**Appendix 1**

# TEWKESBURY BOROUGH COUNCIL

# Data Protection Policy

**Policy contents**

## SECTION ONE – POLICY OBJECTIVES

1.1 **Policy Objectives**

- To comply with all relevant legislation and good practice to protect the Personal Data held by the Council.
- To monitor, demonstrate and review compliance with legislation and introduce changes where necessary.
- To ensure that Personal Data is processed fairly and lawfully.
- To respect the confidentiality of all Personal Data.
- To provide staff with appropriate procedures and training to handle Personal Data.
- To assist members of the public in exercising their rights over their Personal Data held by the Council
- To co-operate with the Information Commissioner and the external auditor as required.

1.2 **Staff and Member responsibility**

It is the duty of individual staff and Members to ensure that Personal Data held by the Council is handled in accordance with current Data Protection Legislation and this Policy. Action may be taken against any employee or Member who fails to comply or commits any breach of the Data Protection Legislation and/or this Policy.

## SECTION 2 – INTRODUCTION TO DATA PROTECTION LEGISLATION

2.1 Data Protection Legislation was introduced to balance the rights of individuals, to protect their Personal Data and an organisation's right to use their Personal Data. Data Protection Legislation covers both electronic information and manual files the Council holds.

2.2 This Policy is applicable to all Data Protection Legislation relating to the use of Personal Data.

2.3 The Council processes and keeps Personal Data about Data Subjects to enable it to conduct Council business, provide services and to employ staff.

**The Data Protection Principles**

2.4 The Council will:

- process Personal Data lawfully, fairly and transparently (the first data protection principle)
- only obtain Personal Data for specified, explicit and legitimate purposes (the second data protection principle)
- only collect Personal Data that is adequate, relevant and not excessive (the third data protection principle)
- ensure that Personal Data is accurate and kept up to date (the forth data protection principle)
- ensure that Personal Data is not being kept for longer than is necessary (the fifth data protection principle)
- ensure that Personal Data is processed in a secure manner (the sixth data protection principle).

## SECTION THREE – ACCOUNTABILITY AND DEMONSTRATING COMPLIANCE

3.1 The Council is accountable for and must be able to demonstrate compliance with the Data Protection Legislation.

### Roles and Responsibilities

3.2 The Council allocates the following roles and responsibilities:

SENIOR INFORMATION RISK OWNER (SIRO) – to ensure information assets and risks with the Council are managed as a business, actively work with the Data Protection Officer and other experts within or outside the Council to determine the most effective and proportionate information control measure. The SIRO is responsible for building an informed culture within the Council to promote the best practice for the use and protection of Information assets. The SIRO is responsible for implementing current Data Protection Legislation on behalf of the Council (the Data Controller).

SINGLE POINT OF CONTACT FOR CONTROLLER (SPoC) – to act as single point of contact for customers, staff and the Data Protection Officer in relation to Personal Data. Support the SIRO in ensuring the Council can demonstrate compliance with current Data Protection Legislation.

DATA PROTECTION OFFICER (DPO) – to undertake the statutory role by monitoring compliance and by providing training, advice and assistance to the SIRO.

INFORMATION ASSET OWNERS – Service managers have been nominated as Information Asset Owners for the information held within their service areas and are responsible for ensuring that their services area can demonstrate compliance with current Data Protection Legislation.

STAFF – all staff are responsible for ensuring that the Personal Data they handle is processed in accordance with this Policy and current Data Protection Legislation.

MEMBERS - all members are responsible for ensuring that the Personal Data they handle when acting as a member of the Council is processed in accordance with this Policy and current Data Protection Legislation.

### Demonstrating Compliance

3.3 The Council must be able to demonstrate to its customer, supplier, staff, members and the Information Commissioner that it is compliant with current Data Protection Legislation.

