Lavendon Parish Council

Information Technology Policy

Adopted: 10th November 2025

1. Purpose

The purpose of this policy is to ensure that all employees, Councillors and any third parties using Parish Council information technology (IT) have a clear understanding of what is and is not permitted. This will ensure the appropriate use of the Council's equipment, safeguard the security of its IT systems and data, and assist compliance with Data Protection law. The policy should be read in conjunction with the Council's Data Protection Policy.

2. Policy Coverage

This policy covers the security and use of all Lavendon Parish Council's information and IT equipment. It also includes the use of email, internet and mobile IT equipment. This policy applies to the Clerk (as the Council's sole employee), Councillors and contractors, when using Council 's equipment and software.

The policy applies to all information, in whatever form, relating to the Council's activities, and to all information handled by the Council relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by the Council or on its behalf.

3. IT Provision

The Council provides a laptop and other input and out devices to the Clerk which at all times remains the property of the Council and are to be used for Councill business.

The Council's internet and email are intended for business use. Personal use is permitted where such use does not interfere with work responsibilities, is not detrimental to the Council in any way, not in breach of any terms and conditions of employment and does not place the employee or the Council in breach of statutory or other legal obligations. Unauthorised installation of software or use of unlicensed products is strictly prohibited.

Access to the Council's IT system is controlled by the use of user ID and password. Strong, unique passwords must be used for all Council accounts; these must not be shared. Council

devices must be encrypted, updated, and protected with antivirus software.

All Council equipment must be returned to the Council upon termination of contract. All Council data or intellectual property developed or gained during the period of employment remains the property of the Council and must not be retained beyond the period of employment by Lavendon Parish Council.

4. Mobile Devices and Bring Your Own Device Policy

Mobile devices include, but are not limited to:
- Laptops, computers and notebooks
- Mobile phones etc.
- Any other mobile device capable of storing and connecting to a network

Use of personally owned mobile devices to access and store Council information, as well as an individual's own personal content, is commonly known as Bring Your Own Device (BYOD).

This mobile policy applies to all personally owned mobile devices that are used to access Council information, ICT facilities, including but not limited to, Council information systems, email and Council managed storage.

The policy applies to all Councillors and third parties (i.e Contractors) operating on behalf of the Council or undertaking Council functions and thereby accessing the above systems.

This policy recognises that personally owned mobile devices are and will be used to access Council information, but makes no comment on the requirement or recommendation to do so, nor does it mandate or recommend the use of personally owned mobile devices. The Council is under no obligation to modify its systems to allow users to connect their personally owned mobile devices to them where such modification may be required.

The Council, staff members and Councillors, are committed to processing all personal data in accordance with current UK Data Protection law, as specified within the Council's Data Protection Policy, regardless of the device used to access the information. Councillors are required to keep Council information and personal data secure. This applies equally to Council information held on Council systems and devices or accessed/held on personally owned mobile devices. The Council reserves the right to refuse to allow access to devices or software where it considers that there is security or other risk to its information or IT systems.

The Council is the owner of all Lavendon Parish Council information and the contents of the Council's systems together with everything which is created on, transmitted to, received on or printed from, or stored or recorded on each mobile device, in each case during the course of the Council's business or otherwise on the Council's behalf, irrespective of who owns that mobile

device.

The Council reserves the right to request access to inspect or delete Council information held on a personally owned mobile device to the extent permitted by law and for legitimate business purposes. Every effort will be made to ensure that the Council does not access the private information of the individual.

5. User Responsibilities

Mobile Device Users are responsible for:

- The security of Council information and of the device on which the information is held.
- Storing Council information on the mobile device only for so long as necessary.
- Deleting Council information from the mobile device when no longer required, or sooner if required by the Council to delete it.
- Ensuring where possible that the device has an up-to-date operating system and antivirus protection.
- Complying with this policy and the related policies.

6. Data Access and Storage

Use of any personally owned mobile device for Council purposes is at the user's risk and the Council is not liable for any losses, damages, or liability arising out of such use, including but not limited to loss, corruption or misuse of any content or loss of access to or misuse of such personally owned mobile device, its software or its functionality.

Confidential or sensitive information should be stored within and accessed from Council information systems and Council managed storage to ensure security of and appropriate secure access to the information.

Users should only store the minimum amount of information necessary to carry out the required task on a mobile device. A temporary cache may be held on the device; therefore, any confidential, sensitive, or personal information should be deleted from the device as soon as the information is no longer required.

7. Device and Physical Security

Information should be protected against loss or compromise when working remotely, for example at home or in public places. Mobile devices accessing Council information must have strong (4 or more alphanumeric characters/pattern) passwords, passcode or PIN enabled to reduce opportunity for unauthorised access. These must be kept secure. The device should be set to automatically lock if inactive for 5 minutes or less, or locked manually using Ctrl, Alt and Delete keys.

Mobile devices used to access or store confidential, personal, or sensitive data should be subject to additional protection measures (such as encryption) to reduce opportunities for loss or compromise of the information. Mobile devices should, where possible, have operating system and antivirus updates enabled.

Councillors must delete all Council information from their device at the end of any period of holding office, or if the device is repaired, exchanged, sold, given away or otherwise disposed of. Councillors may be required to provide a written undertaking that this will be done. Without relieving users of their obligation to delete all Council information, Lavendon Parish Council's rights under the above apply, including after termination of employment.

8. Council Owned Information Held on Third Party Web Sites

All Council information produced, collected, and/or processed remains the property of the Council. This applies regardless of where the information is stored, including on third party platforms such as webmail service providers or social networking sites (e.g. Facebook).

9. Reporting Security Incidents

Any suspected data breach or security incident must be reported to the Clerk and the Chair immediately and, if necessary, to the Information Commissioner's Office (ICO).

10. Data Protection and Confidentiality

- The Council will comply with the UK GDPR, Data Protection Act 2018, and the Freedom of Information Act 2000.
- Personal and confidential information must be stored securely and accessed only for legitimate Council purposes.
- Councillors and the Clerk must use Council provided email addresses (not personal email accounts) for all official communications.

11. Transparency and Accountability

Emails and documents relating to Council business must be retained in an organised and accessible manner to support public inspection, audit, and accountability.

The Council's IT system must support Councillors access to accurate and complete information when making decisions.

Where cloud storage is used, it must be with reputable providers that comply with UK data protection laws.

12. Internet and Communications Use

- All digital communications must be respectful, professional, and consistent with the Council's Code of Conduct.
- Internet use must comply with the law, including copyright, licensing, and defamation.
- The Council official responsible for the Council's website must ensure that any information published online (e.g., website content) is accurate, lawful, and approved by the Council where appreciate.

13. Training and Awareness

The Council will provide regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and Councillors will receive regular training on email security and best practices. All new employees and Councillors will be given a copy of this Policy.

14. Policy Review

This policy will be reviewed at least every two years or earlier if there is a change in law, guidance, or Council practices.