



Information Technology (IT) Policy

Issue Status: 1 **Last Updated:** 07.01.2026 **Last Reviewed:** 01.05.2026
Originated by: Parish Clerk Venetia Davies & Cllr. Ken Brown
Approved by: Cuddington Parish Council **Date:** 27.05.2026
THIS DOCUMENT IS UPDATED REGULARLY AND REVIEWED ANNUALLY

CONTENTS

1. Introduction.....	2
2. Acceptable Use of IT Resources and Email.....	3
3. Device and Software Usage.....	3
4. Data Management and Security.....	3
5. Network and Internet Usage.....	3
6. Email Communication.....	3
7. Password and Account Security	3
8. Mobile devices and Remote Work.....	4
9. Email Monitoring	4
10. Retention and Archiving	4
11. Reporting Security Incidents	4
12. Training and Awareness	4
13. Compliance and Consequences	4
14. Responsibilities.....	4
15. Social and Digital Communication.....	4
16. Contact and Assistance.....	4
17. Policy Review	4
18. Appendix 1 - Retention Schedule	5

1. Introduction

Cuddington Parish Council (the Council) recognises the importance of effective and secure Information Technology (IT) and email usage in supporting its business, operations, and communications. This policy:-

Applies to all individuals who use the Council's IT resources, including computers, networks, software, devices, data, and email accounts.

Applies to all individuals who use the Council's IT systems for Council business, including computers, networks, software, devices, data, and email accounts. Regardless of whether they are using council-owned or personal devices.

Outlines the guidelines and responsibilities for the appropriate use of IT resources and email by council members, employees, volunteers, and contractors.

The Council meets the Governments digital communication requirements - SAAPP 2025 for email communication and website accessibility (WCAG)2.2AA.

2. Acceptable Use of IT Resources and Email

The Council's IT resources and email accounts 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.

3. Device and Software Usage

Where possible, authorised devices, software, and applications will be provided by the Council for work-related tasks. Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

4. Data Management and Security

All sensitive and confidential 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. See the Councils Data Policy for further information.

Council laptops must not have software installed without prior consent and no personal data should be stored unencrypted on any devices or cloud platforms without Council approval.

5. Network and Internet Usage

The 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.

6. 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. The Council must be cautious with attachments and links. It must verify the source before opening any attachments or clicking on links to avoid phishing and malware.

7. 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.

8. Mobile devices and Remote Work

Mobile devices provided by the 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. To protect devices from being accessed All devices must lock after 3 attempts to log in and lock after a short time of inactivity.

9. 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.

10. Retention and Archiving

Under the Freedom of Information Act 2000, the Council is required to maintain a retention scheme which lays down the length of time records need to be retained and the action which should be taken when it is of no further administrative use. The Clerk is responsible for regularly reviewing emails and documents. Deleting/destroying any unnecessary emails/documents taking into account different retention periods using the Retention Schedule shown in Appendix 1.

11. Reporting Security Incidents

All suspected security breaches or incidents should be reported immediately to the designated IT point of contact for investigation and resolution. Report any email-related security incidents or breaches to the IT administrator immediately.

12. Training and Awareness

Appropriate training and resources will be available to educate users about IT security best practices, privacy concerns, and technology updates.

13. Compliance and Consequences

Breach of this IT and email Policy may result in the suspension of IT privileges and further consequences as deemed appropriate.

14. Responsibilities

All staff and councillors are responsible for the safety and security of the Council's IT and email systems. By adhering to this IT and email Policy, the Council aims to create a secure and efficient IT environment that supports its mission and goals.

15. Social and Digital Communication

The website www.cuddingtonvillage.com is the Council's official digital communication. Information posted on the Website will have had the authorisation of the Clerk or Chairperson. The Council also uses Facebook - Cuddington Village and for instant communication to its villagers WhatsApp.

16. Contact and Assistance

For IT-related enquiries or assistance, users can contact the parish clerk at:-
clerk@cuddington-bucks-pc.gov.uk

17. 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.

END

18. Appendix 1 - Retention Schedule

DOCUMENT	MINIMUM RETENTION	REASON	ACTION
Minute Books	Indefinite		Archive
Annual Audited Accounts	Indefinite		Archive
Annual Return	Indefinite		Archive
Deeds, leases	Indefinite		Archive
Assets register	Indefinite	Audit	Preserve
Cert of Employers Liability	40 years	Audit/Legal	Destroy
Cert of public liability	40 Years	Audit/Legal	Destroy
Tax & NI records	12 years	Audit	Destroy
Bank statements	6 years	Audit	Destroy
Quotations	6 years	Audit	Destroy
Paid invoices	6 years	Audit/VAT	Destroy
VAT records	6 years	VAT	Destroy
Salary records	6 years	Audit	Destroy
Cllrs Declaration of Office	4 Years	Management	Destroy
Complaints	1 Year	Management	Destroy
Routine Correspondence	6 months	Management	Destroy
General Information	12 Months	Management	Destroy
Insurance policies	Whilst Valid	Audit	Destroy
Cheque book stubs	Last completed audit	Management	Destroy
Paying in books	Last completed audit	Management	Destroy
Register of Electors	Once updated	Management	Destroy
Risk Assessments	Once Superseded	Management	Destroy
Members interests	Term of Office	Management	Destroy
Governance Policies	Once Superseded	Management	Destroy

All planning applications and relevant decision notices are available at Buckinghamshire County Council. There is no requirement to retain duplicates locally. All Council recommendations in connection with planning applications are recorded in the Council minutes retained indefinitely. Correspondence received in connection with planning applications will follow the above schedule.