FINSTALL
PARISH COUNCIL

IT POLICY

Adopted date	02/07/2024	**Minute:**
Review date	01/2026	**8f**
Next Review	01/2027	

1. Introduction
Finstall parish council recognises the importance of effective and secure information technology (IT) usage in supporting its business, operations and communications.
This policy outlines the guidelines and responsibilities for the appropriate use of IT resources by council members, employees, volunteers, and contractors.

2. Scope
This policy applies to all individuals who use Finstall parish council's IT resources, including computers, networks, software, devices, and data.

3. Acceptable use of IT resources
Finstall parish council IT resources are to be used for official council-related activities and tasks. Personal use should be limited and should not interfere with Finstall parish council work responsibilities.
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
Where possible, authorised devices, software, and applications will be provided by the Finstall parish council for work-related tasks.
Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

5. Data management and security
All sensitive and confidential Finstall 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
Finstall parish council's network and internet connections 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 Finstall parish council are for official communication only.
Email signatures should be used and emails should be professional and respectful in tone.

Be cautious when opening email attachments or clicking on links to prevent phishing and malware threats.

8. Password and account security
Finstall parish council 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.

9. Mobile devices and remote work
Mobile devices provided by Finstall parish council 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. Reporting security incidents
All suspected security breaches or incidents should be reported immediately to the designated IT point of contact for investigation and resolution.

11. Training and awareness
Finstall parish council will provide regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates.

12. Compliance and consequences
Breach of this IT policy may result in the suspension of IT privileges and further consequences as deemed appropriate.

13. 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.

14. Contacts
For IT-related enquiries or assistance, users can contact the Clerk to Finstall Parish Council by email: clerk@finstallparishcouncil.gov.uk or by online reporting via Contact Us – Finstall Parish Council (https://finstallparishcouncil.gov.uk/contact-us) .
All staff and councillors are responsible for the safety and security of Finstall Parish Council's data and IT equipment. By adhering to this IT policy, Finstall parish council aims to create a secure and efficient IT environment that supports its mission and goals.