GREAT LONGSTONE PARISH COUNCIL
INFORMATION TECHNOLOGY AND USE OF SOCIAL MEDIA POLICY

Table of Contents

1. Introduction

Great Longstone Parish Council recognises the importance of effective, secure, and responsible use of information technology (IT), email, and social media in supporting its business, operations, and communications. This policy outlines the guidelines and responsibilities for the appropriate use of IT resources, email, and social media platforms by all council members, employees, volunteers, and contractors.

As a small council operating without a dedicated office or network, this policy is particularly focused on the use of personal devices, remote working, and online conduct, which are the primary ways council business is conducted and how the council is represented publicly.

2. Scope

This policy applies to all individuals who use Great Longstone Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts, regardless of whether those devices are council-owned or personal. It also applies to the use of social media platforms, whether accessed on council or personal accounts, where that use relates to council business or could reasonably be associated with an individual's role on the council.

3. Use of Council Devices and Email

All council activity must be conducted in accordance with this policy, whether carried out on a council-owned device, a personal device, or via email or social media. Users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing, downloading, or sharing inappropriate, offensive, or unlicensed content.

Where the council provides equipment, the device remains the property of the council at all times and must be returned in good working order on leaving the role, with all council data intact. Council-owned devices must not be used by anyone other than the authorised user, and no unauthorised software should be installed.

Email accounts provided by the council are for official communication only. Emails should be professional and respectful in tone, and confidential or sensitive information must not be sent via email unless encrypted. Users should exercise caution with attachments and links, and verify the source before opening anything from an unexpected or unfamiliar sender.

Limited personal use of council-owned devices and email accounts is permitted, provided it does not interfere with council duties or violate any part of this policy.

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

As a small council, councillors, staff, and other authorised users will typically use their own personal devices (including smartphones, tablets, and laptops) to carry out council business. This is accepted and supported, subject to the following requirements.

All users accessing council data or systems on personal devices must:

- Protect their device with a strong password, PIN, or biometric lock, and ensure it locks automatically after a short period of inactivity.
- Keep their device’s operating system and apps up to date so that security vulnerabilities are addressed promptly.
- Use a council email account for all council-related correspondence, rather than a personal email address.
- Ensure that council data cannot be accessed by family members or others who may use the same device.
- Where the device supports separate work and personal profiles, use the work profile for all council-related activity.

- Activate remote wipe functionality where available, so that council data can be erased if the device is lost or stolen.
- Report any lost or stolen device that may contain council data to the Clerk immediately.
- Delete all council-related data from personal devices upon leaving the council.
- Not store council data in personal third-party cloud accounts (e.g. personal iCloud, Google Drive, or Dropbox), other than for documents that are already in the public domain, where those accounts are not secured to the same standard as council systems.

Users are personally responsible for their own devices. The council cannot be held liable for any damage, data loss, or costs arising from use of a personal device for council purposes.

5. Remote Working

As council members and staff work from home or other locations rather than a shared office, the following security practices apply at all times when carrying out council business remotely:

- Only use secure, trusted Wi-Fi networks when accessing council data or email. Avoid using public or unsecured Wi-Fi (e.g. in cafés, hotels, or public transport) without the use of a VPN or alternatively use a personal mobile hotspot.
- When accessing council systems from a device you do not own (for example a shared or public computer), do not save passwords, and log out fully at the end of the session, clearing browser history and any cached data. If the device does not clearly support this, do not use it to access council systems.
- Position your screen so that confidential council information cannot be read by others nearby — particularly on public transport or in public spaces. Use a privacy screen filter where possible.
- Any confidential documents printed for council purposes must be collected promptly, stored securely, and disposed of by shredding when no longer needed.
- Electronic files containing sensitive council information should be password protected.
- Council documents and devices must not be left unattended in vehicles, except for short unavoidable periods, in which case they must be stored out of sight in the boot.

6. Data Management and Security

All sensitive and confidential Great Longstone Parish Council data should be stored and transmitted securely using approved methods. Regular data backups should be performed to prevent data loss, and secure data destruction methods should be used when necessary. Unauthorised installation of software on any council owned device is prohibited.

