Finsbury Place, Ashdown Close,
Sticker, PL26 7EU

T 07716 896635
clerk@keaparishcouncil.org.uk
www.keaparishcouncil.org.uk

KEA PARISH COUNCIL – DATA PROTECTION AND DATA BREACH POLICY

1. Purpose

Kea Parish Council holds and processes information in order to carry out its duties and provide services to the community. This policy sets out how the Council protects personal data and other information to ensure it is handled lawfully, securely and responsibly.

The Council is committed to complying with:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- Relevant guidance issued by the Information Commissioner's Office (ICO)

This policy applies to councillors, employees, contractors and any other authorised persons who process information on behalf of the Council.

2. Data Protection Principles

Personal data must be handled in accordance with the principles of data protection law. Personal data must be:

1. Processed lawfully, fairly and transparently.
2. Collected for specified and legitimate purposes.
3. Adequate, relevant and limited to what is necessary.
4. Accurate and kept up to date.
5. Kept only as long as necessary.
6. Stored securely and protected from unauthorised access, loss or damage.

3. Responsibility for Data Protection

The Parish Clerk is responsible for overseeing data protection and data security within the Council.

Responsibilities include:

- ensuring compliance with data protection legislation
- maintaining appropriate data security arrangements
- managing data breach responses
- responding to requests from individuals regarding their data.

All councillors, staff and authorised users are responsible for following this policy and protecting council information.

4. Data Security

4.1 General Security

Council information must be protected against unauthorised access, loss, damage or misuse.

Information may exist in various forms including:

- electronic records
- emails
- paper documents
- photographs
- audio recordings.

Security measures must be applied to all forms of information.

4.2 Password Security

Passwords must be used to protect access to council systems and accounts.

Users must:

- create strong passwords (for example using three random words)
- keep passwords confidential
- not share passwords with others
- change passwords immediately if compromise is suspected.

4.3 Multi-Factor Authentication

Where available, multi-factor authentication (MFA) should be used for council systems, particularly email accounts and cloud storage platforms.

MFA provides an additional layer of protection beyond a password.

4.4 Physical Security

Paper files and physical records containing council information must be stored securely.

This may include:

- locked cabinets
- secure offices
- restricted access to keys or storage areas.

Sensitive documents should not be left unattended in public areas.

Documents containing personal data must be disposed of securely, for example by shredding.

4.5 Access Control

Access to council information should be limited to those who need it for legitimate council purposes.

The Clerk is responsible for ensuring appropriate access controls are in place for:

- council email accounts
- document storage systems
- council devices.

4.6 Backups

Council data must be backed up regularly to reduce the risk of data loss.

Backups may be maintained through secure cloud systems or other approved backup systems.

Backup procedures should ensure that important council records can be restored if necessary.

4.7 Data Retention and Deletion

Council records must be retained in accordance with the Council's records retention arrangements.

Personal data must not be kept longer than necessary.

When information is no longer required it must be securely deleted or destroyed.

5. Use of Personal Devices (Bring Your Own Device)

The Council recognises that councillors and staff may sometimes use personal devices such as laptops, tablets or smartphones for council work.

Where personal devices are used, the following rules apply.

Users must:

- protect devices with a password or PIN
- keep devices updated with security updates
- ensure council data cannot be accessed by other users of the device.

Council information should normally be stored within council systems rather than permanently on personal devices.

If council data is temporarily stored on a personal device, it must be deleted once no longer required.

Any loss or theft of a personal device containing council data must be reported immediately to the Clerk.

6. Email and Data Storage

Council information should be handled using approved systems.

Email

Council business should be conducted using official council email accounts wherever possible.

Personal email accounts should not be used to store or manage council data.

Storage Platforms

Council data should be stored only on authorised systems such as council-approved cloud storage or council devices.

Council documents must not be stored on personal cloud storage accounts unless specifically authorised.

7. Use of Instant Messaging and Social Media

Messaging platforms such as WhatsApp, Facebook Messenger or similar applications should not be used to store or manage council records.

Such platforms may only be used for limited communication where appropriate, and they must not be used to share confidential or sensitive information.

Council decisions must always be made in accordance with proper council procedures and not through informal messaging platforms.

8. Data Breach Policy

8.1 Definition of a Data Breach

A personal data breach occurs when personal data is accidentally or unlawfully:

- lost
- destroyed
- altered
- disclosed
- accessed by unauthorised persons.

Examples include:

- sending an email containing personal data to the wrong person
- losing a laptop or memory device containing council data
- unauthorised access to council systems
- accidental publication of personal information.

8.2 Reporting a Data Breach

Any councillor, employee or authorised person who becomes aware of a potential data breach must report it immediately to the Clerk.

Prompt reporting allows the Council to assess the situation and take appropriate action.

8.3 Responding to a Data Breach

The Clerk will assess the breach and determine:

- the type of data involved
- the number of individuals affected
- the risks to individuals' rights and freedoms.

Where necessary the Council will take steps to contain the breach and prevent further damage.

8.4 Notification to the Information Commissioner's Office

Where a data breach presents a risk to individuals' rights and freedoms, the Council must report the breach to the Information Commissioner's Office (ICO).

This must be done within **72 hours** of becoming aware of the breach.

Where required, affected individuals will also be informed.

8.5 Recording Data Breaches

All data breaches, whether reportable or not, will be recorded in a Data Breach Log maintained by the Clerk.

This helps the Council learn from incidents and improve data security.

9. Rights of Individuals

Individuals have legal rights regarding their personal data, including:

- the right to access their personal data (Subject Access Request)
- the right to request correction of inaccurate information
- the right to request deletion of data in certain circumstances
- the right to restrict or object to processing.

Requests may be made verbally or in writing.

All such requests must be passed to the Clerk as soon as possible.

The Council will normally respond within **one calendar month**, in accordance with legal requirements.

Requests for deletion may be refused where the Council is legally required to retain records.

Individuals who are not satisfied with the Council's response may raise concerns with the Information Commissioner's Office.

10. Policy Review

Kea Parish Council reserves the right to review and amend this policy from time to time to ensure that it remains effective, up to date and compliant with relevant legislation and guidance.

Any amendments will be approved by the Council and recorded in the Council's minutes.

Adopted	19th March 2026
Min ref	41/26
Review date	2028