UCKFIELD TOWN COUNCIL

DATA PROTECTION POLICY

Policy Number 87		
Issue No.	**Date completed**	**Details of amendments**
1.	June 2026	Ratification at Full Council – 29.06.26

1.0 Introduction

1.1 Uckfield Town Council is committed to protecting the privacy and security of personal information held about residents, service users, councillors, employees, volunteers, contractors and other individuals.

1.2 The Council recognises that the lawful and responsible handling of personal data is essential to maintaining public confidence and meeting its legal obligations.

1.3 This policy sets out the Council's approach to data protection and explains how personal information must be collected, used, stored, shared and disposed of.

1.4 This policy has been developed to support compliance with:

- The UK General Data Protection Regulation (UK GDPR);
- The Data Protection Act 2018;
- Other relevant legislation relating to confidentiality and information governance.

2.0 Scope

2.1 This policy applies to:

- Councillors;
- Employees (full time and part-time);
- Volunteers;
- Contractors;
- Temporary workers;
- Anyone acting on behalf of the Council who accesses or processes personal data.

2.2 It applies to personal information held in any format, including:

- Electronic records;
- Emails;
- Computer systems;
- Mobile devices;
- Paper files;
- Meeting records;
- Photographs;
- CCTV recordings;
- Audio or video recordings.

3.0 What is Personal Data?

3.1 Personal data is any information relating to an identifiable living individual.

Examples include:

- Name;
- Address;
- Telephone number;
- Email address;
- Photographs;

- Financial information;
- Employment information;
- Records relating to Council services.

3.2 Consideration also has to be given to consider whether the Town Council holds any categories of personal data, known as sensitive personal data, which require additional protection, including information relating to:

- Health;
- Disability;
- Ethnic origin;
- Religious beliefs;
- Trade union membership;
- Criminal convictions;
- Biometric or genetic information.

3.3 Sensitive data will only be processed where there is a lawful basis and appropriate safeguards are in place. Uckfield Town Council has no reason to process this level of data for its customers or residents. The only data held of this nature would such as health records for employees.

4.0 Data Protection Principles

The Town Council will ensure that personal data is:

4.1 Lawfully, fairly and transparently processed
Individuals will be informed about how their information is used and the Council will only process information where there is a lawful basis.

4.2 Collected for specific purposes
Personal information will only be collected for clear, legitimate purposes and will not be used in ways incompatible with those purposes.

4.3 Adequate, relevant and limited
The Council will only collect information necessary for the purpose required.

4.4 Accurate
The Council will take reasonable steps to ensure information is accurate and kept up to date.

4.5 Retained only as long as necessary
Information will only be kept for as long as required by legislation, operational needs or the Council's retention schedule.

4.6 Securely processed
Appropriate technical and organisational measures will be used to protect information from:

- Unauthorised access;
- Loss;
- Damage;
- Accidental disclosure;
- Unlawful processing.

4.7 Accountability

The Council will maintain appropriate records and procedures to demonstrate compliance with data protection legislation.

5.0 Lawful Basis for Processing Information

5.1 The Council may process personal data where one or more of the following applies:

- It is necessary to comply with a legal obligation;
- It is necessary to perform a public task or exercise official authority;
- It is necessary for a contract;
- Consent has been provided;
- It is necessary to protect an individual's vital interests;
- It is necessary for legitimate interests where appropriate.

5.2 Where consent is relied upon, individuals will be informed that they may withdraw consent at any time.

6.0 How the Council Uses Personal Data

6.1 The Council may use personal information to:

- Deliver Council services;
- Respond to enquiries;
- Manage bookings, facilities and events;
- Maintain accounts and records;
- Process payments;
- Manage grants;
- Communicate Council information;
- Meet statutory obligations;
- Support safeguarding responsibilities;
- Prevent fraud and misuse of public funds;
- Monitor and improve services;
- Maintain accurate records.

7.0 Responsibilities

7.1 The Chief Officer (Town Clerk) /Data Protection Lead

The Town Clerk is responsible for ensuring appropriate data protection arrangements are maintained.

Responsibilities include:

- Advising the Council on data protection matters;
- Maintaining policies and procedures;
- Ensuring compliance monitoring takes place;
- Maintaining records of processing activities where required;
- Arranging appropriate training;
- Managing data breaches;
- Supporting responses to information requests.

