Terrington Parish Council

Data Protection Policy (adopted 11 May 2026)

1. Context and Purpose

Terrington Parish Council ('TPC') recognises its responsibility to comply with the UK General Data Protection Regulations (GDPR) 2018 and the Data Protection Act 2018 which regulate the use of personal data (ie any information relating to an identified or identifiable living person).

This policy sets out how TPC manages personal data and outlines the responsibilities and requirements for councillors and officers who use personally owned devices (e.g. smartphones, tablets, laptops) and paper records to store, access or process TPC data to protect the integrity and confidentiality of that data. It seeks to:

- ensure that councillors and officers handling personal information for TPC are fully aware of the requirements of relevant legislation and comply with data protection procedures;
- outline how TPC meets its legal obligations in safeguarding confidentiality and adheres to information security standards.

The policy is accompanied by a Privacy Notice which sets out the rights of individuals whose personal information is held by TPC.

2. Background and Definitions

This policy covers storage, accessing and processing of all personal information whose storage and use is controlled by TPC whether organised and stored in physical or IT-based record systems.

Personal Information is information about living individuals that enables them to be identified, eg names, addresses and phone numbers. It does not apply to information about organisations, companies or agencies but applies to named persons, such as individual volunteers, employees or members of the public.

TPC is both a ***Data Controller*** (ie it decides what personal information the Council will hold and how long it will be held or used) and a ***Data Processor*** (ie it stores, accesses and processes that personal information). This policy sets out the responsibilities of TPC in these roles.

Data Subjects (ie those about whom personal information is processed) have rights which are described in the accompanying Rights Statement.

The Council is registered as a Data Controller with the ***Information Commissioner's Office*** (ICO) which is an independent body responsible for upholding the information rights of the public. The Council's Registration reference is **ZC110809** and its details can be seen on the public register.

The Council is not required to appoint a Data Protection Officer but one councillor or officer, currently the Clerk, has responsibility for ensuring that the Parish Council follows data protection policy, complies with the relevant legislation, and deals with any data breaches.

Sensitive data includes but is not limited to data relating to racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health, criminal record or proceedings.

3. Collection and handling of personal data

TPC may need to retain certain information to carry out its day-to-day business and to comply with its legal obligations. The information it holds is normally limited to name, address and other contact details and, for employees, information required by HMRC for tax purposes.

TPC will maintain a register of personal data held including how and why it was collected and how the data is stored and protected.

To ensure compliance with the relevant legislation, councillors and officers handling personal data in pursuance of their roles must ensure that:

- when collecting personal information they make it clear to the data subject why the information is required and how it will be used;
- personal data is only collected for specified, explicit and legitimate purposes and is not further processed in a manner that is incompatible with those purposes;
- personal data collection is limited to what is adequate, relevant and necessary in relation to the purposes for which it is to be used;
- as far as possible, personal data is accurate and, where necessary, kept up to date;
- personal data is stored for no longer than is necessary for the purposes for which it was collected or because the Council is required by law to keep it. When data is no longer needed or required by law to be retained it will be shredded or securely deleted.
- personal data is kept secure and is processed in a manner that ensures appropriate security. Digital data must only be stored on password protected devices and processed in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage. Hard copy files must be stored in locked cabinets.

TPC must be able to demonstrate compliance with the above requirements.

4. Sharing personal data

TPC will only share personal data with third parties beyond the councillors and officers under one of the following circumstances:

- With the consent of the data subject;
- In order to fulfil a contract with the data subject;
- If it has a legal obligation to do so;
- If it is necessary to protect someone’s life; or
- If it is necessary in order for TPC to carry out its proper functions.

5. Confidentiality

Councillors and officers must maintain confidentiality in relation to complaints or queries made by members of the public unless the subject has given permission otherwise.

6. Data breaches

GDPR defines a personal data breach as a 'breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or, or access to, personal data transmitted, stored or otherwise processed'. Examples include:

- access by an unauthorised third party;
- sending personal data to an incorrect recipient;
- computing devices or hard copy data containing personal information being lost or stolen;
- alteration of personal data without permission.

Depending on the circumstances, a data breach can have serious consequences for data subjects and so must be taken very seriously and appropriate action taken.

As soon as a data breach is identified the responsible councillor or officer must be informed immediately. It must then be reported to the data subject(s) and to the Information Commissioner's Office (ICO) without undue delay and, where feasible, not later than 72 hours after becoming aware of the breach.

If the ICO is not informed within 72 hours, the Council must give reasons for the delay when they report the breach.

When notifying the ICO of a breach, the Council must:

i. describe the nature of the breach including the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
ii. communicate the name and contact details of the responsible councillor or officer;
iii. describe the likely consequences of the breach;
iv. describe the measures taken or proposed to be taken to address the personal data breach including, measures to mitigate its possible adverse effect.

When notifying the individual affected by the breach, the Council must provide the individual with (ii)-(iv) above.

All data breaches must be recorded to help to identify the system failures and so that they can be used as a way to improve the security of personal data.

7. Review

The Council will review this policy at least every 2 years or in response to changes in relevant legislation.

8. Contact details

All communications should be sent to the Clerk at clerk@terringtonpc.co.uk.