LAVENHAM PARISH COUNCIL

INFORMATION TECHNOLOGY POLICY

1 Hardware

1.1 Council computer equipment is provided for Council purposes, reasonable personal use of such equipment is permitted, reasonable interpreted in the opinion of the Council.

1.2 All Councillors and staff must lock their computers when leaving their desks to prevent unauthorised access. This applies to all Council and personal devices used for work. Failure to comply by staff may lead to disciplinary action.

1.3 All Council owned computer and other electronic equipment supplied should be treated with good care at all times. Computer equipment is expensive, and any damage sustained to any equipment will have a financial impact on the Council.

1.4 Council owned Computer and electronic hardware should be kept clean, and every precaution taken to prevent food and drink being dropped or spilled onto it.

1.5 All Council owned computer and mobile equipment will carry a number which is logged against the current owner of that equipment. A database of equipment issued will be kept.

1.6 All Council owned Equipment should not be dismantled or reassembled without seeking advice.

1.7 In cases of legal proceedings against the Council the Council may need to temporarily take possession of Council owned equipment to retrieve the relevant data.

1.8 Personal disks, USB sticks, CDs, DVDs, data storage devices etc cannot be used on Council owned equipment without the prior approval of the Council.

1.9 Data on Council owned equipment should be regularly backed up.

1.10 All Council owned portable equipment must be stored safely and securely when not in use in the office, i.e. when travelling or when working from home. Such equipment (unless locked in a secure cabinet or office) should be kept with or near the user at all

times; should not be left unattended when away from Council premises and should never be left in parked vehicles.

1.11 It is important to ensure all portable devices are protected with encryption in case they are lost or stolen. All portable devices that hold Council data, including emails and files, must be protected with a pin code. Where possible, these devices should also be programmed to erase all content after several unsuccessful attempts to break in. Any security set on these devices must not be disenabled or removed.

1.12 If an item of Council owned portable equipment is lost or damaged this should be reported to the Council. If the loss or damage is due to an act of negligence, the individual responsible may be liable to meet the cost of the loss/damage.

1.13 To protect confidential information, unless it is a requirement of the job and this has been authorised, it is forbidden for photographs, sound recordings or videos to be taken on Council premises, without the prior written permission of the Council.

1.14 Under no circumstances should any non-public meeting or conversation be recorded without the permission of those present. This does not affect statutory rights (under The Openness of Local Government Regulations 2014).

1.15 In addition, the Council does not permit webcams (which may be pre-installed on many laptops) to be used in the workplace, other than for conference calls for Council purposes. If there is any doubt as to whether a device falls under this clause, advice should be sought from the Clerk.

2 Use of own devices

2.1 The Council recognises that some Councillors may wish to use their own smartphones, tablets, laptops etc to access their email and the Councils SharePoint facility. Such devices should be kept up to date so that any vulnerabilities in the operating system or other software on the device are appropriately patched or updated.

2.2 Any Council emails sent from own devices should be sent from a Council email account and should not identify the individual's personal email address.

2.3 Accessing inappropriate websites or services or material on any device via the IT infrastructure that is paid for or provided by the Council carries a high degree of risk, and, for employees, may result in disciplinary action, including summary dismissal (without notice). An example would be downloading copyright music illegally or accessing pornographic material.

2.4 Wherever possible the user should maintain a clear separation between the personal data processed on the Council's behalf and that processed for their own personal use, for example, by using different apps for Council and personal use. If the device supports both work and personal profiles, the work profile must always be used for work-related purposes.

2.5 Councillors and staff who intend to use their own devices for Council matters must:

- use a strong password to protect their device(s) from being accessed. For smartphones and tablets this should lock the device after ten failed login attempts;
- configure their device(s) to automatically prompt for a password after a period of inactivity of more than ten minutes.
- always password protect any documents containing confidential information that are sent as attachments to an email, and notify the password separately (preferably by a means other than email);
- ensure secure WiFi networks are used;
- ensure that work-related data cannot be viewed or retrieved by family or friends who may use the device;
- inform the Clerk if their device(s) is/are lost, stolen, or inappropriately accessed where there is risk of access to Council data or resources. To prevent phones being used, they will need to retain the details of their IMEI number and the SIM number of the device as their provider will require this to deactivate it.

2.6 Personal data relating to Councillors, staff, associates, residents and external stakeholders should not be saved to any personal accounts as this may breach data protection legislation or create a security risk if the device is lost or stolen,

2.7 Prior to the disposal of any device that has Council data stored on it the device must be wiped or the device returned to the Council.

3 Passwords

3.1 Initial user account passwords must be generated by the IT provider.

3.2 Default passwords provided by vendors or the IT provider must be changed immediately upon installation or setup.

3.3 Other

- Passwords are personal and must not be shared under any circumstances.
- Only the assigned user of an account may access or use the associated password.
- In exceptional cases (e.g., incident response or employee offboarding), access to system credentials may be granted to authorised personnel by the IT provider with appropriate approvals and logging.
- Administrative credentials must be stored securely and only accessible to authorised personnel with a copy provided to the Chair of the Council in a sealed envelope, only to be accessed in an emergency.
- Passwords must not be stored in plain text or written down in insecure locations.
- Immediately change password if compromise is suspected.

