EDINGTON

PARISH COUNCIL

SMALLER AUTHORITIES IT POLICY

1. Introduction

Edington Parish Council henceforth known as "The Authority" recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications.

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

Mr Steve Forward acts as the authority's IT manager. The Clerk acts as the IT Proper Officer.

2. Scope

This policy applies to all individuals who use IT resources, including computers, networks, software, devices, data, and email accounts. The authority does not provide digital devices but acknowledges that the Clerk and members may be using their own personal devices. Everyone must adhere to this policy to maintain digital security.

3. Training and awareness

The Authority will source regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. You should engage in regular training on email security and best practices, including but not limited to:

- the Parish Council Domain Helper Service's virtual cybersecurity workshops for councils.
- The National Cyber Security Centre Cyber Security training for small organisations and free Cyber Action Toolkit.

4. Acceptable use of council provided IT resources and email

When using IT resources for the council's purposes, you must adhere to ethical standards, and respect copyright and intellectual property rights.

Where possible, authorised devices, software, and applications will be provided by the Authority for work-related tasks.

You must not install unauthorised software without checking with the clerk, and you must not use equipment or email to access or forward inappropriate or offensive content.

5. What you must do if you use your own personal devices

The Authority will endeavour to provide individuals with devices to use for council business. If you are using your own device, you must make sure you are:

- using strong passwords for all your accounts (preferably using a password manager).
- downloading the latest operating system security updates.
- using anti-virus software.

6. Network and internet usage

You must be careful about which Wi-Fi networks you join. Public Wi-Fi networks in coffee shops or on trains can be targeted by hackers. Always make sure you are using a trusted internet connection, which is password protected when carrying out official business.

7. Password and account security

You are responsible for maintaining the security of your accounts and passwords. Use the National Cyber Security Centre's advice for choosing a strong password. For business continuity, login details and passwords of official accounts need to be stored securely so they can be accessed by trusted individuals in an emergency; the Clerk and Mr Steve Forward retain this list. If you change a password of an official account, then you must inform Mr Steve Forward as soon as practical so that the stored details can be updated. Never share password details with anyone other than the Clerk or Mr Steve Forward.

8. Email communication

The Authority will endeavour to provide you with an official email account for organisation-related communication only. If you are currently using a personal email account, you should aim to move over to an official email account as soon as practically possible. You must make sure that emails are professional and respectful in tone. You must always check you are sending any confidential or sensitive information to the correct recipients.

Always be cautious when downloading attachments and opening links to avoid phishing and malware. Before opening any attachments or clicking on links, verify the source by looking at the email it has come from carefully. Do not download and open anything if you are unsure who has sent it.

9. Email access

The Authority reserves the right to check email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR. Clerks may need to access emails so that they respond to FOI or subject-access requests. If you are using a personal email account for council business, this is still subject to data protections laws and FOI requests.

10. Data management, data retention and security

All sensitive and confidential data should be stored and transmitted securely. You must regularly backup any important data to prevent data loss and follow your organisation's data retention policies (see Annex A).

You should retain and archive emails in compliance with your data retention policies. Regularly review and delete unnecessary emails to maintain an organised inbox.

11. Reporting security incidents

All suspected security breaches, including email breaches or incidents should be reported immediately to Mr Steve Forward.

12. Compliance and consequences

Breach of this IT and Email Policy may result in the suspension of IT privileges.

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 Mr Steve Forward.

All staff and councillors are responsible for the safety and security of IT and email systems.

Date of adoption: _____at a meeting of the authority on _____

Date for next review:

Annex A to EDINGTON PARISH COUNCIL Smaller Authorities IT Policy

Data Retention and Disposal Policy

1. Introduction

1.1 Purpose

The purpose of this policy is to ensure that the Council manages, retains, and disposes of its records systematically, efficiently, and in full compliance with all relevant statutory and regulatory obligations. As a public body, the Council recognizes that the proper management of its data is essential to maintaining public trust, supporting administrative transparency, and protecting individual privacy rights.

This policy establishes controls over how long specific categories of information must be kept, balancing the legal necessity to preserve historical, financial, and administrative records with the explicit legal requirement to delete personal information once its purpose has been served.

It is recognised that up to date, reliable and accurate information is a vital to support the work that the Council do and the services that it provides to its residents. This policy will help us to ensure:

- the retention and availability of the minimum amount of relevant information that is necessary for the Council to operate and provide services to the public;
- we comply with legal and regulatory requirements, including the Freedom of Information Act 2000, the Data Protection Act 2018, UK-GDPR and the Environmental Information Regulations 2004;
- efficiency in retrieving information by reducing the amount of information that may be held unnecessarily;
- archival records that are of historical value are appropriately retained for the benefit of future generations.

1.2 Scope

This policy applies universally to all information created, received, or maintained by the Council in the course of its official business. It covers all data formats, including paper documents, digital records, emails, website content, and mobile communication logs. This policy is strictly binding on all Councillors, the Clerk, any employed staff, volunteers, and any contractors acting on behalf of the Council.

1.3 Legal Framework

This policy is constructed to adhere to standard local government best practices and conforms to the following:

- The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (specifically the principle of storage limitation).
- The Freedom of Information Act 2000.
- The Local Government Act 1972 (Section 228 regarding public access to minutes).

- The Limitation Act 1980 (governing legal time limits for claims).
- The National Association of Local Councils (NALC) Legal Topic Note 40 (LTN 40).[1]

2. Responsibilities

- **The Council:** Overall accountability for data compliance.
- **The Clerk / Proper Officer:** Day-to-day management, storage, and secure destruction of records.
- **Individual Members:** Management of council data on their personal or official devices.

3. Retention Principles

- **Data Minimisation:** Do not hold personal data longer than necessary.
- **Accuracy:** Maintain up-to-date records and delete duplicates.
- **Secure Storage:** Protect digital data with passwords, and physical data with lock & key.

4. Retention Schedule

A detailed list of retention requirements is at Appendix. The following summary provides an overview of key areas:

Record Type	Retention Period	Reason / Statutory Requirement
Members' Declarations of Acceptance of Office	Term of Office + archived permanently	Statutory requirement; historical/public record
Register of Members' Interests Forms	18 months post-member leaving office	Good practice per NALC guidelines; removes expired personal data
Signed Council & Committee Minutes	Indefinite / Permanent	Statutory public record; to be archived
Draft Minutes/Rough notes taken at meeting	Until formal approval/signing	No longer needed once confirmed
Agendas, Public Reports and Financial records	6 years	Audit cycle and legal challenge window
Routine Emails & Correspondence	Retain only as long as useful	UK GDPR; purge when no longer of operational value
Complaint Files	5 years after case closed	Management and risk mitigation
Unsuccessful Job Applications	6 months	Defence against discrimination claims under the Equality Act 2010

[1] NALC Legal Topic Note 40 (LTN 40) is the definitive guide for local councils on document management and retention. It outlines statutory retention periods for various council records to ensure compliance with the Limitation Act 1980 and to satisfy audit and legal requirements

5. Disposal and Destruction

- **Paper Records:** Confidential papers must be shredded or disposed of via a secure waste contractor.
- **Electronic Records:** Hard drives, emails, and cloud storage must be permanently deleted (and purged from electronic bins).
- **Leaving Office:** Mandatory protocol for departing councillors is to delete all council emails and files held on personal devices (including archives and backups), and return/shred papers.

6. Policy Review

- **Frequency:** This policy is reviewed annually at the Annual Meeting of the Parish Council.
- **Next Review Date:** 31/03/2027