

Digital Policy

Version:	V1
New or Replacement:	New
Document Author(s):	Parish Clerk
Contributor(s):	None
Minutes Approved By:	May 2026
Date Approved:	21/5/2026
Review Date:	May 2027

Version History Log

Version	Date Published	Details of key changes
1.0	May 2026	n/a

Contents

1.	Introduction	3
2.	Scope.....	3
3.	Acceptable use of Digital resources and email	3
4.	Device and software usage.....	3
5.	Data management and security	3
6.	Network and internet usage	3
7.	Email communication	3
8.	Password and account security	4
9.	Mobile devices and remote Work.....	4
12.	Reporting security incidents	4
13.	Training and awareness.....	4
14.	Compliance and consequences	4
15.	Policy review	5
16.	Contacts.....	5

1. Introduction

Ludford Parish Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications, to meet legislation and national guidelines.

This policy outlines the guidelines and responsibilities for the appropriate use of digital resources by Council members, employees, volunteers, and contractors.

2. Scope

This policy applies to all individuals who use Ludford Parish Council's digital resources, including computers, networks, software, devices, data, and email accounts.

3. Acceptable use of Digital resources and email

Ludford Parish Council digital resources and email accounts are to be used for official Council-related activities and tasks. Limited personal use is permitted, provided it does not interfere with work responsibilities or violate any part of this policy. All users **must** adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

4. Device and software usage

The Council does **not** currently provide devices, software and/or any applications to the Clerk or Council Members.

If devices were provided the unauthorised installation of software on authorised devices, including personal software, would be strictly prohibited due to security concerns.

5. Data management and security

All sensitive and confidential Ludford 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.

6. Network and internet usage

Ludford Parish Council does not have a council-owned network or internet connection. If these are provided, they should be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited.

7. Email communication

Email accounts provided by Ludford 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 it is encrypted.

Caution should be used with attachments or links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

8. Password and account security

Ludford Parish Council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong ideally not using themes that can easily be identified such as names or dates (such as anniversaries or birthdays) using short easily remembered sentences are best, such as “the cat sat on the mat” replacing some words with numbers and capitals “Th3c4tsat0NtheM4t” makes a good strong password.

Do not shared Usernames or passwords with others. Good, strong passwords need to be changed less often, but users are encouraged to change to enhance security.

9. Mobile devices and remote Work

Mobile devices are not provided by Ludford Parish Council, but devices should be secured with passcodes and/or biometric authentication. When working remotely, users should follow the same security practices as if they were in the office.

10. Email monitoring

Ludford 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 and GDPR.

11. Retention and archiving

Emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an organised inbox.

12. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the Parish Clerk or Chairman for investigation and resolution. Report any email related security incidents or breaches to the Parish Clerk or Chairman immediately.

13. Training and awareness

ELDC work with a range of organisations to provide support with using devices and working securely online, the recommended is Lincs Digital, more information can be found here - [Digital Inclusion - East Lindsey District Council](#) which provides resources to users about Digital security best practices, privacy concerns, and technology updates when requested.

14. Compliance and consequences

Breach of this Digital Policy may result in the suspension of Digital privileges and further consequences as deemed appropriate.

15. Policy review

This policy will be reviewed annually to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

16. Contacts

For Digital related enquiries or assistance, users can contact the Parish Clerk.

All staff and Councillors are responsible for the safety and security of Ludford Parish Council's digital systems. By adhering to this Digital Policy, Ludford Parish Council aims to create a secure and efficient digital environment that supports its mission and goals.