7.2 Councillors and Staff

All councillors and staff must:

- Handle personal information responsibly;
- Follow this policy and related procedures;
- Keep information secure;
- Only access information required for their role;
- Report concerns, losses or breaches immediately;
- Avoid unauthorised disclosure.

7.3 Managers and Supervisors

Managers must ensure:

- Staff handling personal information understand their responsibilities;
- Appropriate training is provided;
- Contractors and volunteers understand confidentiality requirements;
- Information is managed securely.

8.0 Information Security

8.1 The Council will use appropriate safeguards including:

- Password protection;
- Secure storage systems;
- Access controls;
- Secure disposal arrangements;
- Appropriate backup systems;
- Confidentiality procedures.

8.2 Paper records must be:

- Stored securely;
- Protected from unauthorised access;
- Removed from public view;
- Destroyed securely when no longer required.

9.0 Email and Electronic Communication

9.1 Care must be taken when sending emails containing personal information. Staff and councillors must:

- Check recipients' details before sending;
- Avoid forwarding information unnecessarily;
- Use secure methods when sharing sensitive information;
- Not disclose personal information without authority.

9.2 Personal information received through Council email accounts must not be forwarded externally without appropriate authorisation.

10.0 Sharing Personal Information

10.1 The Council may share information where necessary and lawful.
Information may be shared with:

- Other public authorities;
- Contractors and suppliers;
- Service providers;
- Partner organisations;
- Legal or regulatory bodies.

10.2 Where information is shared with external organisations, appropriate agreements and safeguards must be in place.

10.3 Personal information will never be sold.

11.0 Retention and Disposal

11.1 The Council will retain information in accordance with the Town Council's Retention Policy.

11.2 Information will be securely destroyed when:

- It is no longer required;
- The retention period has expired;
- There is no legal reason to retain it.

11.3 Confidential waste, including handwritten notes containing personal information, must be securely destroyed.

12.0 Individuals' Rights

Individuals have rights under data protection legislation, including:

12.1 Right to be informed
Individuals have the right to understand how their information is used.

12.2 Right of access
Individuals may request copies of personal information held about them.
This is referred to as a Subject Access Request. Details can be found on the Town Council website,
https://www.uckfieldtc.gov.uk/your-council/transparency-on-spend/data-protection-and-privacy/

12.3 Right to rectification
Individuals may request correction of inaccurate information.

12.4 Right to remove
Individuals may request deletion of information where appropriate.

12.5 Right to restrict processing
Individuals may request limits on how information is used.

12.6 Right to data portability
Individuals may request transfer of certain information in a structured format where applicable.

12.7 Right to object
Individuals may object to certain processing activities.

13.0 Data Breaches

13.1 A personal data breach includes:

- Loss of personal information;
- Unauthorised access;
- Accidental disclosure;
- Theft;
- Destruction of information.

13.2 Any suspected breach must be reported immediately to the Chief Officer (Town Clerk)/Data Protection Lead.

13.3 The Town Council will:

- Assess the risk;
- Take steps to reduce harm;
- Record the breach;
- Notify the Information Commissioner's Office (ICO) where required.

14.0 Confidentiality

14.1 Everyone working for or with the Council has a duty of confidentiality.
Personal information must not be:

- Discussed where it may be overheard;
- Shared without authority;
- Used for personal purposes;
- Removed without permission.

14.2 Unauthorised disclosure may result in disciplinary action and may constitute a criminal offence.

15.0 Training and Awareness

15.1 The Town Council will ensure appropriate training and guidance is available for councillors, employees and others handling personal information.

15.2 Everyone handling personal data must understand their responsibilities.

16.0 Related Policies

16.1 This policy should be read alongside the following documents which are available to view on the Town Council's website:

- Handling 'Access to Information' Requests Policy
- Freedom of Information Procedures;
- Publication Scheme;
- Retention Policy;
- IT Policy;
- Complaints Policy.

17.0 Complaints

17.1 Individuals who believe their information has been handled incorrectly should contact:

Data Protection Lead:
Chief Officer (Town Clerk)

Email:
townclerk@uckfieldtc.gov.uk

Individuals may also contact:

Information Commissioner's Office (ICO)
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone: 0303 123 1113

18.0 Review

18.1 This policy will be reviewed every three years, or sooner if:

- Legislation changes;
- Guidance changes;
- Council procedures change;
- A significant data protection issue occurs.