



**SANDBACH  
TOWN COUNCIL**

# DATA PROTECTION POLICY

VERSION NUMBER

V1 1 February 2023

DATE & MINUTE REFERENCE (Council)

230201  
Finance, Policy and Governance Committee Meeting Item 5

DATE OF NEXT REVIEW

February 2025

**Introduction..... 3**

**Definitions..... 3**

**Scope..... 4**

**The principles ..... 5**

**Accountability and transparency ..... 5**

**Our procedures..... 6**

**Special categories of personal data..... 7**

**Responsibilities ..... 8**

**Accuracy and relevance..... 9**

**Rights of individuals ..... 10**

**Privacy notices ..... 12**

**Subject Access Requests (SAR) ..... 12**

**Right to erasure ..... 13**

**The right to restrict automated profiling or decision making..... 14**

**The right to data portability..... 15**

**Third parties..... 15**

**Criminal offence data ..... 16**

**Audits, monitoring and training..... 16**

**Reporting breaches ..... 17**

**Failure to comply ..... 17**

## Introduction

Sandbach Town Council (STC) is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all of our legal obligations.

We hold personal data about our employees, residents, and other individuals for a variety of purposes.

This policy sets out how we seek to protect personal data and ensure that we understand the rules governing the use of the personal data to which we have access in the course of delivering our services.

## Definitions

<p><b>Purposes</b></p>	<p>The purposes for which personal data may be used by us:</p> <p>Personnel, administrative, financial, regulatory, payroll and service development purposes <i>including the following:</i></p> <ul style="list-style-type: none"> <li>- <i>Compliance with our legal, regulatory requirements and good practice including compliance with employment contracts</i></li> <li>- <i>Gathering information to enable us to deliver our services</i></li> <li>- <i>Operational reasons, such as recruitment, recording transactions, training, security vetting</i></li> <li>- <i>Investigating complaints and responding to enquiries</i></li> <li>- <i>Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments</i></li> <li>- <i>Monitoring staff conduct, disciplinary matters</i></li> </ul>
<p><b>Personal data</b></p>	<p><b>'Personal data' means any image or information relating to an identified or identifiable natural person ('data subject');</b> an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.</p> <p><i>Personal data we gather may include: individuals' phone number, home address, email address, educational background, financial and pay details, details of education and skills, marital status, nationality and CV.</i></p>

<b>Special categories of personal data</b>	Special categories of data include information about an individual's 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, and genetic and biometric information — any use of special categories of personal data should be strictly controlled in accordance with this policy.
<b>Data controller</b>	'Data controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.
<b>Data processor</b>	'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
<b>Processing</b>	'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
<b>Supervisory authority</b>	This is the national body responsible for data protection. The supervisory authority for our organisation is the Information Commissioners Office.

## Scope

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

This policy supplements our other policies relating to internet and email use, and document retention We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated before being adopted.

## The principles

Sandbach Town Council shall comply with the principles of data protection (the Principles) enumerated in the Data Protection Act 2018 (DPA 2018). We will make every effort possible in everything we do to comply with these principles. The principles are:

### 1. Lawful, fair and transparent

Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.

### 2. Limited for its purpose

Data can only be collected for a specific purpose.

### 3. Data minimisation

Any data collected must be necessary and not excessive for its purpose.

### 4. Accurate

The data we hold must be accurate and kept up to date.

### 5. Retention

We cannot store data longer than necessary.

### 6. Integrity and confidentiality

The data we hold must be kept safe and secure.

## Accountability and transparency

We must ensure accountability and transparency in all our use of personal data. We must show how we comply with each Principle. STC are responsible for keeping a written record of how all the data processing activities that we are responsible for comply with each of the Principles. This must be kept up to date and must be available to the Data Protection Officer (DPO) for auditing compliance with this policy.

To comply with data protection laws and the accountability and transparency principle of data protection, we must demonstrate compliance. STC are responsible for understanding our particular responsibilities to ensure we meet the following data protection obligations:

- Fully implement all appropriate technical and organisational measures
- Maintain up to date and relevant documentation on all processing activities
- Conducting data audits and risk assessments including Privacy Impact Assessments where these are required
- Implement measures to ensure privacy by design and default:
  - Data minimisation
  - Pseudonymisation where this is identified as necessary
  - Transparency
  - Allowing individuals to monitor processing
  - Creating and improving security and enhanced privacy procedures on an ongoing basis

## Our procedures

- **Fair and lawful processing**

We must process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. This generally means that we should not process personal data unless we have a lawful basis for processing the personal data.

If we cannot apply a lawful basis (explained below), our processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed erased.

- **Data Controller**

Sandbach Town Council is classified as a data controller (and we also process data). We must maintain our appropriate registration with the Information Commissioner's Office (ICO) in order to continue lawfully controlling and processing data.

