LEA AND COTTAM PARISH COUNCIL

IT & USE OF PERSONAL DEVICES POLICY

1. Introduction

Lea and Cottam Parish Council (the Council) recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications

2. Scope

This policy applies to all individuals who use the Council's IT resources which include computers, networks, software, devices, data, and email accounts. At the time of the adoption of this policy the Council do not supply computers, networks, software or devices to individuals recognising the benefits that can be achieved by allowing councillors to use their own electronic devices for council business whether that is at home or at meetings (see later guidelines re use of personal devices and software)

The use of such devices to create and process council information and data creates issues that need to be addressed, particularly in relation to information security.

The Council must ensure that it remains in control of the data for which it is responsible, regardless of the ownership of the device used to carry out processing.

3. Acceptable use of IT resources including email

The Council's IT resources (in this case email accounts) are to be used for official council-related activities and tasks only. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content. Emails should also be professional and respectful in tone. Users must be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

4. Passwords and account security

Users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others. Regular password changes are encouraged to enhance security.

5. Email monitoring

The 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 and GDPR.

6. Retention and archiving

Emails should be regularly reviewed and deleted in order to maintain an organised inbox.

7. Responsibility of Councillors

Individuals using their own devices must take responsibility for their own device and how they use it

They must familiarise themselves with their device and its security features so that they can ensure the safety of council information (as well as their own information)

Invoke the relevant security features

Maintain the device themselves ensuring it is regularly patched and upgraded

Ensure it is used only in line with the values in the Code of Conduct and the Nolan Principles

The Council cannot take responsibility for supporting devices that it does not provide.

They should take all reasonable steps to prevent theft or loss of data. Keep information confidential, maintain the integrity of data and information and take responsibility for any software they down load onto their device.

Set up passwords, passcodes, passkeys or biometric equivalents which are of sufficient length and complexity for the particular type of device.

Only maintain Council information on a device where it is essential and delete such information as soon as possible once it is no longer required. This includes information within emails.

Be aware of any data protection issues and ensure personal data is handled in accordance with legislation and is deleted once the purpose for which it was held has come to an end.

No Council information must be left on any personal device indefinitely, taking particular care if a device is disposed of/sold/transferred to a third party.

Ensure they immediately delete all Council data from their personal devices once they have left the Council

8. Monitoring and Access

The Council will not routinely monitor personal devices but reserves the right to take such action as appropriate to retrieve information owned by the Council.

The Information Commissioners Office may also take such action as appropriate to retrieve Council information relating to a Subject Access Request

9. Data Protection

The Council must process 'personal data' in accordance with the Data Protection Act 2018 and the General Data Protection Regulations. The Council, in line with guidance from the Information Commissioners Office recognises that there are inherent risks in using personal devices to hold third party personal data. Therefore, Councillors must follow the guidance in this document when using their own devices to process personal data. A breach of the Data Protection Act 2018 or the GDPR can lead to a Council being fined. Any Councillor found to have deliberately breached the Act or Regulations may be subject to disciplinary measures or even a criminal prosecution.

10 Personal Data

'Personal Data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

ADOPTED 1ST DECEMBER 2025