

# **Camborne Town Council**

## **Data Protection Policy**

### **1. Introduction**

Camborne Town Council holds personal data about employees, residents, suppliers and other individuals for a variety of Council purposes.

This policy sets out how we seek to protect personal data and ensure that Councillors and Officers understand the rules governing their use of personal data to which they have access during their work.

This policy should be read in conjunction with the CCTV Policy which deals particularly with the procedures for protecting the personal data collected and stored by the closed circuit cameras managed by Camborne Town Council.

This policy requires officers to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

#### 1.1 Purpose of collecting data

The purposes for which personal data may be used by us:

Personnel, administrative, financial, statutory and legislative purposes, payroll, consultations and business development purposes.

Council purposes include the following:

- Compliance with our legal, regulatory and corporate governance obligations and good practice
- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests
- Ensuring Council policies are adhered to (such as policies covering email and internet use)
- Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of sensitive information, security vetting and checking
- Investigating complaints
- Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments
- Monitoring staff conduct, disciplinary matters
- Promoting Council services

- Improving services

## 1.2 Personal Data

Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts, members of the public, Council service users, residents, grant applicants, hirers, correspondents.

Personal data we gather may include:

- Individuals' contact details
- Educational background
- Financial and pay details
- Details of certificates and diplomas, education and skills
- Marital status
- Nationality
- Job title
- CV
- Organisation contact details
- Correspondence
- Emails
- Databases
- Council records

## 1.3 Sensitive personal data

There is stronger legal protection for more sensitive personal data such as:

- Race and/or ethnic background
- Political opinions
- Religious beliefs
- Trade union membership
- Health
- Genetics
- Biometrics (where used for identification)
- Sexual orientation
- Criminal offences, or related proceeding

## **2. SCOPE**

This policy applies to all Councillors and staff who must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time.

Any new or modified policy will be circulated to staff after adoption by the Council.

### **3. WHO IS RESPONSIBLE FOR THIS POLICY?**

The Data Protection Officer (DPO) (Town Clerk) has overall responsibility for the day-to-day implementation of this policy.

### **4. PROCEDURES**

#### 4.1 Fair and lawful processing

The Council must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

The Council will ensure any use of personal data is justified and processed in compliance with the six data protection principles:

- 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
- 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
- and this will be specifically documented. All staff who are responsible for processing
- personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice (Appendix A).

#### 4.2 The Data Protection Officer's responsibilities

- Reviewing all data protection procedures and policies on a regular basis
- Keeping the Council updated about data protection responsibilities, risks and issues
- Answering questions on data protection from staff, council members and other

- stakeholders
- Responding to individuals such as members of the public, service users and employees who wish to know which data is being held on them.
- Checking and approving with third parties that handle the council's data any contracts or agreement regarding data processing.

#### 4.3 Responsibilities of the IT contractor

- Ensure all systems, services, software and equipment meet acceptable security standards.
- Checking and scanning security hardware and software regularly to ensure it is functioning properly.
- Researching third-party services, such as cloud services the company is considering using to store or process data.

#### 4.4 Responsibilities of the Line Managers

- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

#### 4.5 The processing of all data must be:

- Necessary to deliver Council services.
- In the Council's legitimate interests and not unduly prejudice the individual's privacy.
- In most cases this provision will apply to routine business data processing activities.

#### The Privacy Notice:

- Sets out the purposes for which we hold personal data on customers, employees, residents and service users
- Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers
- Provides that service users and correspondents have a right of access to the personal data that we hold about them

## **5. SENSITIVE PERSONAL DATA**

In most cases where sensitive personal data is processed, the data subject's explicit consent will be required to do this unless exceptional circumstances apply, or we are

required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work, comply with allotment legislation). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

### 5.1 Accuracy and relevance

The Council will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained.

We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the Data Information Officer (DIO).

### 5.2 Your personal data

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the DIO so that they can update your records.

