Culmington Parish Council

Data Security Policy

Adopted: 6th January 2026
Review: January 2029

Data security means keeping council information safe, accurate, and only accessible to the right people. Risks often arise when data is moved outside secure council systems, such as onto personal email accounts or devices, where it can be lost or mishandled. This Data Security Policy sets the ground rules for how information is stored, shared, and protected. It aligns with this council's IT Policy and cover both security measures for the council systems (e.g. passwords, backups, and locked storage) and rules on transferring out of council systems, ensuring everyone works consistently, protects individuals' privacy, and makes it easier to handle data requests or breaches.

The council follows the General Data Protection Principles which state that personal information must be:

- Processed fairly, lawfully and transparently
- Obtained for a specific, explicit and legitimate purpose
- Adequate, relevant and limited to what is necessary
- Accurate and where necessary up to date
- Not kept longer than is necessary
- Handled ensuring appropriate security

When Culmington Parish Council processes personal information it must have a lawful basis for doing so as defined by the UK Data Protection Regulations and the General Data Protection Regulations 2018.

Personal information must not be given to anyone internally or externally, unless the person giving the information is satisfied that the receiver is authorised and legally entitled to the information. Only the minimal amount of data should be given and a secure method of transfer used.

Individuals Rights

Individuals have rights under the UK DPR and the GDPR 2018. They are:

- The rights to be informed
- The right to access
- The right to rectification
- The right to erasure

- The right of data portability
- The right to object
- The rights related to automated decision making/profiling.

Responsibility — The Clerk oversees data security on behalf of Culmington Parish Council.

Passwords – All council emails, laptops, storage drives and websites must be password protected and the password kept confidentially and changed regularly.

Physical security — Paper files must be kept in a locked cupboard/filing cabinet.

Who has access to different files or systems – the clerk and councillors have access to all council emails, laptops, storage drives, websites and locked paper files. Deliberate unauthorised use is strictly forbidden.

Backups – Data is stored on Microsoft One Drive, which is password protected and automatically backs up data.

Deletion – The Retention of Documents Schedule must be referred to before deleting data. Data is securely erased when no longer needed from emails/laptop/One Drive. Paper documents are shredded.

Personal Devises:

- Email — Councillors use personal devises to access their emails. The clerk can only access emails and data via the council laptop.
- Storage — One Drive is the authorised data storage system for all electronic data.
- Restrictions — Whether downloading council files to personal devices is allowed.
- Equipment — The council does not provide equipment for councillors. The Council provides a laptop for specific use of the Clerk.
- Instant messaging/social media – the council does not use any social media or instant messaging.

Security Incidents:

The Council has a responsibility to monitor and record and investigate incidents which may breach its personal information security.

Definition — loss of laptop, unauthorised access to laptop/onedrive/paper data storage facility, damage to data, email sent in error, hacking attempt.

Responsibility — The Clerk will lead the response to a data breach.

Reporting — Councillors should report any breach immediately to the clerk.

Timescales — Key actions within the 72-hour window. The council has one month to respond to a Subject Access Request (SAR) provided the applicant has stated the nature of their request and provided suitable proof of identity. An extension may be applied when a request is complex, and the requester should be informed of the extension. The Council has a responsibility to monitor and record and investigate incidents which may breach its personal information security.

Escalation — the clerk is authorised to fix issues and if necessary seek Information Technology support, and when to notify the ICO.

Record keeping — Breaches are recorded in the folder entitled Data Breach Record and the policy and procedures are reviewed at the next Parish Council meeting.

Accountability:

The council demonstrates its compliance with the legislation by

- Having appropriate policies in place
- All activities/processes/services must have data protection enshrined within its design
- Use data processing agreements in contracts
- Maintain records of data processing activities
- Implement organisational security
- Monitor, investigate and record and where necessary report data breaches
- Complete data audits and impact assessment
- Have an appropriately skilled Data Protection Officer
- Review the policies and procedures regularly