3.4 Password Access Control and Logging.

- All access to administrative or shared credentials must be logged and auditable.
- Attempts to access unauthorised passwords will be treated as a security incident. Users are responsible for creating and maintaining secure passwords for their accounts.

The IT security provider is responsible for:

- Managing system/service credentials.
- Enforcing password policies. Auditing and monitoring password-related security practices.

4 Monitoring

4.1 The Council reserves the right to monitor and maintain logs of Council owned computer usage and inspect any files stored on its network, servers, computers, or associated technology to ensure compliance with this policy as well as relevant legislation.

4.2 The Council may monitor the use of electronic communications using Council owned devices and use of Council provided internet in line with the Investigatory Powers (Interception by Councils etc for Monitoring and Record-keeping Purposes) Regulations 2018.

4.3 Monitoring of an employee's email and/or internet use will be conducted in accordance with an impact assessment that the Council has carried out to ensure that monitoring is necessary and proportionate. Monitoring is in the Council's legitimate interests and is to ensure that this policy is being complied with.

4.4 The information obtained through monitoring may be shared internally, including with relevant Councillors and IT staff if access to the data is necessary for performance of their roles. The information may also be shared with external HR or legal advisers for the purposes of seeking professional advice. Any external advisers will have appropriate data protection policies and protocols in place.

4.5 The information gathered through monitoring will be retained only long enough for any breach of this policy to come to light and for any investigation to be conducted.

4.6 Councillors and staff have a number of rights in relation to their data, including the right to make a subject access request and the right to have data rectified or erased in some circumstances.

4.7 Such monitoring and the retrieval of the content of any messages may be for the purposes of checking whether the use of the system is legitimate, to find lost messages or to retrieve messages lost due to computer failure, to assist in the investigation of wrongful acts, or to comply with any legal obligation.

4.8 The Council reserves the right to inspect all files stored on its computer systems in order to assure compliance with this policy. The Council also reserves the right to monitor the types of sites being accessed and the extent and frequency of use of the internet at any time, both inside and outside of working hours to ensure that the system is not being abused and to protect the Council from potential damage or disrepute.

4.9 Any use that the Council considers to be 'improper', either in terms of the content or the amount of time spent on this, may result in disciplinary proceedings.

4.10 All Council owned computers will be periodically checked and scanned for unauthorised programmes and viruses.

5 Personal Email

5.1 Email messages sent on the Council's accounts should be for Council use only. Personal communications are permitted provided they do not encroach upon working time or interrupt Council business in any way. Employees are asked to use their personal email accounts, rather than Council addresses for personal emails.

6 Copyright

6.1 Much of what appears on the Internet is protected by copyright. Any copying without permission, including electronic copying, is illegal and therefore prohibited. The Copyright, Designs and Patents Act 1988 set out the rules. The copyright laws not only apply to documents but also to software. The infringement of the copyright of another person or organisation could lead to legal action being taken against the Council and damages being awarded and staff may face disciplinary action, including dismissal**.**

6.2 It is easy to copy electronically, but this does not make it any less an offence. The Council's policy is to comply with copyright laws, and not to bend the rules in any way.

6.3 Councillors and staff should not assume that because a document or file is on the Internet, it can be freely copied. There is a difference between information in the 'public domain' (which is no longer confidential or secret information but is still copyright protected) and information which is not protected by copyright (such as where the author has been dead for more than 70 years). Usually, a website will contain copyright conditions; these warnings should be read before downloading or copying.

6.4 Copyright and database right law can be complicated. Councillors, staff, and other authorised users should check with the Clerk if unsure about anything.

7 Data protection

7.1 Special rules apply to the processing of personal and sensitive personal data. For further guidance on this, see the Council's Communication Policy.

8 Accuracy of information

8.1 One of the main benefits of the internet is the access it gives to large amounts of information, which is often more up to date than traditional sources such as libraries. Be aware that, as the internet is uncontrolled, much of the information may be less accurate than it appears.

9 Use of social media

9.1 Personal use of social networking/media and chat sites by staff should be restricted to breaks during working hours.

9.2 The Council recognises the importance of Councillors and staff joining in and helping to shape sector conversation and enhancing its image through blogging and interaction in social media.

9.3 However, inappropriate comments and postings can adversely affect the reputation of the Council, even if it is not directly referenced. Councillors and staff should conduct themselves in accordance with the Councils Social Media policy.

9.4 Councillors and staff must be aware that they are personally liable for anything that they write or present online (including on an online forum or blog, post, feed or website). Councillors should always be mindful of the Members Code of Conduct and Nolan Principles. Employees may be subject to disciplinary action for comments, content, or images that are defamatory, embarrassing, pornographic, proprietary, harassing, libellous, or that can create a hostile work environment.

9.5 Note that the Council may, from time to time, monitor external postings by staff on social media sites. Any employee who has a profile (for example on LinkedIn or Facebook) must not misrepresent themselves or their role with the Council. Staff are also advised that social media sites are not an appropriate place to air Council concerns or complaints: these should be raised with the Council or formally through the grievance procedure.

Review Date: January 2028

Document control

Version and date	Adopted
Created December 2025 V1.0	Adopted at Full Council meeting 8 January 2026