

The Parish Council of Little Harrowden

Clerk: Sylvia Tilaks
Mulberry Cottage
15 Main Road
Grendon, NN7 1JW



Telephone 07942 292479
Email: clerk@littleharrowdenparishcouncil.gov.uk
<https://littleharrowdenparishcouncil.gov.uk/>

INFORMATION TECHNOLOGY (IT) POLICY

Procedure reviewed and adopted at the meeting of Little Harrowden Parish Council held on: 09.09.26

This policy will be reviewed annually or sooner if legislation, technology or council practices change. Relevant additional policies and procedures must be referred to in association with this document. **Next review September 2027**

Signed:

Name:

Position:

Date:

Information Technology (IT) Policy

Including Data Breach Processes, Digital Security and Social Media.

1. Purpose of this Policy

This policy sets out how Little Harrowden Parish Council will safely and responsibly use computers, mobile devices, email, cloud storage, the council website and social media. The policy supports:

- Good governance and internal control
- Data protection and confidentiality
- Transparency and accountability
- Business continuity
- Secure management of council information

This policy should be read alongside the Council's:

- Financial Regulations
- Data Protection Policy
- Privacy Policy
- Records Retention Policy
- Social Media Policy
- Publication Scheme

2. Scope

This policy applies to:

- Parish Councillors
- Employees
- Contractors or volunteers acting on behalf of the Council
- Any device or account used for official Parish Council business

3. Council Devices and Security

All devices used for Parish Council business should:

- Be password protected
- Use up-to-date software and security updates where possible
- Be kept secure and not left unattended in public places
- Not be shared with unauthorised persons

Councillors borrowing a council laptop must not install or add software without permission.

Personal data must not be stored unencrypted on USB sticks, personal laptops or Cloud services .

Council laptops require anti-virus software, 2 factor authentication and regular updates on council devices. Where possible, council information should only be stored on secure council-managed systems or protected cloud storage.

Personal data must not be stored unnecessarily on personal devices.

Any suspected cyber incident, lost device, phishing email or data breach must be reported immediately to the Clerk.

4. Email and Electronic Communications

Official council business should be conducted using recognised council email accounts where possible. Users must:

- Take care when opening attachments or clicking links
- Check recipient details before sending emails
- Avoid sending sensitive personal information unless necessary
- Delete spam or suspicious emails immediately

Emails form part of the council's records and may be subject to Freedom of Information or Subject Access Requests.

5. Website Management

The Parish Council website is maintained solely by the Clerk / Proper Officer.

The Clerk is responsible for:

- Publishing agendas, minutes and transparency information
- Ensuring information is accurate and up to date
- Maintaining website security and access controls
- Managing accessibility and publication requirements

No other person may upload, amend or remove website content unless specifically authorised by Full Council.

6. Social Media

The Council recognises that social media is an important communication tool for engaging with residents and sharing public information. Parish Council Social Media pages are for Parish Council information only. Only authorised individuals may post official content on behalf of the Council. These may include:

- The Chair
- Vice Chair
- Police Liaison Representative (PLR)
- Neighbourhood Plan leads
- Approved bank signatories where relevant to finance notices
- Any other councillor specifically authorised by Full Council

Authorised users must:

- Act respectfully and professionally
- Share factual and lawful information only
- Avoid political or personal comments when acting in a council capacity
- Avoid publishing confidential or personal information
- Refer complaints, legal matters or formal correspondence to the Clerk

Social media must never be used:

- To make council decisions
- To conduct official debates outside meetings
- To disclose confidential information
- To harass, bully or intimidate any person

All Councillors and employees with administrative authority may remove inappropriate content where necessary.

7. Data Protection and Confidential Information

The Council will comply with:

- UK GDPR
- Data Protection Act 2018
- Freedom of Information Act 2000

Personal data will only be collected, stored and processed where necessary for council business.

The Clerk / Responsible Financial Officer is responsible for:

- Managing any council contact databases
- Controlling access to personal data
- Responding to information requests
- Ensuring records are retained and destroyed appropriately

The Council currently holds no public contact database or mailing list. Any contact databases created will remain under the sole control of the Proper Officer/RFO.

Councillors must not copy, retain or use personal data for non-council purposes.

See the Council's Data Protection Policy for detailed information regarding compliance with data protection legislation, data road map/breach processes, and ROPA (Record of Processing Activities).

8. Backups and Business Continuity

Important council records should be backed up electronically where possible.

Key financial and governance records should be capable of being recovered following equipment failure, cyber incident or accidental deletion.

The Council will maintain reasonable arrangements to allow essential functions to continue during periods of disruption.

9. Training and Awareness

Councillors and staff should maintain a basic awareness of:

- Cyber security risks
- Phishing and scam emails
- Data protection responsibilities
- Safe use of council information

Advice and guidance may be provided by the Clerk, Internal Auditor, DPO or relevant professional bodies.

10. Breaches of this Policy

Failure to comply with this policy may result in:

- Removal of access permissions
- Referral under the Council's Code of Conduct
- Disciplinary action where appropriate
- Reporting to the Information Commissioner's Office where legally required