LOSTOCK GRALAM
PARISH COUNCIL

LOSTOCK GRALAM PARISH COUNCIL

INFORMATION TECHNOLOGY (IT) POLICY

1. Introduction

Lostock Gralam Parish Council uses information technology to support its work and to communicate with residents, councillors and partners. This policy sets out how council IT equipment, systems and accounts must be used to ensure security, good governance and compliance with data protection laws.

This policy applies to all councillors, employees and authorised volunteers who use council IT systems or handle council information.

2. Purpose of This Policy

The aims of this policy are to:

- Protect council information and digital records
- Ensure safe and appropriate use of devices and accounts
- Reduce the risk of data loss, cyber incidents or misuse
- Provide simple rules for using email, the internet and personal devices
- Clarify what is acceptable use of council IT resources

3. Equipment and Computer Use

3.1 Council-owned equipment

- Council IT equipment (such as laptops, tablets or mobile phones) is provided for council business.
- Users must take reasonable care of equipment and keep it in a clean and safe condition.
- All devices must be locked or password-protected when left unattended.
- No hardware or software should be purchased or installed without approval from the Clerk or Council.
- Any faults, damage or concerns should be reported to the Clerk.

3.2 Personal devices used for council work

Some councillors and staff may use their own devices (e.g., phones or laptops) for council work. To protect council information:

- Devices must be kept up to date with security updates.
- Council emails must only be sent from official council email accounts.
- Council documents must not be stored permanently on personal cloud services, unencrypted USB sticks or unprotected devices.
- Council information should be stored separately from personal data (e.g., in a separate folder or work profile).
- Personal devices used for council work must be password/PIN protected.

The council may need temporary access to a device to retrieve council information for legal reasons.

4. Data Security, Passwords & Authentication

To protect council information:

- Passwords must follow NCSC guidance (such as using three random words).
- Passwords must not be shared with anyone.
- Multi-Factor Authentication (MFA) must be used where available.
- If a password is believed to be compromised, it must be changed immediately.
- Council data must only be stored or backed up in council-approved locations (for example, the council's email system or a secure shared drive).

5. Backups

The Council will ensure that key digital information and documents are backed up regularly using a secure and approved method.
Backups will be checked occasionally to make sure they can be restored if needed.

6. Monitoring

The Council does not routinely monitor IT use, but may do so when necessary, for example:

- Investigating suspected misuse
- Recovering lost information
- Responding to a legal request

- Ensuring security following a suspected breach

Any monitoring will be lawful, proportionate and carried out by the Clerk or the Council's IT provider.

7. Remote Working

Where councillors or staff work from home:

- Council information must be kept secure and not accessible to other household members.
- Devices must be locked when not in use.
- Public or unsecured Wi-Fi must not be used unless a secure (encrypted) connection is available.

8. Email Use

- Council email accounts must be used for all council business.
- Personal email accounts must not be used for council work.
- Users should be cautious about opening attachments or links from unknown sources.
- Confidential information must be shared securely (not via personal email or messaging apps).
- Email accounts may be withdrawn if misused.

9. Internet Use

- Users must comply with copyright law—online content is not automatically free to copy.
- Users should only access websites that are appropriate and safe.
- Personal browsing should be limited and must not interfere with council work.
- No council trademarks, logos or new domains may be created without council approval.

10. Social Media

This section covers:
Facebook, X/Twitter, Instagram, TikTok, YouTube, WhatsApp, local forums, blogs and other online platforms.

10.1 Council-related use

- Only authorised users may post on official council social media accounts.
- Official council accounts must be accessible to the Clerk and the Council.
- Council information must not be posted without approval.

10.2 Personal use by councillors and staff

- Personal posts must not imply they represent the Council unless authorised.
- Personal views should be clearly marked as personal.
- Confidential, sensitive or internal council information must not be shared.
- Users must not post defamatory, discriminatory or offensive content about the Council, residents or colleagues.

11. Data Protection and Breach Reporting

The Council must comply with the UK GDPR and its own Data Protection Policy.

- Any loss of council data, accidental disclosure or suspected breach must be reported immediately to the Clerk.
- The Clerk will assess whether the incident needs reporting to the ICO.

12. Misuse of IT Systems

Misuse includes (but is not limited to):

- Sharing passwords
- Accessing inappropriate websites
- Using council accounts for personal business
- Posting unauthorised information online
- Storing council data insecurely

Serious misuse may result in withdrawal of access, reporting to the Council, or disciplinary action (for employees).

13. Review of This Policy

This policy will be reviewed every two years or sooner if required by changes in legislation or council practice.