Dennington Parish Council

DATA & EMAIL POLICY

To be considered: January 2026

Next review: May 2026

1. Introduction

Dennington Parish Council recognises the importance of using information technology (IT) and email safely, responsibly and securely to support its work and communications.

This policy sets out simple and practical rules for councillors, the Clerk and any other authorised users when using IT and email for Parish Council business.

2. Scope

This policy applies to all councillors, the Clerk and any volunteers or contractors who handle Parish Council information or communicate on behalf of the Council.

It applies regardless of whether Council business is conducted using Council-provided systems or personal devices.

All users must comply with relevant legislation, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Freedom of Information Act 2000.

3. Acceptable Use

IT systems and Council emails must be used **primarily for Parish Council business**.

- Limited personal use is acceptable provided it does not interfere with Council business or breach this policy
- Users must act professionally, respectfully and lawfully at all times
- Illegal, offensive or inappropriate material must not be accessed, stored or shared

4. Devices and Software

- Parish Council business should only be carried out using trusted devices and software
- Users must not install unapproved software that could pose a security risk
- USB sticks or external storage devices should not be used for Council data unless necessary and approved by the Clerk

5. Data Protection and Security

All Parish Council information must be handled carefully.

Users must ensure that:

- Personal and sensitive data is kept secure
- Data is only shared with those who have a legitimate need to see it
- Council data is not stored unnecessarily or indefinitely
- Information is deleted securely when no longer required

Council information should not be stored on personal devices unless necessary and appropriate safeguards are in place.

6. Internet and Online Use

Internet access should be used responsibly and mainly for Parish Council purposes.

- Copyright laws must be respected
- Council-related social media or website content must be accurate, appropriate and authorised
- Excessive or inappropriate internet use is not permitted

7. Email Use

Email is the primary method of conducting Parish Council business. Councillors will use the councils' .gov official email addresses for all Council Business.
Users must:

- Use a clear, professional and courteous tone
- Avoid sending sensitive or confidential information unless absolutely necessary
- Use BCC when emailing multiple external recipients to protect personal data
- Be alert to phishing emails and suspicious links or attachments

Personal email accounts and messaging apps (such as WhatsApp) must **not** be used to make decisions, give instructions, or conduct formal Council business. Any substantive matters discussed informally must be confirmed by email.

All Council emails form part of the official record and may be subject to Freedom of Information requests. All emails, whether on mobile phones or PCs, can be subject to access by the ICO or Courts if there are concerns that full disclosure for Subject Access Requests (SAR) or FOI requests has not occurred.

When councillors leave office, they must not retain or continue to use Council information obtained during their term. They must provide written confirmation to the clerk that they have removed or deleted Council data from all devices.

8. Passwords and Account Security

Users are responsible for keeping their accounts secure.

- Passwords should be strong and kept private
- Passwords must not be shared
- Multi-factor authentication should be used where available
- Accounts should be secured when devices are left unattended
- To protect Council data from unauthorised access to Council business Councillors should ensure that they have recognised and adequate virus software on their PC.

9. Remote Working

When accessing Parish Council information remotely:

- Users must ensure devices are secure
- Public or unsecured Wi-Fi should be avoided where possible
- Council data must not be left visible or accessible to others

10. Monitoring

The Parish Council reserves the right to access or review Council email and data where necessary for legal, audit, continuity or security reasons, in line with data protection legislation.

11. Retention of Information

Council emails and documents must be kept in accordance with legal requirements and the Council's retention arrangements. All Council documents that are received and are stored on Councillors' computers, tablets or mobile phones that contain personal information should be relevant and necessary, any names and addresses of people should be deleted when the business has been completed and finalised.

Users should:

- Keep records that relate to Council decisions or actions
- Delete duplicate or unnecessary emails
- Assist the Clerk in maintaining orderly records

12. Reporting Incidents

Any suspected data breach, security issue or loss of Council information must be reported to the Clerk as soon as possible. This includes:

- Suspicious emails
- Accidental disclosure of personal data
- Lost or stolen devices containing Council information

13. Training and Awareness

Users are expected to familiarise themselves with this policy and follow good data protection and cyber security practices.

14. Social Media

Councillors using their own social media accounts must ensure that any comments made is clearly defined as their own and not representative of the Council.

15. Breaches of Policy

Failure to comply with this policy may result in:

- Loss of access to Council systems
- Formal action by the Parish Council
- Further steps where required by law
- The clerk will be the responsible officer for the administration of this policy on behalf of Dennington Parish Council and will report breaches to the ICO, the Chair or all Council members as appropriate.

16. Review

This policy will be reviewed annually or sooner if required due to changes in legislation or working practices.