



DITCHLING PARISH COUNCIL

Information and Communications Technology (ICT) Policy

1. Introduction

Ditchling Parish Council (The Council) recognises the importance of effective and secure information and communications technology (ICT) in supporting all its functions.

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

2. Scope

This policy applies to all individuals who use the Council's ICT resources, including computers and other hardware devices, networks, software, data and email accounts.

3. Acceptable use of ICT resources

The Council ICT resources 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 provision

Staff working in the Parish Office have devices provided by the Council for work-related tasks, in addition to the licensed software made available to most users. Staff also have additional specialised software.

Installation of additional software on the devices provided should be authorised by the Council.

5. Data management and security

All Council data should be stored and transmitted securely using approved methods, which currently consist of those within its Microsoft cloud system.

Regular data backups to the same system should be performed to prevent data loss and data should be deleted, if required, when the data have been retained for periods defined in the Council's Document Retention Policy.

6. Copyright materials

The Council's ITC resources 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 the 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.

Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

8. Password and account security

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 and personally owned devices and remote work

Devices provided by the Council and all personally owned devices used to access Council ICT resources should be secured with passcodes and/or biometric authentication. When working remotely, users should follow the same security practices as if they were in an office.

10. Email monitoring

The 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 and the Council's Document Retention Policy. Regularly review and delete unnecessary emails.

12. Reporting Security Incidents

All suspected security breaches or incidents should be reported immediately to the Clerk for investigation and resolution.

13. Training and awareness

The Council will provide regular training and resources to educate users about security best practices and technology updates.

14. Compliance and consequences

Breach of this ICT policy may result in the suspension of ICT privileges and further consequences as deemed appropriate by the Council.

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 ICT-related enquiries or assistance, users can contact the Clerk, who may refer users to the Council's ICT support partner.

All staff and councillors are responsible for the safety and security of the Council's ICT systems. By adhering to this ICT Policy, the Council aims to create a secure and efficient ICT environment.