- **Lawful basis for processing data**

We must establish a lawful basis for processing data. Ensure that any data STC are responsible for managing has a written lawful basis approved by the council. It is our responsibility to check the lawful basis for any data we are working with and ensure all of our actions comply the lawful basis. At least one of the following conditions must apply whenever we process personal data:

1. **Consent**

We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.

2. **Contract**

The processing is necessary to fulfil or prepare a contract for the individual.

3. **Legal obligation**

We have a legal obligation to process the data (excluding a contract).

4. **Vital interests**

Processing the data is necessary to protect a person's life or in a medical situation.

5. **Public Task**

Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

6. **Legitimate interest**

The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

- **Deciding which condition to rely on**

If STC are making an assessment of the lawful basis, we must first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. We cannot rely on a lawful basis if we can reasonably achieve the same purpose by some other means.

Remember that more than one basis may apply, and STC rely on what will best fit the purpose, not what is easiest.

Consider the following factors and document the answers:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Is STC in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Is STC able to stop the processing at any time on request, and have factored in how to do this?

Our commitment to the first Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

We must also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This should occur via a privacy notice. This applies whether we have collected the data directly from the individual, or from another source.

## **Special categories of personal data**

What are special categories of personal data?

Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include, for example, information about an individual's:

- race
- ethnic origin
- politics
- religion
- trade union membership
- health

In most cases where we process special categories of 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). 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.

The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity must cease.

## **Responsibilities**

- **Council responsibilities**
  - Analysing and documenting the type of personal data we hold
  - Checking procedures to ensure they cover all the rights of the individual
  - Identify the lawful basis for processing data
  - Ensuring consent procedures are lawful
  - Implementing and reviewing procedures to detect, report and investigate personal data breaches
  - Store data in safe and secure ways
  - Assess the risk that could be posed to individual rights and freedoms should data be compromised
- **Responsibilities of STC**
  - Fully understand the data protection obligations
  - Check that any data processing activities STC is dealing with comply with our policy and are justified
  - Do not use data in any unlawful way
  - Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through our actions
  - Comply with this policy at all times
  - Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay



- **Support from the Data Protection Officer (DPO)**
  - Keeping the council updated about data protection responsibilities, risks and issues
  - Reviewing all data protection procedures and policies on a regular basis
  - Reviewing the data inventory
  - Reviewing compliance with the data protection legislation
  - Answering questions on data protection from staff and councillors
  - Checking data processing agreements with relevant third parties are in place
  - Supporting the completion of Privacy Impact Assessments
  - Investigating and reporting data breaches
- **IT Security Responsibilities**
  - 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 council is considering using to store or process data

### **Accuracy and relevance**

We 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 STC believe that information is inaccurate we should record the fact that the accuracy of the information is disputed and take appropriate action.

- **Data security**

STC must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, contracts must be implemented with those third-party organisations including specific data security arrangements.

- **Storing data securely**

- In cases when 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 with reference to the time limits in the council's Document Retention Policy
- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords
- Data stored on CDs or memory sticks or plug in hard drives must be encrypted or password protected and locked away securely when they are not being used
- Servers containing personal data must be kept in a secure location, away from general office space, and protected by security software
- Data should be regularly backed up in line with the council's backup procedures
- Personal Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- All possible technical measures must be put in place to keep data secure

- **Data retention**

We must retain personal data for no 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 our data retention guidelines as specified in our data retention policy.

- **Transferring data internationally**

There are restrictions on international transfers of personal data abroad. STC must not transfer personal data abroad, or anywhere else outside of normal rules and procedures without first securing appropriate guidance.

## **Rights of individuals**

Individuals have rights to their data which we must respect and comply with to the best of our ability. We must ensure individuals can exercise their rights in the following ways:

### **1. Right to be informed**

- Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.
- Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

### **2. Right of access**

- Enabling individuals to access their personal data and supplementary information.
- Allowing individuals to be aware of and verify the lawfulness of the processing activities.

### **3. Right to rectification**

- We must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.
- This must be done without delay, and no later than one month. This can be extended to two months where valid reason(s) have been identified.

### **4. Right to erasure**

- We must delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

### **5. Right to restrict processing**

- We must comply with any request to restrict, block, or otherwise suppress the processing of personal data.
- We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

### **6. Right to data portability**

- We must provide individuals with their data so that they can reuse it for their own purposes or across different services.
- We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

### **7. Right to object**

- We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- We must respect the right of an individual to object to direct marketing, including profiling.
- We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

### **8. Rights in relation to automated decision making and profiling**

- We must respect the rights of individuals in relation to automated decision making and profiling.
- Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

## Privacy notices

What to include in a privacy notice

Privacy notices must be concise, transparent, intelligible and easily accessible. They are provided free of charge and must be written in clear and plain language, particularly if aimed at children

The following information must be included in a privacy notice to all data subjects:

- Identification and contact information of the data controller and the data protection officer
- The purpose of processing the data and the lawful basis for doing so
- The legitimate interests of the controller or third party, if applicable
- The right to withdraw consent at any time, if applicable
- The category of the personal data (only for data not obtained directly from the data subject)
- Any recipient or categories of recipients of the personal data
- Detailed information of any transfers to third countries and safeguards in place
- The retention period of the data or the criteria used to determine the retention period, including details for the data disposal after the retention period
- The right to lodge a complaint with the Information Commissioner's Office (ICO), and internal complaint procedures
- The source of the personal data, and whether it came from publicly available sources (only for data not obtained directly from the data subject)
- Any existence of automated decision making, including profiling and information about how those decisions are made, their significances and consequences to the data subject
- Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences for any failure to provide the data (only for data obtained directly from the data subject).

