

# North Tawton Town Council Data Protection Policy

## Introduction

We hold personal data about our 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 in the course of their work.

This policy requires Officers and employees to ensure that compliance with the relevant legislation is checked before any significant new data processing activity is started.

## Data Protection Terminology

**Data subject** - means the person whose personal data is being processed.

**Personal data** - means any information relating to a natural person or data subject that can be used directly or indirectly to identify the person. It can be anything from a name, a photo, and an address, date of birth, an email address, bank details, and posts on social networking sites or a computer IP address.

**Sensitive personal data** - includes information about racial or ethnic origin, political opinions, and religious or other beliefs, trade union membership, medical information, sexual orientation, genetic and biometric data or information related to offences or alleged offences where it is used to uniquely identify an individual.

**Data controller** - means a person who (either alone or jointly or in common with other persons) (e.g. Parish Council, employer, council) determines the purposes for which and the manner in which any personal data is to be processed.

**Data processor** - in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

**Processing information or data** - means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- organising, adapting or altering it
- retrieving, consulting or using the information or data
- disclosing the information or data by transmission, dissemination or otherwise making it available
- aligning, combining, blocking, erasing or destroying the information or data. regardless of the technology used.

## **Definitions**

### **Business purposes**

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

### **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, hirers, correspondents

Personal data we gather MAY include any of the following:

- individuals' contact details
- educational background
- financial and pay details
- details of certificates and diplomas
- education and skills
- marital status
- nationality
- job title
- CV
- contact details
- correspondence
- emails
- databases
- council records

## **Sensitive personal data**

Any use of sensitive personal data should be strictly controlled in accordance with this policy. This could include the following personal data about an individual:

- racial or ethnic origin
- political opinions
- religious or similar beliefs
- trade union membership (or non-membership)
- physical or mental health or condition
- criminal offences, or related proceedings
- salary and pension

## **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 before being adopted.

## **Who is responsible for this policy?**

North Tawton Town Council, the Town Clerk, and the Assistant Town Clerk all have responsibility for the day-to-day implementation of this policy.

## **Our procedures**

### **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 responsibilities of the North Tawton Town Council, the Town Clerk, and the Assistant Town Clerk:**

- Ensure procedures are in place to keep the Council updated about data protection responsibilities, risks and issues.
- Review all data protection procedures and policies on a regular basis.
- Ensure the provision of relevant data protection training and advice for all staff members and those included in this policy
- Answer questions or consult a relevant expert to answer questions on data protection from staff, council members and other stakeholders
- Respond to individuals such as members of the public, service users, and other relevant persons, who wish to know which data is being held on them by North Tawton Town Council.
- Ensure procedures are in place for checking and approving with third parties that handle the council's data any contracts or agreement regarding data processing

## **Responsibilities of the Council's IT Contractor AND providers of IT services**

North Tawton Town Council's IT Contractor and IT service providers will be required to:

- Ensure all systems, services, software and equipment meet acceptable security standards

## **Responsibilities of the Council's IT Contractor:**

- Checking and scanning security hardware and software regularly to ensure it is functioning properly.
- Undertaking any other such tasks the Council may request in respect of data storage and processing.

## **Responsibilities of the Officers**

- Approving data protection statements attached to emails and/or other documentation.
- Addressing data protection queries from external organisations.
- Take appropriate steps to ensure all Council initiatives adhere to data protection laws and the Council's Data Protection Policy.

## **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 Council data processing activities.
- The Council has a Privacy Notice in place, relating to data protection.

## **North Tawton Town Council Privacy Notice:**

- Outlines what information we may store when people contact the Council, and the rights of North Tawton Town Council to process information
- Advises as to the Council's information security processes
- Advises that service users and correspondents have a right of access to the personal data that the council holds about them.
- Advises on customer's rights in relation to correction and deletion of personal information.

## **Sensitive personal data**

We very rarely process sensitive personal data. In cases where we might process sensitive personal data we will require the data subject's explicit consent 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 burial legislation and 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.

## **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 Council by contacting the Town Clerk in the first instance.

## **Your personal data**

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. If the information you have provided us changes, please inform the Town Clerk so that your records can be updated.

## **Data security**

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

## **Storing data securely**

- If data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it.
- Printed data should 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 Council and the Council's IT Contractor must approve any cloud used to store data.
- Data should be regularly backed up.
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.
- Computers containing sensitive data must be approved and protected by security software and a strong firewall.

## **Data Retention**

- The Council will not retain personal data for longer than is necessary.
- What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with the Council's data retention guidelines.

## **Subject Access Requests**

- Under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them.
- Please contact the Town Clerk in the first instance if you wish to correct or request information that we hold about you.
- There are restrictions on the information to which you are entitled under applicable law.

## **Processing data in accordance with the individual's rights**

- The Council will abide by any request from an individual not to use their personal data for direct marketing purposes.
- The Council will not send direct marketing material to someone electronically (e.g. via email) unless we have an existing business relationship with them in relation to the services being marketed.

## **Training**

- Staff and Councillors will receive training on this policy.
- New joiners will receive training as part of their induction process.
- Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

Training will cover:

- The law relating to data protection
- Our data protection and related policies and procedures.
- Completion of training is compulsory.

## **Privacy Notice - transparency of data protection**

Here are details on how we collect data and what we will do with it:

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

Information to allow the Council to fulfil its duties and respond to complaints and enquiries – including names, addresses, email addresses, telephone numbers.

### **Who is collecting it?**

North Tawton Town Council.

### **How is it collected?**

Electronically, via hard copies, orally.

### **Why is it being collected?**

To carry out the legitimate functions and powers of the Council.

To ensure compliance with the Council's legal obligations in carrying out statutory functions and powers.

**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 if necessary.

**Who is the data controller?**

North Tawton Town Council

**Who are the data information officers?**

The Town Clerk, the Assistant Town Clerk, the Administration Officer.

**Retention period**

As set out in the Council's Data Retention Policy.

**Conditions for processing**

The General Data Protection Regulations Article 6 (1) (a) (b) and (c)

Processing is with the consent of the data subject or

Processing is necessary for compliance with a legal obligation

Processing is necessary for the legitimate interests of the Council

The Council will ensure any use of personal data is justified using at least one of the conditions for processing 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.

**Justification for personal data**

The Council will process personal data in compliance with all six data protection principles.

We will document the additional justification for the processing of sensitive data and will ensure any biometric and genetic data is considered sensitive.

**Consent**

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

**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.

**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.

## **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.

*May 2018*