

Tunbridge Wells Commons Conservators:

Privacy (GDPR) Policy

Introduction

Tunbridge Wells Commons Conservators (TWCC) are committed to protecting the personal data it holds and processes, and to complying with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

In accordance with DPA 2018, TWCC are classified as both a data controller and data processor.

Scope

Personal data is defined as any information relating to an identified or identifiable living individual (the “data subject”). This might include name, home address, personal email contact details, or telephone number. Personal data does not include information where identity has been removed (i.e., anonymous data). TWCC do not collect or use any special category data such as race or ethnic origin, political opinions, health data or trade union membership.

Lawful basis for processing

TWCC collect very little in the way of personal data and only as necessary to perform duties and roles, for example:

- Legal obligation - meeting statutory requirements.
- Contract management - managing invoices submitted for payment, insurance documents and risk assessments.
- Community engagement - via social media, email exchange via the website’s ‘get in touch’ function, completion of a survey, taking part in a focus group, event or competition.
- Call for action – in response to an initial contact to assist with an issue, concern or complaint.
- Volunteering – in response to a request to have details added to an email distribution list.

Access to personal data

Access to personal data is restricted to Officers and very occasionally Conservators. Personal data is only used if we are satisfied that it is lawful and fair to do so. Personal data is never sold or shared with third parties who might use it for their own commercial purposes. Any sharing of personal data is done on a case-by-case basis using the minimum personal data necessary.

Data storage

TWCC will implement appropriate technical and organisational measures to keep personal data secure, including:

- Password protection and encryption for digital files.

- Lockable storage for paper records.
- Regular review of access permissions.
- Secure disposal (shredding or deletion) of confidential waste.
- Staff awareness and training, where required.

Data retention and disposal

Personal data will only be kept for as long as necessary, following guidance here:

Type of data	Retention period	Legal/practical basis
Financial records	6 years from the end of the financial year	Legal
Audit and AGAR data	5 years	Legal
General correspondence	3 years (unless genuine need is identified)	Good practice
Minutes	Indefinitely	Historical record/public interest
Email addresses for distribution lists	Indefinitely/until request to remove.	

Records no longer required will be securely destroyed or archived.

Data breaches

Any data breach (loss, unauthorised disclosure, or access to personal data) must be reported immediately to the Clerk, who will assess the risk and mitigate as required. In the case of high risk to individuals, they will be notified. A log of all breaches will be maintained.

Accessing, updating, and deleting personal information

Individuals have the right to request:

- Access to personal data (commonly known as a "data subject access request").
- Correction of incomplete or inaccurate personal data.
- Erasure of personal data from our files and systems where there is no good reason for us continuing to hold it.
- Object to and or restrict processing of personal data.
- Transfer of personal data to another person or organisation.

To exercise any of these rights, to raise a question or complaint relating to this policy, the individual should contact the Clerk via info@twcommons.org or PO Box 729, Tunbridge Wells, TN9 9WF.

Individuals have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

Date of review: October 2025
Date of next review: October 2028