



## IT POLICY

**Girton Parish Council  
The Pavilion,  
Girton Recreation Ground  
Cambridge Road, Girton,  
Cambridge CB3 0FH  
[www.girton-cambs.org.uk](http://www.girton-cambs.org.uk)**

**Date of policy:** 04 August 2025

**Approving committee:** Girton Parish Council – Full Council

**Date of committee meeting:** 13 August 2025

**Policy version reference:** GPC - Version One

**Supersedes:** Not Applicable

**Policy effective from:** 13 August 2025

**Date for next review:** 08 May 2026 (GPC Annual Meeting 2026)

## **1. Purpose**

This policy sets out how Girton Parish Council manages and governs the use of information technology (IT) systems and equipment. It aims to ensure secure, lawful, and effective use of IT by councillors, staff, contractors, and volunteers.

## **2. Scope**

This policy applies to all individuals who access or use council IT systems, including:

- Computers and laptops
- Email and internet access
- Council website and social media
- Mobile phones and smart devices
- File storage and cloud services

## **3. Responsibilities**

The Parish Clerk is responsible for monitoring compliance, reviewing this policy annually, and ensuring staff and councillors understand its provisions.

## **4. Related Policies**

This policy should be read alongside:

- Data Protection Policy
- Disciplinary Policy
- Equality and Diversity Policy
- Records Retention Policy

## **5. Acceptable Use**

Council IT systems must be used for official purposes only. Limited personal use may be permitted during breaks, provided it does not interfere with council business or breach this policy.

## **6. Monitoring**

The council reserves the right to monitor IT usage for legitimate reasons, including security, data protection, and performance. Users will be informed of any monitoring.

## **7. Passwords and Access**

- Passwords must be strong, confidential, and changed regularly.
- Passwords must not be shared.
- Access to systems may be granted to the Clerk or Chair in cases of absence or emergency.
- Password-protected documents must be shared securely (e.g. via phone or encrypted message).

## **8. Device Use**

- Devices must be shut down daily and locked when unattended.
- Documents must be saved in designated council folders or cloud storage.
- Public access areas require additional precautions (e.g. screen privacy filters).

## **9. Personal Devices**

Use of personal devices for council business is discouraged. Where permitted, devices must comply with council security standards.

## **10. Data Protection**

All personal data must be processed in accordance with UK GDPR. This includes:

- Lawful collection and use
- Secure storage and disposal
- Prevention of unauthorised access or disclosure

## **11. Mobile Communication**

Text messages must be professional and appropriate. Abbreviations and informal language should be avoided. Messages are subject to the same standards as emails.

## **12. Email Use**

- Council email accounts must be used for all official correspondence.
- Emails must be professional, accurate, and respectful.
- Staff must not enter into binding agreements via email without council approval.

## **13. Internet Use**

- Internet access is provided for council business.
- Accessing inappropriate content, chat rooms, or personal messaging services is prohibited.

- A firewall is in place to protect council systems.

#### **14. Software**

Only authorised software may be installed on council devices. Downloads must be approved by the Clerk.

#### **15. Training**

All staff and councillors will receive basic IT and data protection training, including email security and password management, during induction.

#### **16. Misuse**

Misuse of IT systems may result in disciplinary action. Examples include:

- Attempting to bypass security
- Installing malicious software
- Using council systems abusively
- Leaving devices unattended in public places

#### **17. Review**

This policy will be reviewed annually or sooner if required by changes in legislation or council operations.