WHITEHILL
TOWN COUNCIL
Serving Whitehill & Bordon

DATA PROTECTION POLICY

Date of adoption: 16.07.2018 Review date: 06.11.2025 Next Review: November 2026

1.0 INTRODUCTION

1.1 Whitehill Town Council (WTC) holds and processes information about employees, councillors, residents, contractors, service users and other data subjects for administrative, statutory and operational purposes.

1.2 When handling such information, WTC and all those acting on its behalf must comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and any subsequent amendments or replacement legislation.

1.3 WTC recognises that it must, at times, keep and process sensitive and personal information about both employees and the public. It has, therefore, adopted this policy, not only to meet its legal obligations but to ensure that high standards of GDPR are maintained.

1.4 The Data Protection Act 2018 (DPA 2018) seeks to balance individuals' rights with other public and private interests, such as **national security**, **law enforcement**, **crime prevention**, **safeguarding vulnerable people** and the **facilitation of research**. It ensures personal data is processed fairly, lawfully, and securely, while also allowing for its use in specific situations where these legitimate interests outweigh privacy concerns.

1.5 WTC will periodically review and revise this policy in the light of experience, comments from data subjects and guidance from the Information Commissioner's Office (ICO).

2.0 DATA PROTECTION PRINCIPLES

The UK GDPR outlines seven key data protection principles that govern the processing of personal data, ensuring lawful, fair, and transparent handling of information.

The Seven Principles of UK GDPR:

2.1 **Lawfulness, Fairness, and Transparency**: Personal data must be processed lawfully, fairly and in a transparent manner. Organisations must identify a lawful basis for processing data, such as consent, contractual necessity or legal obligation, and must inform individuals about how their data will be used.

2.2 **Purpose Limitation**: Data should be collected for specified, explicit, and legitimate purposes an d not further processed in a manner incompatible with those purposes. This principle ensures t hat data is not used for unrelated activities without further consent.

2.3 **Data Minimisation:** Organisations should only collect personal data that is adequate, relevant, and limited to what is necessary for the purposes for which it is processed. This principle encourages organisations to avoid excessive data collection.

2.4 **Accuracy**: Personal data must be accurate and kept up to date. Organisations are required to take reasonable steps to ensure that inaccurate data is erased or rectified without delay.

2.5 **Storage Limitation:** Personal data should be kept in a form that permits identification of data subjects for no longer than is necessary for the purpose for which the data is processed. Organisations must establish retention policies to ensure data is not held indefinitely.

2.6 **Integrity and Confidentiality:** Organisations must process personal data in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. This involves implementing appropriate technical and organisational measures.

2.7 **Accountability:** Organisations are responsible for complying with the UK GDPR principles and must be able to demonstrate their compliance. This includes maintaining documentation, conducting regular assessments, and implementing data protection policies.

3.0 ROLES AND RESPONSIBILITIES

Data Controller - A person who, either alone, jointly or in common with other persons (e.g. Town Council, employer or councillor), determines the purposes for which and the way in which any personal
data is to be processed. WTC appointed the Town Clerk and Deputy Clerk to be the data controllers.

Data Processor - A processor follows the instructions of, and handles data for, the controller, not for their own purposes. The processing activities must align with the instructions given by the data controller. The processor may act as an external service, often a third-party service provider, such as outsourced IT services or web agencies. Responsibilities include: ensuring data security, storing and transferring data, deleting or disposing of data as instructed, and notifying the controller of any breaches. They are usually bound by contract and the relationship between the controller and processor is governed by a contract or other legal act that outlines the processor's duties.

Data Protection Officer - Under the GDPR, public authorities must appoint a data protection officer (DPO). The role is to monitor internal compliance, audit, give advice on data protection obligations and data protection impact assessments, and to act as a point of contact for data subjects and the Information Commissioners Office (ICO). They also help WTC to demonstrate compliance. The person(s) WTC has appointed for this role is our internal auditor, Mark Mulberry (*Mulberry Local Authority Services Ltd).*

Also, this may be reviewed by BDO, our external auditor, due to The Practitioners' Guide 2025 introducing a strengthened focus on digital standards through Assertion 10 – **Digital and Data Compliance**, setting out mandatory IT and data requirements for smaller authorities.

4.0 PROCESSING INFORMATION OR DATA

This means obtaining, recording, holding information or data, and carrying out any operation on the information or data, including:

4.1 Organising, adapting or altering it;
4.2 Retrieving, consulting or using it;
4.3 Disclosing the information or data by transmission, dissemination or otherwise making it available;
4.4 Aligning, combining, blocking, erasing or destroying the information or data, regardless of the technology used.

5.0 PROCESSING PERSONAL DATA

WTC promises to:

5.1 Fulfil its duties as an employer by complying with the terms in contracts of employment, safeguarding the employee and maintaining information required by law;
5.2 Pursue the legitimate interests of its business and its duties as a public body, by fulfilling contractual terms with other organisations, and maintaining information required by law;
5.3 Monitor its activities, including the equality and diversity of its activities;

5.4 Fulfil its duties in operating the business premises, including security;
5.5 Assist regulatory and law enforcement agencies;
5.6 Process information, including the recording and updating details about its Councillors, employees, partners and volunteers.
5.7 Process information including recording and updating details about individuals who contact it for information, to access a service, or to make a complaint;
5.8 Undertake surveys, censuses and questionnaires to fulfil the objectives and purposes of the Council;
5.9 Undertake research, audit and quality improvement work to fulfil its objects and purposes;
5.10 Carry out Council administration;
5.11 Have competitions or awards ceremonies where personal data is required.