## **6. DATA SECURITY**

The Council must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

### 6.1 Storing data securely

- In cases when data is stored on printed paper, it must be kept in a secure place where unauthorised personnel cannot access it.
- Printed data must be shredded when it is no longer needed.
- Data stored on a computer must be protected by strong passwords that are changed regularly.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used.
- The DIO and IT contractor must seek the DPO's approval of any cloud used to store data.
- Servers containing personal data must be kept in a secure location.
- Data should be regularly backed up.
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.

- All servers containing sensitive data must be approved and protected by security software and a strong firewall.

## **7. DATA RETENTION**

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, considering the reasons that the personal data was obtained, but should be determined in a manner consistent with the Council’s Retention and Disposal Policy.

## **8. SUBJECT ACCESS REQUESTS**

Under the General Data Protection Regulation 2018 (GDPR), individuals are entitled, subject to certain exceptions, to request access to information held about them.

If you receive a subject access request, you should refer that request immediately to the DIO who may ask the DPO for help in complying with those requests.

Please contact the DIO if you would like to correct or request information that we hold about you. There are also restrictions on the information to which you are entitled under applicable law.

## **9. PROCESSING DATA IN ACCORDANCE WITH THE INDIVIDUAL’S RIGHTS**

The Council should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DIO about any such request.

The Council will not send direct marketing material to someone electronically (e.g. via email) unless there is an existing business relationship with them in relation to the services being marketed.

## **10. PRIVACY NOTICE – TRANSPARENCY OF DATA PROTECTION**

Being transparent and providing accessible information to individuals about how their personal data will be used is important for our organisation.

### 10.1 Consent

The data that is collected is subject to active consent by the data subject. This consent can be revoked at any time.

The following are details on how data is collected and how it will be used:

### **What information is being collected?**

Who is collecting it?	The Council
-----------------------	-------------

How is it collected?	Electronically, hard copies, orally
Why is it being collected?	To carry out the legitimate functions and powers of the Council: The Council is a public authority and has certain powers and duties. Most of your personal data is processed for compliance with a legal obligation which includes the discharge of the Council's statutory functions and powers. Sometimes when exercising these powers or duties it is necessary to process personal data of residents or people using the Council's services. We will always consider your interests and rights. We may also process personal data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract. Sometimes the use of your personal data requires your consent. We will first obtain your consent to that use.
How will it be used?	For Council purposes, in the exercise of official authority, to perform a task that is in the public interest and that is set out in law.
Who will it be shared with?	Authorised third parties.
The Data Controller	Camborne Town Council
The Data Information Officer	Deputy Town Clerk
The Data Processors	Council Officers
The Data Protection Officer	Town Clerk
Retention Period	Refer to the Council's Document Retention and Disposal Policy

## 10.2 Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

## **11. DATA PORTABILITY**

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system.

This must be done for free.

## **12. RIGHT TO BE FORGOTTEN**

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request.

An erasure request can only be refused if an exemption applies.

## **13. PRIVACY BY DESIGN AND DEFAULT**

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The DPO will be responsible for monitoring Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.

## **14. DATA AUDIT AND REGISTER**

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

### 14.1 Reporting breaches

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows the Council to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures

### 14.2 Monitoring

Everyone must observe this policy. The DPO has overall responsibility for this policy and will monitor it regularly to make sure it is being adhered to.

## **15. CONSEQUENCES OF FAILING TO COMPLY**

Compliance with this policy is taken very seriously. Failure to comply puts both the individual and the organisation at risk. Failure to comply with any requirement may lead to disciplinary action under Council procedures which may result in dismissal.

### 15.1 Breaches

Any individual who believes that the Council has breached any of the requirements of GDPR should raise the matter with the Town Council in the first instance. Alternatively, a complaint can be made to the Information Commissioners Office on 0303 123 1113 via email <https://ico.org.uk/global/contact-us/> or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Designated Authority

Supervisory Authority	Information Commissioner's Office
Data Controller	Camborne Town Council
Data Protection Officer	Town Clerk
Data Information Officer	Deputy Town Clerk

**POLICY DATED: 12<sup>th</sup> March 2026**

**REVIEW DATE: 2 years after date of policy**

Version number	Date	Description of changes	Author/Responsible party
1	12.06.2026	Adopted/Reviewed by Camborne Town Council Resolution number	Deputy Town Clerk