3.4 Examples of how the Council will do this:

- holding a list of processing and keep it up to date (kept by the SIRO)
- minimising the Personal Data collected (Information Asset Owners)
- having and complying with its retention schedules (Information Asset Owners)
- being open and transparent and tell people what we are doing with their data (SIRO)
- checking any Processors are Data Protection Legislation compliant and have written processing agreements and written data sharing agreements in place (Information Asset Owners)
- carrying out privacy by design and privacy impact assessments where necessary (Information Asset Owners)
- ensuring it has appropriate technical and organisational security (SIRO)
- regularly review and update it policies and procedures (SIRO)

3.5 The Council will pay the fee due to the Information Commissioner on an annual basis (SIRO).

## SECTION 4 – ORGANISATIONAL SECURITY

### Security

4.1 The Council will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks arising from the processing of Personal Data.

4.2 Security shall be applied to all stages of processing to prevent unauthorised access, disclosure (internal or external), loss, damage (accidental or deliberate), or unauthorised alteration.

4.3 Examples of security measures are:

- Personal Data must not be left on display or unsecured when unattended
- System entry passwords shall be kept secure and be changed regularly and not shared
- All emails and documents must be classified in accordance with the Governments Document Classification scheme. Government Security Classifications- Guidance

4.4 The SIRO will undertake a regular review of security measures and an audit shall be made of the way Personal Data is managed. This will include an assessment of the methods of handling Personal Data and processing carried out by a third party on behalf of the Council or jointly with other local authorities shall be subject to a written contract, which stipulates compliance with the data protection principles.

**Privacy by design**

4.5 Privacy by design means that privacy and data protection is a key consideration in the early stages of any project and throughout its lifecycle.

4.6 Where the Council changes the way it processes Personal Data or purchases a new or upgrades an IT system that processes large amounts of Personal Data, the Council will carry out a Privacy Impact Assessment in accordance with the current Data Protection Legislation and Information Commissioner guidance and ensure that privacy by design is built in the processing.

4.7 Examples of when privacy by design should be considered:

- building, developing or purchasing a new IT systems for storing or accessing Personal Data;
- developing policy, procedures or strategies that have privacy implications;
- embarking on a data sharing initiative; or
- using Personal Data for new purposes.

4.8 The Privacy Impact Assessment form is available here

4.9 Copies of the Privacy Impact Assessments carried out will be held by the SIRO and available for inspection by the Data Protection Officer.

**Storing Personal Data**

4.10 The fifth data protection principle requires that Personal Data should not to be kept longer than necessary for the purpose for which it is processed. It is the responsibility of the Information Asset Owner to ensure that Personal Data is used and stored properly to prevent any unauthorised access and ensure that a retention schedule is in place for the Personal Data used within their service area and ensure staff comply with that retention schedule.

4.11 Personal Data should:

- be stored in locked desks or filing cabinets
- be securely protected on computers using industry standards authentication methodologies and limited access
- not be visible on screens by unauthorised persons (including other members of staff)
- not be taken out of the Council offices or stored externally unless such use or storage is necessary and authorised by a line manager or Information Asset Owner.
- only be kept for as long as is necessary and disposed of securely when it is no longer needed. It should be reviewed regularly and deleted promptly when no longer needed

4.12 Special Categories of Data should be kept secure and subject to very limited access.

4.13 Duplicate records should be kept to a minimum to reduce the risk of unauthorised access or loss and to avoid anomalies in Personal Data being kept longer than is necessary.

4.14 Portable storage devices such as handheld devices, mobile phones and laptops must be encrypted; they should not be left unattended and should be locked away when not in use.

**Protective Marking**

4.15 The protective marking scheme supplied by the Government Protective Marking Scheme (GPMS) provides a framework for users to share and protect information.

## SECTION 5 – HANDLING PERSONAL DATA

**Collecting Personal Data/information**

5.1 The Council will only collect Personal Data that is necessary to carry out the purpose for which it was collected. Staff will not collect Personal Data on the grounds that it might come in useful. Extra care will be taken when collecting or using Special Categories of Data and will only be collected where absolutely necessary.

5.2 When collecting Personal Data the Information Asset Owner will ensure that the person is told what will be done with their Personal Data at the time it is collected This must be conveyed in a concise, transparent, intelligible, easily accessible way, and use clear and plain language.