## Subject Access Requests (SAR)

- **What is a subject access request?**

An individual has the right to receive confirmation that their data is being processed, access to their personal data and supplementary information which means the information which should be provided in a privacy notice.

- **How we deal with subject access requests**

We must adopt SAR procedures to ensure requests are dealt with correctly.

WE must provide an individual with a copy of the information the request, free of charge. This must occur without delay, and within one month of receipt. We endeavour to provide data subjects access to their information in commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system.

If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month.

We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting.

Once a SAR has been made, STC must not change or amend any of the data that has been requested. Doing so is a criminal offence.

## **Right to erasure**

- **What is the right to erasure?**

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed
- Where consent is withdrawn
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation
- The processing relates to a child

- **How we deal with the right to erasure**

We can only refuse to comply with a right to erasure in the following circumstances:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority or the comply with a contract
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

If personal data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those recipients.

- **The right to object**

Individuals have the right to object to their data being used on grounds relating to their particular situation. We must cease processing unless:

- We have legitimate grounds for processing which override the interests, rights and freedoms of the individual.
- The processing relates to the establishment, exercise or defence of legal claims.

### **The right to restrict automated profiling or decision making**

We may only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:

- It is necessary for the entry into or performance of a contract.
- Based on the individual's explicit consent.
- Otherwise authorised by law.

In these circumstances, we must:

- Give individuals detailed information about the automated processing.
- Offer simple ways for them to request human intervention or challenge any decision about them.
- Carry out regular checks and user testing to ensure our systems are working as intended.

## **The right to data portability**

We must provide the data requested in a structured, commonly used and machine-readable format. We must provide this data either to the individual who has requested it, or to the data controller they have requested it be sent to. This must be done free of charge and without delay, and no later than one month. This can be extended to 2 months for complex or numerous requests.

## **Third parties**

- **Using third party controllers and processors**

As a data controller we must have written contracts in place with any third party data processors that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities.

As a data controller, we must only appoint processors who can provide sufficient guarantees under the DPA 2018 and that the rights of data subjects will be respected and protected.

- **Contracts**

Our contracts must comply with the standards set out by the ICO and, where possible, follow the standard contractual clauses which are available. Our contracts with data processors must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

At a minimum, our contracts must include terms that specify:

- Acting only on written instructions
- Those involved in processing the data are subject to a duty of confidence
- Appropriate measures will be taken to ensure the security of the processing
- Sub-processors will only be engaged with the prior consent of the controller and under a written contract
- The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under the DPA 2018
- The processor will assist the controller in meeting its data protection obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments

- Delete or return all personal data at the end of the contract
- Submit to regular audits and inspections, and provide whatever information necessary for the controller and processor to meet their legal obligations.
- Nothing will be done by either the controller or processor to infringe the DPA 2018.

## **Criminal offence data**

### 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. We cannot keep a comprehensive register of criminal offence data. All data relating to criminal offences is considered to be a special category of personal data and must be treated as such.

## **Audits, monitoring and training**

- **Data audits**

Regular data audits to manage and mitigate risks will inform the data inventory. 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. STC must conduct a regular data audit to ensure an up to date data inventory is maintained.

- **Monitoring**

Everyone must observe this policy. The DPO will carry out periodic internal audits to monitor compliance of the council with this policy. The council will keep this policy under review and amend or change it as required. STC should notify the DPO of any breaches of this policy. We must comply with this policy fully and at all times.

- **Training**

**Sandbach Town Council will provide staff briefing session to ensure all staff are aware of the importance of data protection.** Also, there is training on provisions of data protection law specific for each staff and Member. All staff and Members must complete all training as requested. If they move role or responsibilities, they are responsible for requesting new data protection training relevant to their new role or responsibilities.

If any staff or Member have queries on data protection matters, contact the DPO.



## **Reporting breaches**

A data breach register will be maintained on an ongoing basis. Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as STC have become aware of a breach. The council has a legal obligation to report any reportable data breaches to the ICO within 72 hours.

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

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

Any member of staff who fails to notify of a breach or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

## **Failure to comply**

We take compliance with this policy very seriously. Failure to comply puts both STC and the member of staff at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures.