ACTON TURVILLE PARISH COUNCIL

DATA PROTECTION POLICY

1. INTRODUCTION

Acton Turville Parish Council ('the Parish Council') has a statutory duty to comply with the General Data Protection Regulations (GDPR) 2018 and the Data Protection Act 2018. This policy document sets out how we seek to discharge our responsibilities to protect personal data, and ensure that Councillors and Officers understand the rules governing their use of personal data in the course of their work.

2. DATA PROTECTION AND THE PARISH COUNCIL

The GDPR and the DPA 2018 place controls on the processing of personal data. Personal data is any data which concerns a living and identifiable individual, who can be identified directly from that data, or indirectly by reference to other data held. Such personal data can be a name, photo, address, email address, bank details, or other information which uniquely identifies an individual.

Processing includes obtaining, recording, holding or using information.

The Parish Council processes personal data to enable it to

- carry out its statutory duties
- represent its parishioners
- provide and promote its services
- maintain its accounts and records, and
- manage its employee(s) and contractors.

The Parish Council will comply with the GDPR and the DPA 2018 by ensuring that personal data:

- is processed lawfully, fairly and in a transparent manner
- is for specified, explicit and legitimate purposes
- is adequate, relevant and limited to those purposes
- is accurate, kept up to date and only held for as long as necessary
- is secure

3. GENERAL PROVISIONS

The Parish Council will be the registered Data Controller with the Information Commissioner's Office, ICO, and so has ultimate responsibility for ensuring compliance with data protection legislation. The Clerk will be registered as the main contact for the Parish Council with the ICO.

The Parish Council is not required to appoint a Data Protection Officer. Implementation of the procedural requirements of the policy will be effected and monitored by the Parish Clerk as part of their job description's specified responsibility to ensure that statutory and other provisions governing or affecting the running of the Council are observed. NB - Should small Parish Councils be confirmed in the future as public authorities for the purposes of the GDPR, the appointment of a Data Protection Officer will be made.

The Parish Council processes personal data in the following ways:

- pursuing the legitimate interests of its duties as a public body and maintaining the information required by law
- recording and maintaining details about its Councillors, employee(s), partners and volunteers
- recording details concerning individuals who contact it on any matter relevant to its defined duty, access its services or facilities, or raise a complaint;
- maintaining records on its current, past and potential employees

The Parish Council's right to process personal data is defined under Articles 6 (1) (a), (b) and (e) of the GDPR as follows:

(a) processing is with consent of the individual;

(b) processing is necessary for the individual to enter into or for the performance of a legal contract

(e) processing is necessary for the legitimate interests of the Parish Council.

4. MANAGEMENT OF PERSONAL DATA

The use of personal data shall be minimised so far as is reasonably practicable. Documents including agendas, minutes, governance documents, as well as all Parish Council text and documents published on the Parish Council's website, will not contain personal data unless this is unavoidable, and the inclusion has been deemed lawful for the purpose or the data subject has given consent. The lawful basis will be documented alongside the reference to the personal data. Where possible, records should use generic references such as Parishioner, Planning Officer etc.

In the circulation of documents provided by other authorities for purposes such as planning proposals, consultation documents and regulatory notices etc, the lawful processing requirement of any personal data will be considered to be satisfied because a statutory right of inspection applies and because the supplying authority will be assumed to have stated in its literature that letters of representation may be seen by others.

Where it is necessary to obtain consent to hold personal data this will:

- be obtained by the Clerk;
- use the standard Parish Council consent form which will include reference to an individual's data rights;
- be filed so as to facilitate retention/update/deletion under the specified timescales.

Emails sent to personal email accounts regarding Parish Council business must be forwarded to the Clerk to check if Personal Data is included, so that the Clerk can confirm any necessary additional action to ensure lawful processing.

Personal Data will not be shared or provided to any other third party or be used for any purpose other than that for which it was provided.

Personal Data will not be transferred outside the United Kingdom.

5. DOCUMENT MANAGEMENT

Data Retention

The Parish Council shall retain personal data for no longer than is strictly necessary. What is necessary will depend on the circumstances of each case, including the reasons why the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Documents which include personal data processed under lawful purposes not requiring a time limited consent will be retained for the minimum retention period in accordance with the Parish Council's Document Retention Policy.

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
- 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 must be locked away securely when they are not being used
- The Council must approve any cloud used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the council's backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

6. REPORTING BREACHES

It is the duty of all Councillors to report any actual or suspected breaches in information security to the Clerk

This allows the Council to:

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

The Clerk will report any data breach to the ICO as soon as reasonably practicable. If the incident involves or impacts personal data it must be reported to the ICO within 72 hours.

Breaches may result in disciplinary action in accordance with the Council's Conduct or Capability procedures and, in certain circumstances may be considered to be gross misconduct, resulting in dismissal. It should also be noted that breach of the policy could also lead to criminal or civil action if legal material is involved or legislation is contravened. Councillors found to be in breach of this policy may also be deemed to have breached the Code of Conduct and referred to the District Council's Monitoring Officer.

7. RIGHTS OF THE INDIVIDUAL

Under the Data Protection Act 1998, individuals are entitled (subject to certain exceptions) to request access to information held about them by submitting a Subject Access Requests (SAR). Upon receipt of such a request, the Parish Clerk should provide 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. An individual may also request that their data is transferred directly to another system. This must be done for free.

Furthermore, an individual 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.

8. COMPLAINTS

Complaints regarding the processing of personal data should be made to the Clerk or the ICO

on email casework@ico.org.uk, or Tel: 0303 123 1113.

9. TRAINING AND COMPETENCE

All staff will receive appropriate training on this policy. New joiners will receive training as part of the induction process. Refresher training will be provided at least every two years or whenever there is a substantial change in the law or the Parish Council's policy and procedure.

Completion of training is compulsory. Training records shall be maintained by the Parish Clerk.

10. DATA AUDIT AND REGISTER

Regular data audits to manage and mitigate risks will inform the data register. 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.

11. MONITORING

The Parish Council has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

12. POLICY REVIEW

This policy will be subject to continual monitoring and be reviewed at least every two years to ensure continued compliance with legal requirements and best practices.

Signed:

Chair…*Signed on original*

Clerk… *Signed on original*

Date Adopted: April 2026

Date of Last Review: April 2026

Date of Next Review: April 2027