5.3 The Council will provide individuals with all the following privacy information:

- The contact details of the Council
- The contact details of the Council's SpoC.
- The contact details of the Council's Data Protection Officer
- The purposes of the processing
- The lawful basis for the processing
- The legitimate interests for the processing (if applicable).
- The categories of Data Subjects and Personal Data obtained
- The recipients or categories of recipients of the Personal Data
- Details of the use of profiling
- The categories of transfers of the Personal Data to any third countries or international organisations (if applicable)
- Where possible, a general description of the Council's technical and organisational security measures
- The retention periods for the Personal Data.
- The rights available to individuals in respect of the processing.
- The right to withdraw consent (if applicable).
- The right to lodge a complaint with the ICO.
- The source of the Personal Data (if the Personal Data is not obtained from the individual it relates to)
- The details of whether individuals are under a statutory or contractual obligation to provide the Personal Data (if applicable, and if the Personal Data is collected from the individual it relates to).
- The details of the existence of automated decision-making, including profiling (if applicable).

5.4 All staff will inform their line manager or Information Asset Owner if Personal Data is collected or used in a new or different way so that this can be added to the list of processing held by the SIRO.

**Using Personal Data**

5.5 When processing Personal Data, the first data protection principle requires that it must be done lawfully and in a fair and transparent manner. Personal Data is considered to be lawfully processed if one of the following conditions apply:

- The Data Subject has given their consent to the processing
- The processing is necessary for:
  - the performance of a contract to which the Data Subject is a party
  - the compliance with any legal obligation of the Council as a Data Controller
  - the protection the vital interests of the Data Subject. This means a life or death situation
  - the exercise of a function conferred on the Council by law
  - for the exercise of any other function of a public nature exercised in the public interest by the Council
  - for the purposes of legitimate interests of the Council subject to the legitimate rights and freedoms of the Data Subject.

5.6 When processing Special Categories of Data a further processing condition set out in the Data Protection Legislation is required.

5.7 The second data protection principle requires that Personal Data should only be used for the purpose(s) for which it is collected and not for any incompatible purpose. If it is to be used for any other purpose then the individual concerned must be informed and there must be a legal basis for processing the Personal Data for the other purpose.

**Disclosing Personal Data**

5.8 Before disclosing Personal Data staff must ensure that they are speaking to the Data Subject or that they have the Subject's consent to release it to a third party acting on their behalf. If the person is present with the third party and staff are satisfied that it is the correct person and they provide verbal consent, a record of the circumstances of the situation shall be kept at the time of releasing the information. In any other circumstance written consent of the Data Subject is required.

5.9 In some cases staff may be asked to provide information by law. It is the responsibility of staff to ensure that there is a sound basis for releasing that Personal Data. Personal Data must not be disclosed until staff are satisfied it is lawful to do so. The Data Protection Legislation may give the person the right to ask for the information but staff may not be under a legal obligation to release that information. Do not disclose any Personal Data until you are satisfied it is lawful to do so.

5.10 Disclosure may be necessary to protect the vital interests of the Data Subject for example to prevent serious harm, or in a life or death situation. Do not disclose any Personal Data until satisfied it is lawful to do so.

5.11 Obtain legal advice if you are unsure.

**Disclosing Personal Data to Members**

5.12 Before releasing information to elected Members, staff need to ascertain for what purpose the Member is requesting the information. Elected Members have up to 3 roles:

1. **Acting as a Member**

   Members have the same rights of access to Personal Data as staff when acting in this role. Staff should ensure that Members need the Personal Data to carry out their official duties and when releasing the information should specify the purpose(s) for which the Personal Data may be used or disclosed.

2. **Acting on behalf of local residents**

   Staff do not, generally, need to obtain the individuals consent to disclose their Personal Data to a Member if:

   - The Member represents the ward in which the individual lives; and
   - The Member makes it clear that they are representing the individual when requesting the Personal Data; and
   - The information is necessary to respond to the individual's complaint or requests

   Otherwise, Members must obtain consent from the Data Subject before any Personal Data is released.

3. **Acting for political purposes**

   Personal Data should not be released for political purposes without the individual's consent. Exceptions to this:

   Personal Data which the Council is required by law to make public for that purpose.

   Personal Data presented in a form which does not identify any living individuals, for example statistical information or Council tax band information and any other information that cannot be linked to the individual concerned, for example by comparing data to the electoral register.

**Disposal of Personal Data**

5.13 Personal Data must be disposed of securely.

5.14 **Paper records** must be shredded. If an outside company is used they must be Data Protection compliant and a certificate of shredding must be obtained when the information is shredded.

5.15 **Electronic records** must be removed permanently. Just because it is not visible on the screen does not mean it is not still recoverable.

5.16 Information Asset Owners are responsible for ensuring staff follow their retention schedule when disposing of Personal Data.

**Dealing with Data Subject Requests**

5.17 Individuals (Data Subjects) have rights over their Personal Data held by the

Council on computer and paper records.

5.18 Data Subjects are entitled

- To know what information is being processed and why
- To have information about them erased (be forgotten)
- To object to direct marketing and automated decisions
- To be told about automated profiling
- To obtain information about decision making
- To data portability – consent or contract

- To have information about them rectified – if inaccurate
- To the right to restrict or object to processing – inaccurate/unlawful
- To the right to withdraw consent

5.18 The Council shall respond to Data Subject request as soon as possible and at the latest within one month.

5.19 In certain circumstance the Council may charge a reasonable fee or refuse a Data Subject Request where it is manifestly unfounded, excessive or repetitive.

5.20 Data Subject request forms are available on the Council's website.

**Data Protection breaches**

5.21 Any **breach of security** leading to or which is likely to lead to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed must be reported to your line manager or the Information Asset Owner immediately and the process for breach reporting in the Information Security Policy followed.

5.22 The Information Security Form available here will be completed by the Information Asset Owner and sent to SIRO. The SIRO in consultation with the Data Protection Officer shall report breaches to the Information Commissioner within 72 hours in accordance with current Data Protection Legislation and any guidance issued by the Information Commissioner or Article 29 Working Party.

5.23 Copies of Incident Breach report forms will be held centrally by the SIRO.

## SECTION SIX – SHARING PERSONAL DATA AND PROCESSING OF PERSONAL DATA BY THIRD PARTIES

6.1 To share Personal Data and/or Special Categories of Data for another purpose it must be done lawfully.

**Internal one off requests for Personal Data**

6.2 Staff requesting Personal Data must do so in writing and demonstrate that the Personal Data is necessary and that the sharing is lawful. Staff receiving requests must be satisfied that the sharing is lawful before any Personal Data can be released. A record of the Personal Data released, together with the legal basis for sharing, shall be kept by the Information Asset Owner to demonstrate compliance with the Data Protection Legislation.

**Regular or bulk transfers of Personal Data and Special Categories of Data**

6.3 In many instances the Council shares data with other internal departments and external organisations on a regular basis. For instance, the Council's shares Personal data with third party services providers, the Police or other councils as part of a joint initiative such as Domestic Violence and Homelessness.

6.4 Although there may be a statutory requirement placed on the Council to transfer data, the Council is the Controller and is responsible for demonstrating compliance with Data Protection Legislation. It is the responsibility of the Information Asset Owners to ensure that appropriate data processing and/ or sharing agreements are in place.

6.5 The Council recommends all staff read the Information Commissioners Office advice and guidance to ensure they comply with legislation.

Data sharing - code of practice and checklist.

If you require assistance please contact One Legal email: legalservices@tewkesbury.gov.uk

6.7 Information Asset Owners will be responsible for ensuring copies of the data sharing/processing agreement are sent to the SIRO and are regularly reviewed and kept up to date.

Copies of Data Sharing and Processing agreements will be held by the SIRO.

## SECTION SEVEN – SPECIFIC USES

**Processing of Criminal Convictions**

7.1 Processing of Personal Data relating to criminal convictions and offences or related security measures shall be carried out only under the control of official authority or when the processing is authorised by UK law providing for appropriate safeguards for the rights and freedoms of data subjects.

