Great Tey Parish Council

Data Security Policy

1. Purpose:

Great Tey Parish Council is committed to protecting the security, confidentiality, and integrity of the information it holds. Data security means ensuring that council information is kept safe, accurate, and accessible only to authorised individuals.

Risks to data security can arise when information is removed from secure council systems, for example by being transferred to personal email accounts or stored on personal devices. This policy sets out the rules and responsibilities for protecting council data and reducing the risk of loss, misuse, or unauthorised access.

This policy should be read alongside the Council's IT Policy and applies to all councillors, employees, contractors, and volunteers who handle council information.

2. Scope:

This policy applies to:

- All council data, whether held electronically or in paper form
- All systems, devices, and storage used for council business
- All individuals who process or access council data

3. Responsibilities:

Overall responsibility for data security rests with the Clerk, who acts as the Council's principal data controller and oversees compliance with this policy.

All councillors, employees, contractors, and volunteers are responsible for:

- Following this policy and related IT policies
- Protecting any council data they access or handle
- Reporting suspected data breaches or security incidents promptly to the Clerk

4. Password Security:

- All council systems and accounts must be protected with strong passwords.
- Passwords must be unique and not reused across personal accounts.
- Passwords must be kept confidential and not shared with others.
- Passwords must not be written down or stored insecurely.
- Passwords should be changed immediately if compromise is suspected.

5. Multi-Factor Authentication (MFA):

- Multi-factor authentication must be enabled wherever available, particularly for email, cloud storage, and remote access systems.
- MFA must not be disabled without approval from the Clerk.

6. Physical Security:

- Paper records must be stored securely in locked cabinets or rooms when not in use.
- Keys to council premises, cabinets, or equipment must be kept secure and issued only to authorised individuals.

- Council-owned devices, including laptops and tablets, must be stored securely and not left unattended in public places.

7. Access Control:

- Access to council data and systems will be restricted to individuals who require it for their role.
- Different levels of access may be applied depending on responsibilities.
- Access rights must be reviewed regularly and removed promptly when roles change or end.

8. Data Backups:

- Council data must be backed up regularly to protect against loss, corruption, or system failure.
- Backups must be stored securely and, where possible, separately from live systems.
- The Clerk is responsible for ensuring appropriate backup arrangements are maintained.

9. Secure Deletion and Disposal:

- Council data must be securely deleted or destroyed when no longer required, in accordance with the Council's retention schedule.
- Electronic data must be permanently erased so it cannot be recovered.
- Paper records must be shredded or disposed of securely.

10. Bring Your Own Device (BYOD):

The use of personal devices for council business is permitted only with approval from the Clerk and subject to the following conditions:

a) Email:

- Council business must only be conducted using authorised council email accounts.
- Personal email accounts must not be used to send, receive, or store council data.

b) Storage:

- Council data must only be stored on authorised platforms, such as approved cloud services including OneDrive or SharePoint.
- Council files must not be stored on personal cloud services or personal device storage without explicit approval.

c) Device Security:

- Downloading council files to personal devices should be avoided wherever possible.
- Where authorised, devices must be protected by passwords, encryption, and up-to-date security software.

d) Equipment Standards:

- Where practical, the Council will provide devices for council work.
- Personal devices used for council business must meet minimum security standards and be kept up to date.

11. Instant Messaging and Social Media:

- Instant messaging services, including WhatsApp, and social media platforms, including Facebook, must not be used for formal council business, decision-making, or sharing sensitive information.
- Such platforms may only be used for limited informal communication where appropriate and approved.
- Council records must not be stored solely on messaging or social media platforms.

12. Data Breaches:

Any actual or suspected data breach must be reported immediately to the Clerk. The Clerk will assess the incident and take appropriate action in accordance with data protection requirements.

13. Review:

This policy will be reviewed regularly and updated as necessary to reflect changes in legislation, technology, or council practices.