6.0 SPECIAL CATEGORIES OF PERSONAL DATA

Particular attention is paid to the processing of any sensitive personal information that forms the 'special categories of personal data'. The UK GDPR singles out some types of personal data as likely to be more sensitive, and gives them extra protection:

- Personal data revealing **racial or ethnic origin**;
- Personal data revealing **political opinions**;
- Personal data revealing **religious or philosophical beliefs**;
- Personal data revealing **trade union membership**;
- **Genetic data**;
- **Biometric data** (where used for identification purposes);
- Data concerning **health**;
- Data concerning a person's **sex life**; and
- Data concerning a person's **sexual orientation**.
- The presumption is that this type of data needs to be treated with greater care because collecting and using it is more likely to interfere with these fundamental rights or open someone up to discrimination. This is part of the risk-based approach of the UK GDPR to comply with:
- The explicit consent of the individual;
- The requirement by law to process data for employment purposes;
- The requirement to protect the vital interests of the individual or another person.

7.0 STORAGE, SECURITY AND RETENTION

All personal data is held on the WTC server under a secured management folder which has restricted access to data controllers only.

Personal data must not be kept for longer than required.

WTC will inform the provider of a GDPR notice as to why this information is **required** and that it will only be **retained** for the purposes for which it was given, will not be provided to any **third party** and that it will be **deleted** when the purpose for which it was requested, i.e. a competition, has finished.

Our Retention periods are set out in the Council Retention and Disposal Policy.
https://www.whitehilltowncouncil.gov.uk/wp-content/uploads/2024/10/20241002_Document-and-Retention-Disposal-Policy-2024.pdf

8.0 RIGHTS OF DATA SUBJECTS

People have a right to:

- **Confirmation** of how and where their personal information is being processed;
- **A copy** of their information;
- **Know where** their information was collected from;
- **Know what** types of recipients their information may be shared with;
- **Know how long** their information will be stored;
- **Know what their rights are** in terms of rectification, restriction, objection and deletion;
- **Know how to complain** to the relevant data protection authority;
- **Understand the logic** behind any automated processing.

9.0 DATA BREACH PROCEDURE

9.1 A personal data breach is any incident leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

9.2 All breaches must be reported immediately to the Town Clerk, who has delegated responsibility for the day to day running of operations at WTC and is also the Data Controller.

9.3 If there is a breach to people's rights and freedoms, WTC would report this to the ICO (Information Commissioner office) within 72 hours of becoming aware of the breach.

10.0 INTERNATIONAL DATA TRANSFERS

Personal data will not be transferred outside the UK unless:

- The destination country is covered by a UK "adequacy decision" or
- Appropriate safeguards are in place, such as Standard Contractual Clauses and
- Individual's rights are protected and enforceable.

11.0 PRIVACY BY DESIGN AND DEFAULT

WTC will ensure that data protection principles are considered in the design of new systems processes and projects and that only the minimum necessary personal data is collected and processed.

12.0 DATA SHARING

WTC will only share personal data with third parties where necessary and lawful, and subject to a written Data Sharing Agreement or contractual clause ensuring compliance with UK GDPR.

13.0 TRAINING AND AWARENESS

All relevant employees & Councillors will have an opportunity to complete a data protection training course at induction level and/or be provided with the latest information and a copy of the WTC Data Protection Policy, with annual refresher training thereafter.
By the end of this course learners will:

- Understand the key terms used in data protection law;
- Understand their responsibilities under the EU and UK GDPR and the Data Protection Act;
- Have knowledge of the principles of data protection that all organisations must adhere to.
- Understand the lawful grounds for processing personal information;

- Understand how to obtain consent from data subjects;
- Have an understanding of data subject rights, including access rights and the right to be forgotten;
- Recognise the responsibilities of data controllers, data processors and data protection officers;
- Understand how to ensure data security and report personal data breaches;
- Be familiar with the consequences of non-compliance.

14.0 CHILDREN

We will not process any data relating to a child (under 13) without the express parental/guardian consent of the child concerned.

15.0 RIGHTS OF A DATA SUBJECT

An individual has the right to request access to the information we have on them. They can do this by contacting our Data Controllers.

If someone requests a copy of their personal information, which may be by letter, email or phone, this is provided to them free of charge. WTC would only charge a fee if the request were excessive, repetitive or manifestly unfounded, or if the person wants further copies of the same information. The information provided to the person would be transparent, clear and sufficient that the person is able to easily understand it.

16.0 INFORMATION CORRECTION

16.1 The UK GDPR includes a right for individuals to have inaccurate personal data rectified or completed if it is incomplete.
16.2 An individual can make a request for rectification verbally or in writing to WTC.
16.3 You have one calendar month to respond to a request.
16.4 In certain circumstances you can refuse a request for rectification.
16.5 This right is closely linked to the Data Controller's obligations under the accuracy principle of the UK GDPR (Article (5)(1)(d)).

17.0 INFORMATION DELETION "The Right to be forgotten"

If an individual wishes that their information held by WTC should be deleted, they can request this by contacting WTC verbally or in writing and WTC has one calendar month to respond to such requests.

18.0 RIGHT TO OBJECT

If an individual believes their data is not being processed for the purpose it has been collected for, they may object by contacting WTC, and the Data Controllers will investigate this matter and respond to the individual within 5 working days. The Town Council does not use automated decision-making or profiling of individual personal data.

19.0 COMPLAINTS

Complaints about how personal data has been handled should be made to the Town Clerk in the first instance via email to info@whitehilltowncouncil.gov.uk or via post: Whitehill Town Council Forest Community Centre, Pinehill Road, Bordon, Hampshire, GU35 0BS or via telephone: 01420 473123.

Unresolved complaints can be escalated to the Information Commissioners Office (ICO) Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF email: casework@ico.org.uk Tel: 0303 123 1113 & website https://ico.org.uk/