**Law enforcement processing**

**CCTV systems and Data**

7.2 The Council CCTV policy states that any system operator (Service Manager) who has the responsibility for a CCTV scheme must have a scheme specific Code of Practice in place before it becomes operational or within 6 months of the approval of this Policy.

7.3 This Code of Practice will provide the guidance for complying with the requirements of the Data Protection Legislation in respect of the use and operation of these systems.

7.4 The current CCTV codes of practice are available on the Councils website.

**Direct Marketing**

7.5 The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) deals with direct marketing.

7.6 Electronic communications mean any information sent between particular parties over a phone line or internet connection. This includes phone calls, faxes, text messages, video messages, emails and internet messaging. It does not include generally available information such as the content of web pages or broadcast programming.

7.7 Direct Marketing means the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals.

7.8 Genuine market research does not count as direct marketing. However, if a survey includes any promotional material or collects details to use in future marketing campaigns, the survey is for direct marketing purposes and the rules apply.

7.9 PECR cover marketing by phone, fax, email, text or any other type of 'electronic mail'.

7.10 There are different rules for live calls, automated calls, faxes, and electronic mail (this includes emails or texts).

7.11 PECR marketing provisions do not apply to other types of marketing, such as mailshots or online advertising. However, staff must always still comply with the Data Protection Legislation and if online advertising is proposed uses cookies or similar technologies, the provisions about cookies under PECR may apply.

7.12 Most of the rules in PECR only apply to unsolicited marketing messages. They do not restrict solicited marketing. - a solicited message is one that is actively requested. An unsolicited message is any message that has not been specifically requested. So even if the customer has consented to receiving marketing from the Council, it still counts as unsolicited marketing.

7.13 This does not make all unsolicited marketing unlawful. The Council can still send unsolicited marketing messages – as long as it is in compliance with PECR.

7.14 For most Direct Marketing consent will be required. Consent must be knowingly and freely given, clear and specific. A clear records of what a person has consented to, and when and how consent was obtained must be retained. This will enable the Council to demonstrate compliance in the event of a complaint.

7.15 If the Council employs someone else to actually make the calls or send the messages, the Council is still responsible, as the Council is 'instigating' those calls or messages.

7.16 The rules on Direct Marketing to Individuals are stricter than those to businesses.

7.17 Any Direct Marketing made or sent by electronic means must be made or sent in accordance with PECR. Staff must check with the fax and or telephone preference service before making any Direct Marketing calls and not make calls to those numbers on the preference service.

**Data Sharing for public service delivery, debt recovery and fraud investigations**

7.18 Information Asset Owners will be responsible for ensuring copies of the data sharing/processing agreement are sent to the SIRO and are regularly reviewed and kept up to date.

Copies of Data Sharing and Processing agreements will be held by the SIRO.

## SECTION EIGHT – MONITORING AND REVIEW

8.1 The Data Protection Officer will monitor this Policy on an annual basis.

8.2 The SIRO will review this Policy on a regular basis taking into account the advice of the Data Protection Officer.

## DEFINITIONS

| | |
|---|---|
| Controller | The person(s) who determines how and the manner in which Personal Data are or are to be processed (the Council). |
| Processor | The person who processes the data on behalf of the data controller. |
| Data Subject | The person who the Personal Data is about. |
| Personal Data | Any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. |
| Special Categories of Data | Information relating to the racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation |
| Processing data | Includes collecting, recording, use, organising, structuring, storing, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction |
| Data Protection Legislation | (i) The General Data Protection Regulation (Regulation EU 2016/679), the Law Enforcement Directive (Directive EU 2016/680) The Privacy and Electronic Communications (EC Directive) Regulations 2003, Digital Economy Act 2017 and any applicable national implementing Laws as amended from time to time, (ii) The Data Protection Act 2018 subject to Royal Assent to the extent that it relates to Processing of Personal Data and privacy, (iii) all applicable Laws relating to Personal Data and privacy |