workers and voluntary staff).

12.2 All staff will be required periodically to complete update/refresher training.

12.3 Awareness sessions may be given to staff as required, at team meetings or at other events.

12.4 Regular reminders on information governance topics will be made through corporate and local team briefings and emails.

12.5 Policies, procedures, standards and advice are available to staff at any time from the Information Governance pages of the intranet.

# 13. Data Incidents and Breaches

13.1 The ICT Code of Practice is available to all staff. All information security incidents involving digital or manual records whether actual or suspected, should be promptly reported to the ICT Services' Helpdesk via an individual's line manager or Service Manager and to the Information Governance Manager.

13.2 Any incident that could or does lead to loss, disclosure or temporary exposure of personal information must be reported as prescribed by the ICT Code of Practice. The Council has procedures for investigating data protection and privacy breaches and all those affected will be expected to co-operate with any such investigation.

13.3 If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the ICT Services' Helpdesk via an individual's line manager or Service Manager and to the Information Governance Manager and follow the ICT Code of Practice. You should preserve all evidence relating to the potential personal data breach

13.4 The GDPR requires the Council to notify certain personal data breaches to the Information Commissioner's Office and in certain circumstances to the individual concerned. Relevant data protection breaches will be reported to the Information Commissioner's Office and affected individuals by the Information Governance Manager.

13.5 Disregard for the Council's data protection and related policies by employees may be regarded as misconduct to which the Council's Disciplinary Procedure applies and a serious breach of any policy may be treated as gross misconduct and may lead to dismissal. In the case of contractors, representatives, workers and volunteers, this may be grounds for termination of that relationship with the council.

13.6 Disregard for the Council's data protection and related policies by councillors will be regarded as a breach of the Code of Conduct and will be considered in line with the adopted arrangements for the determination of complaints about councillors.

# 14. Retention and Destruction

14.1 Personal data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

14.2 You must not keep personal data in a form which permits the identification of the individual for longer than needed for the purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

14.3 The Council maintains a Retention and Destruction Policy to ensure that personal data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

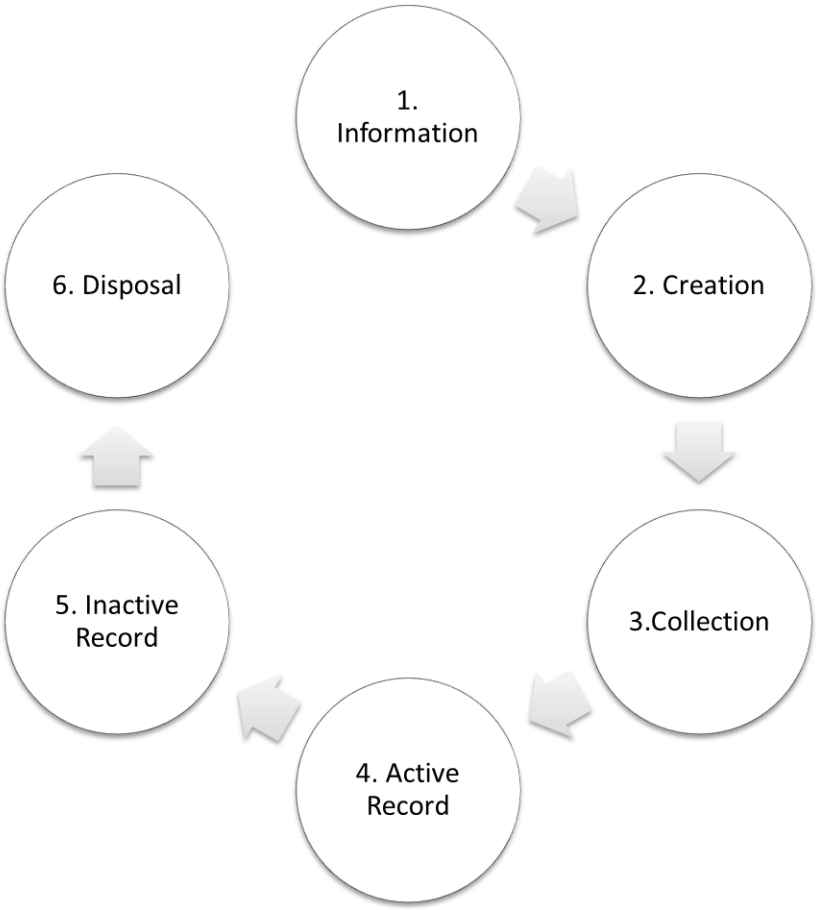
14.4 You will take all reasonable steps to destroy or erase from our systems all personal data that we no longer require in accordance with Retention and Destruction Policy. This includes requiring third parties to delete such data where applicable.

14.5 You will ensure that individuals are informed of the period for which data is stored and how that period is determined in any applicable privacy notice.

14.6 Records may only be disposed of in a secure and controlled way that ensures destruction and provides a full information trail.

14.7 Some records may be considered of future historical interest and the County Records Manager should be consulted regarding their possible preservation.

# Appendix 1 – The Records Lifecycle




| | | | |
|---|---|---|---|
| **1** | **INFORMATION** is received. | **4.** | **ACTIVE RECORD** The record is active and added to by amendments, new information, revised documents and collaboration with other teams or agencies. Searchability is key. |
| **2**. | **CREATION** Documents, emails, letters etc on the same subject are generated | **5** | **INACTIVE RECORD** The purpose that the record was created for is completed and the record is inactive for a specified period. |
| **3** | **COLLECTION** The information is collected and stored safely. | **6** | **DISPOSAL** When the retention period is complete the record is deleted or disposed of. It may be preserved if it is considered to be of future historic interest. |