



EARLEY TOWN COUNCIL

DATA PROTECTION POLICY

Introduction

This policy demonstrates how the Council will comply with the Data Protection Act 2018 (DPA) and UK General Data Protection Regulations (GDPR) to ensure that personal data is processed correctly.

This policy applies to members of staff, councillors, suppliers, contractors or anyone acting on the Council's behalf and should be read in conjunction with the Council's:

- General Privacy Notice
- Information Security Policy
- Information Breach Policy
- Retention of Records & Disposal policy
- Subject Access Request Policy
- Freedom of Information & Environmental Information Regulations guidance.

Our Commitment

The processing of personal information is important to us, and the Council understands the importance of ensuring that personal data, including sensitive personal data is always treated lawfully and appropriately and that the rights of individuals are upheld.

The Council will only collect, use and hold personal data about individuals for the purposes of carrying out its statutory obligations, delivering services and meeting the needs of individuals.

This includes service users, members of the public, current, past and prospective employees, councillors, stakeholders, other local authorities, public bodies or law enforcement agencies.

Data Protection Principles

There are 7 principles set out in the Data Protection Act 2018, that personal data is:

- used fairly, lawfully and transparently.
- used for specified, explicit purposes.
- used in a way that is adequate, relevant and limited to only what is necessary.
- kept accurate and, where necessary, kept up to date.
- kept for no longer than is necessary.
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.
- kept in compliance with other principles of data protection to ensure accountability.

The DPA and GDPR set out differences between 'personal data' and 'special category personal data'.

Personal data is information which can identify a person such as: -

- name
- address
- email address
- date of birth
- IP address
- bank details
- employment details
- photos

There is also protection for more sensitive personal data such as:

- race or ethnic origin
- political opinions
- religious or other beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or sexual orientation

The DPA and GDPR do not include information about criminal allegations, proceedings or convictions as special category data, as there are other safeguarding measures for personal data relating to criminal convictions and offences.

Our Objectives

In order to comply with the requirements of the Data Protection Act 2018, the Council will ensure that:

- Personal data is collected, used and held lawfully and for the purpose it is intended.
- When personal data is collected, individuals are made aware that their information is being collected, the purpose for collecting the data and whether it will be shared with any third parties. This will be done using privacy notices.
- Any data sharing with external partners and other relevant agencies will be subject to information sharing agreements and will only be entered into with third party under a duty of confidentiality and they will be obliged to implement appropriate measures to ensure data security.
- External agencies undertaking any data processing on behalf of the Council will be required to demonstrate compliance with the Data Protection Act 2018 and will require measures to be in place to protect personal data.
- Staff are aware of their responsibilities when processing personal information.
- Training is provided to ensure that those handling personal data are trained appropriately.
- Subject Access rights can be fully exercised and will be dealt with promptly.
- Any new projects being implemented that involve personal data to be subject to a Data Protection Impact Assessment (DPIA).
- A review and update of this policy, procedures and guidance for staff and councillors is carried out on a regular basis.

Meeting our Objectives

In order to meet our objectives, the Council will ensure that appropriate controls and procedures are in place to ensure compliance with the Data Protection Act 2018 and General Data Protection Regulations.

Legal Requirements

The Council may be required by law to share or make available some of the personal data we collect and hold. This information may be shared for a number of reasons such as to safeguard public funds and for the prevention and detection of fraud, and for the prevention and detection of crime.

The Council will fully comply with the requirements of the Data Protection Act 2018 and other legislation, policies and guidance such as the Freedom of Information Act 2000, etc.

The Council is registered as a data controller with the Information Commissioner's Office. Our registration number is Z7740800.

Data Controller

Earley Town Council is the Data Controller for personal data relating to staff, councillors, customers, suppliers, contractors and other individuals and external bodies.

External agencies/companies processing personal data on behalf of the Council will have to demonstrate by written agreement that personal information will be handled in compliance with the DPA and GDPR.

Data Protection Officer

The Council is not required to appoint a Data Protection Officer, however the Deputy Town Clerk acts as a point of contact for any queries in relation to Data Protection and GDPR. The overall responsibility to ensure compliance with legislation is that of the Town Clerk.

Data Security

The Council must ensure the security of personal data and have relevant measures in place. All staff and councillors must comply with the Council's Information Security Policy.

The Council must protect personal data against:

- Unauthorised access.
- Unauthorised or unlawful processing.
- Accidental loss, destruction or damage.

This will be achieved by:

- acting legally when collecting, storing and processing data in accordance with this policy and the Council's data privacy notices.
- reporting any suspected data breaches to the Town Clerk and Deputy Town Clerk, who will notify the Information Commissioner's Office, as required.
- using appropriate levels of security to store or share personal data.

- carrying out a Data Protection Impact Assessment (DPIA) when undertaking new projects involving personal data, to assess any potential privacy risks.

An Information Asset Register will be maintained by the Town Clerk & Deputy Town Clerk identifying:

- all personal data held.
- where it is held.
- how it is processed.
- who has access to it.

Data Breaches

The Council will take reasonable measures to ensure that personal data is not compromised, and Data Breaches will be investigated in accordance with the Council's Information Breach Policy.

Data Sharing

Personal data will not be shared with a third-party organisation without a valid reason and where required, an individual will be notified that sharing will take place in the form of a privacy notice. If any new purposes for data sharing are to take place, consent from the individuals concerned must be obtained.

When personal data is to be shared regularly with a third party, a Data Sharing Agreement must be implemented.

Any data sharing will also take into consideration:

- the statutory basis of the proposed information sharing.
- whether the sharing is justified.
- how to ensure the security of the information being shared.

If the Council transfers personal data to a country or territory outside the UK, the Council will comply with data protection law.

The Council may be required to share personal data with emergency services and local authorities in response to an emergency situation that affects staff or councillors.

The Council will share personal data with law enforcement or government agencies where legally required to do so, including: -

- prevention/detection of a crime
- apprehension/prosecution of an offender
- assessment/calculation of tax owed to HMRC
- legal proceedings
- safeguarding obligations

Data Access

Staff and councillors will have access to personal data only where it is a requirement of their role.

An individual has a right to make a request about the personal data held on them and these rights are:

- The right to be informed.
- The right of access.
- The right to rectification
- The right to restrict.
- The right to erasure.
- The right to object
- The right to portability.
- The right to not be subject to automated decision-making

However, in accordance with the UK's GDPR, exemptions and restrictions can be legitimately applied in some circumstances, to exempt or qualify the exercise of an individuals' rights.

The Council will ensure that any requests regarding personal data are processed in accordance with its Subject Access Request Policy.

Retention of data

The Council will only keep data for as long as it is necessary to do so, in accordance with its Retention of Records & Disposal Policy and Retention Schedule. Some data may be retained or kept permanently, in accordance with legal requirements. The destruction of data will be carried out securely.

CCTV

The use of CCTV will be carried out in accordance with the Information Commissioner's Office guidance. Signage will be clearly visible where there are CCTV cameras to inform individuals that CCTV is in operation. The management of CCTV use will follow the Council's CCTV Policy.

Training & Awareness

Staff and councillors will undertake GDPR training to ensure that they understand their responsibilities when handling and processing personal data.

Compliance with this Policy

This Policy applies to all council staff, councillors and all individuals or organisations acting on behalf of the council.

Date of policy: 27th July 2022

Date of last adoption: 9th September 2026

Next review date: July 2028