Data protection **policy**

March 2023

Tewkesbury
Borough Council

Contents

Section one: Introduction

Tewkesbury Borough Council (the council) is committed to safeguarding the personal data that it collects and processes, and to ensuring that it is used only in ways that people would reasonably expect.

In delivering our services, we collect, store and process personal data about our citizens, service users, employees, suppliers and other third parties. In most cases, this information is held digitally, but also includes information that we hold physically on paper.

We recognise that the correct and lawful treatment of this data maintains trust and confidence in the organisation and provides for successful service delivery.

This policy therefore sets out how the council will fulfil its duties regarding the protection of personal data.

Section two - Policy objectives

2.1 Policy objectives

- To comply with all relevant legislation and good practice in order 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 ensure that staff are able to recognise personal data.
- To provide staff with appropriate procedures and training to handle and process 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.

2.2 Staff and Member responsibility

It is the duty of individual staff and Members to ensure that personal data held by the council is handled and processed 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 three - Data protection legislation

What is personal data

The UK General Data Protection Regulation (GDPR) defines personal data as any information relating to an identified or identifiable natural person (data subject) who can be identified, directly or indirectly, in particular by reference to an identifier such as:

- A name.
- An identification number.
- Location/ address data.
- Online identifier.
- Health information.
- Income.
- Cultural profile.

Special category data (sensitive personal data)

Special category data is personal data that needs more protection because of its sensitive nature. The processing of this data creates more significant risks to a person's fundamental rights and freedoms and as such it is subject to a stricter set of conditions. This includes information such as:

- Racial or ethnic origin.
- Political opinions.
- Religious beliefs.
- Trade Union membership.
- Physical or mental health.
- Sexual orientation or sex life.
- Criminal proceeding or convictions.
- Genetic data.
- Biometric data.

3.1 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.

3.2 This policy is applicable to all data protection legislation relating to the use of personal data. This includes, but is not limited to:

- Data Protection Act 2018.
- UK General Data Protection Regulation (GDPR).
- Freedom of Information Act 2000.
- Environmental Information Regulations 2004.

3.3 The council processes and keeps personal data about data subjects to enable it to conduct council business, provide services and to employ staff.

3.4 The data protection principles

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 fourth 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 four – Accountability and demonstrating compliance

Training and awareness

Regular data protection training is mandatory for all council staff and Members. The training provided is aimed to ensure that all individuals understand their responsibilities for managing data in line with legislation.

4.1 The council is accountable for and must be able to demonstrate compliance with the data protection legislation.

Roles and responsibilities

4.2 The council allocates the following roles and responsibilities:

SENIOR INFORMATION RISK OWNER (SIRO) – to ensure information assets and risks within 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.

Governance

4.3 Compliance with this policy and the related legislation is monitored by the council's Information Governance and Security Board. The board also ensures that information and security risks are properly assessed and mitigated and that data protection procedures are applied consistently across the authority.

4.4 Examples of how the council will do this:

- Holding a list of processing and keeping 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 telling people what we are doing with their data (SIRO).
- Checking that 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 that it has appropriate technical and organisational security (SIRO).
- Regularly review and update it policies and procedures (SIRO).

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

Section five - Organisational security

Security

5.1 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.

5.2 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.

5.3 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.
- Authorised users will only have access to personal data where access is essential to their duties.

- The secure disposal of paper and electronic data.
- Internal procedures must be followed in relation to the disclosure of any personal data.

5.4 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

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

5.6 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.

5.7 Examples of when privacy by design should be considered:

- Building, developing or purchasing new IT systems for storing or accessing personal data.
- Developing policy, procedures or strategies that have privacy implications.
- Embarking on a data sharing initiative.
- Using personal data for new purposes.

5.8 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

5.9 The fifth data protection principle requires that personal data should not 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.

5.10 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.

5.11 Special categories of data should be kept secure and subject to very limited access.

5.12 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.

5.13 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

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

Section six - Handling personal data

Collecting personal data/information

6.1 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.

6.2 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.

6.3 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 world 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).

6.4 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

6.5 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.

6.6 When processing Special Categories of Data a further processing condition set out in the data protection legislation is required. (See section three of this policy).

6.7 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

6.8 The disclosure of personal data must be processed through the council's data request procedure. This ensures that appropriate verification checks are carried out and we can be satisfied that the information is being disclosed to the correct person, or where it is being disclosed to a third party, that they have the authority to receive the information.