7. Email Communication

Email accounts provided by Great Longstone Parish Council are for official communication only. Emails should be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless encrypted.

Users should exercise caution with attachments and links to avoid phishing and malware. Always verify the source before opening any attachment or clicking a link from an unexpected or unfamiliar sender.

8. Password and Account Security

All users are responsible for maintaining the security of their accounts and passwords. The council follows the National Cyber Security Centre (NCSC) recommendations, which include:

- to create long memorable passwords using three random words (e.g. PurpleCandleRiver).
- to not reuse the same passwords across different sites
- not be sharing your passwords with other people
- using password managers to generate and store unique complex passwords for every site
- ensure that your email password is particularly strong, as it is the gateway to resetting all the others. Enabling Multi-Factor Authentication (MFA), where it is available. This requires a second form of verification (such as a code sent to your phone) in addition to a password and significantly reduces the risk of unauthorised access.
- that if you must write passwords down to keep them physically secure and never with the device.

9. Use of Social Media

Social media includes blogs, social networking sites (such as Facebook, X, Instagram, LinkedIn, and NextDoor), messaging apps, and similar platforms. The following rules apply to all councillors, staff, and authorised users, whether posting in a council capacity or on personal accounts, and whether during or outside of working or council hours.

9.1 Personal Liability and Identity

Councillors and staff are personally liable for anything they post online. Any post that could reasonably be associated with your role on the council — even if the council is not named — reflects on the council's reputation. Councillors should be mindful of the Members' Code of Conduct and the Nolan Principles at all times, including in personal online activity.

9.2 Not Speaking on Behalf of the Council

Unless you have been explicitly authorised to do so, you must not post content that could be read as an official statement or position of the council. Where you post about council matters on a personal account, include a clear disclaimer such as: "These views are my own and do not represent the views of Great Longstone Parish Council."

9.3 Confidentiality

Do not post any information that is confidential, relates to matters discussed in closed (exempt) session, or that has not been formally published by the council. This includes details of personnel matters, complaints, financial arrangements, or any information relating to individuals that could breach data protection legislation.

9.4 Resolving Concerns Appropriately

Social media is not an appropriate channel for raising complaints or concerns about the council or its members. Any concerns should be raised directly with the Clerk or through the council's formal complaints procedure.

9.5 Conduct

Posts must not be abusive, harassing, discriminatory, or defamatory towards any individual, including other councillors, staff, parishioners, or partner organisations. Breach of this section may constitute misconduct and could result in formal action.

10. Email Monitoring

Great Longstone Parish Council reserves the right to monitor email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act 2018, UK GDPR, and the Investigatory Powers (Interception by Councils) Regulations 2018, and only where there is a legitimate and proportionate reason to do so. Users will be informed if monitoring is taking place.

11. Reporting Security Incidents

All suspected security breaches or incidents — including lost or stolen devices, accidental disclosure of sensitive information, or suspected phishing attacks — should be reported immediately to the Clerk for investigation and resolution.

12. Training and Awareness

Great Longstone Parish Council will provide guidance and resources to help users understand IT security best practices, data protection responsibilities, and how to stay safe online. All councillors and staff are expected to familiarise themselves with this policy.

13. Compliance and Consequences

Breach of this IT Policy may result in the suspension of IT access and further consequences as deemed appropriate, including, for employees, formal disciplinary action. For councillors, breaches involving conduct on social media or relating to confidential information may be referred under the Members' Code of Conduct.

14. Contacts

For IT-related enquiries or to report a security incident, contact the Parish Clerk at clerk@greatlongstone-pc.gov.uk

15. Reviewing the policy

This is a non-contractual procedure which will be reviewed, in line with the Great Longstone Parish Council Standing Orders, that all Policies will be reviewed on a 12 monthly basis for applicability in line with changes in current legislation and requirements of the Council.

All policies therefore, will be reviewed and adopted at the Annual General Meeting of the Parish Council, irrespective of the date on which they were initially written.

Date of policy: 11th March 2026
Approving body: Full Council
Date of meeting: 11th March 2026
Policy version reference: 1.0
Policy effective from: 12th March 2026
Date for next review: July 2026