Pinchbeck Parish Council

IT & Equipment Policy

1. Purpose

1.1 This policy sets out the principles, practices and conditions under which employees, councillors, contractors and volunteers of Pinchbeck Parish Council (PPC) may access and use IT and communications systems and equipment.

2. Scope

2.1 This policy applies to:

- All Councillors and employees of Pinchbeck Parish Council.
- Any contractors, consultants, suppliers and other third parties who use or access Council IT resources.
- All volunteers who deliver services on behalf of the Parish Council, including Library Volunteers (see Section 13).
- Any device or system accessing or using PPC data or systems, whether Council-owned or personal.

3. Objectives

3.1 The objectives of this policy are to:

- Ensure IT systems are used appropriately and securely.
- Protect data and systems from security threats, misuse, or data breaches.
- Comply with legal obligations including GDPR and the Freedom of Information Act.
- Promote safe, lawful, and productive use of technology.

4. Acceptable Use

4.1 Parish Council-provided IT equipment must be used primarily for Council-related work.

4.2 Users must:

- Use IT equipment and systems only for lawful and authorised purposes.
- Take care to prevent damage or unauthorised access.
- Ensure passwords and logins are secure and not shared.
- Log off from systems when unattended.
- Report any lost or stolen devices immediately.
- Avoid accessing inappropriate websites or material and not compromise Council security, data, or reputation.

4.3 Council provided laptops may be used for personal purposes by the Council's office staff, or councillors, provided such use does not interfere with Council operations, security, or data

integrity.

4.4 Volunteers using shared Council equipment must restrict use to council related tasks only. Personal use is not permitted.

5. Software and Licensing

5.1 Only authorised and properly licensed software may be used. Users must not download or install unauthorised programs.

6. Personal Devices (e.g. laptops, tablets, smartphones)

6.1 Personally owned equipment may be used for Council business only with appropriate safeguards in place.

6.2 Users are responsible for ensuring personal devices:

- Have up-to-date antivirus protection.
- Are protected by a secure password or PIN.
- Are not used to store sensitive Council data unless authorised.

7. Network and Internet Usage

7.1 Council networks must be used responsibly. Use of public Wi-Fi for Council work should be avoided unless a VPN is used. Personal browsing must be appropriate and minimal.

8. Data Protection and Security

8.1 Users must:

- Comply with the Council's Data Protection Policy.
- Store files appropriately and securely.
- Report any suspected data breaches immediately to the Clerk.

8.2 Multi-factor authentication (MFA) must be enabled where available.

8.3 All Council data must be saved in approved secure locations (e.g. Microsoft 365 OneDrive or SharePoint) and not stored solely on local drives or removable media.

8.4 Regular backups must be maintained.

8.5 Confidential information must be securely deleted when no longer needed.

8.6 All suspected security breaches must be reported immediately to the Clerk (or the Chair/Vice-Chair if the Clerk is unavailable). All incidents will be logged and reviewed.

9. Monitoring and Privacy

9.1 The Parish Council reserves the right to monitor use of its equipment and systems, including email and internet usage.

9.2 By using Council systems, users acknowledge and accept that such monitoring may take place to ensure compliance with this policy.

10. Email Use

10.1 Council email accounts must be used for Council business. Users must avoid using personal email accounts for Council business and must not use Council email accounts for personal or non-council business.

10.2 Emails must be professional and respectful.

10.3 Confidential content must be encrypted if sent externally.

10.4 Emails related to Council business should be retained for a minimum of six years unless a shorter retention is justified. Regular inbox maintenance is encouraged.

11. Receipt of Suspicious or Potentially Malicious Emails

11.1 Users must not engage with phishing attempts, spam messages, or suspicious links.

11.2 Users are expected to exercise caution and verify the legitimacy of emails, links, and attachments before interacting with them.

11.3 If a user receives a suspicious or potentially malicious email, they must not forward it, especially if it contains personal data. In most cases, such emails must be deleted immediately.

11.4 If the user is unsure whether the email may represent a data breach or requires further action, they must contact the Clerk for guidance, either by phone or by sending a new separate email (not by replying to or forwarding the suspicious message).

12. Training

12.1 The Council will provide guidance and training on IT use and security where needed. Councillors, volunteers, and staff should inform the Clerk if support is required.

13. Library Volunteers and Public Access IT

13.1 Library Volunteers providing services under the Parish Council's oversight must:

- Comply with the separate Library Volunteer IT Acceptable Use Policy.
- Use only authorised LCC or PPC systems for public service delivery.
- Follow procedures for data handling and safeguarding as outlined in the separate policy.

13.2 The Council acknowledges that Lincolnshire County Council retains separate responsibility for LCC managed equipment and public services within the library. This policy applies to PPC systems and volunteers operating on behalf of the Parish Council.

14. Termination of Duties

14.1 When leaving the Council or ending a role, users must:

- Return all Council-owned equipment and materials.
- Cease access to all Council systems, which will be revoked by the Council.

- Permanently delete or destroy any Council data stored on personal devices or in their possession.
- Complete and submit a declaration of compliance, if requested by the Clerk.

15. Breaches of Policy

15.1 Breaches of this policy may result in disciplinary action or termination of access to IT systems. Where appropriate, legal action may be taken.

15.2 Incidents will be reviewed annually as part of the Council's risk management process.

16. Acknowledgement and Review

16.1 All users are required to sign the accompanying Appendix: User Acknowledgement Form.

16.2 This policy will be reviewed annually to ensure effectiveness and alignment with changes in legislation or technology.

17. Contacts

17.1 For advice or support, please contact the Clerk at:

clerk@pinchbeck-pc.gov.uk

Pinchbeck Parish Council

IT Policy

Appendix: User Acknowledgement Form

I confirm that I have read and understood the IT Policy of Pinchbeck Parish Council and agree to abide by its provisions.

I understand that any use of Parish Council IT equipment, systems, or email accounts may be monitored in accordance with the IT Policy, and that this monitoring may include usage logs, access records, and content where necessary to ensure security, legal compliance, and proper use.

Name: _____

Role: _____

Signature: _____

Date: _____