6.9 In some cases staff may be asked to provide information by law. It is the responsibility of staff to ensure that any requests for personal data are directed through the council's data request procedure. The data protection legislation may give the person the right to ask for the information but we may not be under a legal obligation to release that information. Personal data must not be disclosed outside of the data request procedure unless a specific data sharing agreement is in place.

6.10 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.

6.11 Obtain legal advice if you are unsure.

Disclosing personal data to Members

6.12 Before releasing information to elected Members, staff need to ascertain for what purpose the Member is requesting the information. Elected Members have up to three 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

6.13 Personal data must be disposed of securely.

6.14 **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.

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

6.16 Information Asset Owners are responsible for ensuring that staff follow their retention schedule when disposing of personal data.

Dealing with data subject requests

6.17 Individuals (data subjects) have rights over their personal data held by the council on computer and paper records.

6.18 Data subjects are entitled to:

- Know what information is being processed and why.
- Have information about them erased (be forgotten).
- Object to direct marketing and automated decisions.
- Be told about automated profiling.
- Obtain information about decision making.
- Data portability – consent or contract.
- Have information about them rectified – if inaccurate.
- The right to restrict or object to processing – inaccurate/unlawful.
- The right to withdraw consent.

The council will respond to a data subject request without undue delay and at the latest within one calendar month of receipt. Where we require proof of the data subject's identity, the timescale for responding will not begin until the requested information has been received. In certain circumstances where requests are complex, it may be possible to extend the time to respond by a further two months.

6.19 In certain circumstance the council may charge a reasonable fee or refuse a data subject request where it is manifestly unfounded, excessive or repetitive.

6.20 Data subject requests should be logged via the self service portal on the council website or made in writing and posted to the council offices.

Data protection breaches

6.21 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.

6.22 In all cases a data breach incident form will be completed by the Information Asset Owner and sent to the SPoC. Where these are assessed as low risk they will be reported internally to the Information Governance and Security Board. Where they are reported as high risk, 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.

Section seven - Sharing persona data and processing of personal data by third parties

Data transfers

The council will only transfer any personal data we hold to a third party outside the UK, if the country to which the personal data is transferred ensures an adequate level of protection for the data subjects' rights and freedoms, or if an appropriate safeguard is in place between the council and the third party.

7.1 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

7.2 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

7.3 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.

7.4 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.

7.5 The council recommends that all staff read the Information Commissioners Office advice and guidance to ensure that they comply with legislation.

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

7.6 Information Asset Owners will be responsible for ensuring that 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 - Specific uses

Processing of criminal convictions

8.1 Under data protection legislation there are specific rules regarding the processing of personal data relating to criminal convictions and offences. This includes:

- Criminal activity.
- Allegations.
- Investigations.
- Proceedings.

Such data will only be processed by the council where we have official authority i.e we have a public sector task laid down by law, or where the processing is authorised by law. This means that we must meet one of the conditions set out in Schedule 1 of the Data Protection Act 2018. Advice should be sought from One Legal to determine if these conditions are met

Law enforcement processing

CCTV systems and data

8.2 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 six months of the approval of this policy.

8.3 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.

8.4 The current CCTV codes of practice are available on the council's website.

Direct marketing

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

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.

The council will not participate in direct marketing practices without:

- Explicit consent from the data subject, or
- A legitimate interest reason

All individuals must be given the opportunity to opt-in to receive material at the point of data collection.

Even where legitimate interests or explicit consent has been established, all correspondence must include opt-out options.

Data sharing for public service delivery, debt recovery and fraud investigations

8.6 Information Asset Owners will be responsible for ensuring that 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 nine - Complaints about data protecton matter

Where a complaint is made alleging that the council has not complied with the statutory rights of a data subject, an investigation or review will be carried out by the SPoC, in conjunction with the Data Protection Officer.

Any complainant who is dissatisfied with the outcome or the manner in which their complaint was handled, may make a complaint under the council's formal complaints policy.

Complainants will also be made aware of their right to complain to the Information Commissioners Office (ICO).

Section ten - Monitoring and review

10.1 The Data Protection Officer will monitor this policy on an annual basis.

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

Definitions	
Controller	The person who determines the manner in which personal data is held and processed by the council.
Processor	The person who processes the data on behalf of the data controller.
Data subject	The person/ individual to whom the data relates.
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 UK General Data Protection Regulation (Regulation EU 016/679), 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.
Identifiers	Information that can distinguish an individual from other individuals, such as a name, identification number, location data or online identifier e.g. IP address.

Produced by Tewkesbury Borough Council. 2023