



EARBY TOWN COUNCIL

INFORMATION TECHNOLOGY POLICY

Introduction	2
Definitions	2
Scope	2
Use of Council email	3
IT Provision and Asset Management	4
Privacy, GDPR and Data Protection	5
IT Security and Online Safety	5
Training	6
Review	6
Breaches of the Policy	6

Date of Policy: 24th June 2025
Date of Approval: 30th June 2025
Policy version reference: v1.1
Policy effective from: 30th June 2025
Date for next review: 30th June 2030

Introduction

The purpose of this policy is to ensure that all employees, councillors and third parties requiring access to Earby Town Council Information Technology (IT) have a clear understanding of their responsibilities in **protecting data held by Earby Town Council, maintaining security** and ensuring **compliance with UK legislation**.

It is designed to avoid the Council suffering

- Data breaches – through the loss of, or the inappropriate sharing of personal information.
- Breach of legislation.
- Loss of public confidence.

Definitions

The following definitions are used in this policy:

- **Users:** Council members, employees, contractors and volunteers with access to the council systems on a permanent or temporary basis.
- **Data:** Any digitally stored information, including but not limited to documents, emails, copyrighted material, personal information and accounting records.
- **Hardware:** Includes but is not limited to desktop computers, laptops, tablets, smartphones, IP telephones and
- **Software:** Includes but is not limited to remote access connections, video conferencing, webmail, accounting software, cloud based storage and council websites.
- **Service Provider:** Includes but is not limited to Apple Inc, Microsoft, Parish Online, Intuit Ltd and Amvia Ltd.
- **Data Processor:** The Council processes personal data as part of its usual business and must comply with UK GDPR and the Data Protection Act 2018 which controls how our organisation uses and stores personal information.
- **Data Controller:** The Town Manager is the organisations data controller and responsible for determining the purpose and means of processing how personal data is collected, used, stored, shared and deleted.

Scope

This policy applies to all councillors, employees, contractors and volunteers who use IT systems to carry out council business digitally – whether on council owned devices or using personal equipment for access to council data (e.g. using personal devices to access the earbytowncouncil.gov.uk email service and personal data therein).

This policy should be read in conjunction with the Council's Data Protection Policy and GDPR (General Data Protection Regulations).

Use of Council Email

Earby Town Council uses a UK Government approved email service provider and **.gov.uk** domain for its website and email which provides a higher level of security and public reassurance when used correctly.

On becoming a Member of Earby Town Council, Councillors are allocated a Council email address solely for council business use, including communication with the public and partners on council related matters. The use of a council email address for council communication is a requirement of becoming a councillor with Earby Town Council, members should not use personal email accounts which may then become subject to Freedom of Information Act requirements to retain and reveal when justified.

The Town Manager shall not circulate material containing council/personal data to Members via personal email addresses. This is necessary to prevent data breaches by providing the required minimum levels of security on email servers, deal effectively with spam and phishing attempts, centrally quarantine suspicious email, block known malicious email and provide the necessary archive access should Members be in breach of the Code of Conduct in their email communications, and to serve requests for Freedom of Information enquiries.

Members and staff shall ensure that council email communication always remains civil and respectful and withstands the scrutiny of being read by a third party should the requirement arise. This applies equally to accounts accessed on personal devices as the email service and message archive is stored remotely.

The email addresses for all Members are published online in various locations and are therefore vulnerable to Email Display Name Spoofing whereby criminals attempt to disguise their identity by displaying the name of a council colleague in their email to recipients. Despite tools to prevent this being implemented, this can still occur, caution should be exercised in opening all emails and instances of Spoofing should be reported to the Town Manager for action.

Members should not open suspicious emails identified from the text summary or display name, nor click on links contained in any emails opened and then found to be suspicious. Do not forward suspicious emails, instead take screenshots, mark them as SPAM in your email software and delete them. Users should seek advice if you are unsure how to minimise risk in dealing with malicious email.

Group emails sent from the council account where the recipients are not known to be known to each other, shall not disclose personal email addresses to others by using the TO: address field for all addressees. In this scenario, recipients shall be added to the BCC: (Blind Carbon Copy) address field.

Passwords associated with each council email account shall be allocated by and centrally retained by the Town Manager to facilitate access, when approved by full council, to deal with complaints or to deal with appropriate Freedom of Information requirements. Periodic requirements for password resets will be implemented and passwords will be complex, unique passwords, not used in other software by the user.

Users should ensure that council email is only accessible by the User. Members should not access council email on personal devices that are accessible to family members or others unless it can be secured by logging off a personal profile.

Protected Pages on the Council's Website

On becoming a Member of the Town Council, Councillors will be allocated a password to enable a log in for the Council's website where information is shared for Members information. The information contained therein is subject to copyright held by third parties and is not for further dissemination without consultation with the Town Manager.

Use of USB/Card Storage Devices

Members shall not use USB, SD or other portable storage devices with Council owned desktop computers, laptops, tablets or mobile devices. This is to minimise the risk of transferring and introducing viruses and malicious software into the council's IT environment. Advice should be sought on the transfer method of external files that need to be shared with colleagues and partners.

The following sections primarily apply to the Town Manager, Responsible Finance Officer and any other member of staff or the audit team that has access to the Council's business systems, hardware and software.

IT Provision and Asset Management

Information Technology devices, software, data access and services provided remain property of the Council and hardware shall be recorded on the asset register. At the end of any period of holding office, employment with or work for the Council, all equipment must be returned to the Town Manager, Chair or Vice-Chair in full working condition. If equipment has been lost or damaged, or not returned within 14 days of leaving office, a charge may be made for its replacement or repair. Users must comply with all relevant policies, procedures and UK legislation with respect to the use of IT hardware.

All IT provision should:

- demonstrate value for money.
- provide value for Council or Town Manager/RFO use, in enabling efficient working and not contributing to unnecessary bureaucracy.
- include consideration of purchase/subscription cost vs time spent carrying out tasks which could be offset using the technology.
- maintain the privacy of councillors, council employees, subcontractors and the electorate.

Hardware provided should only be used for Council business and not personal use.

The installation of games, personal social media and TV/film streaming software is not permitted on council hardware. The absence of a TV Licence at the Council Offices shall

prevent the use of a wide range of live TV broadcasting applications (e.g. BBC iPlayer, ITVX, YouTube, Freeview, Sky and Virgin Media) regardless of the device used.

Privacy, GDPR and Data Protection

Users must:

- not leave their user accounts logged in on an unattended and unlocked device.
- use suitable secure methods for storing and accessing data and services.
- not perform any unauthorised changes to the IT systems or information; changes must only be made with agreement from the Chair and at least one other councillor, or at full Council where applicable.
- not attempt to access or use data or software that they are not authorised to use or access.
- not give or transfer Council data or software to any person or organisation outside the Council without the appropriate authority and reason to do so.
- adhere to the Data Protection Policy and Document Retention Policy.
- comply with all relevant policies, procedures and UK legislation with respect to the use of IT software, if unsure about this then users should check with the Town Manager or Chair.

Where users use their own hardware to access Council systems or data, they are responsible for ensuring the security of systems and data as per this policy, the Data Protection Policy and the Document Retention Policy.

Personal use is not permitted for any Council provided communication services, software applications (downloaded or software as a service) or data, unless such data is already in the public domain.

Any correspondence undertaken on behalf of the Council on Council provided or personal devices or services, where retained in line with the Retention Policy, should be provided upon request to the Town Manager or Chair, particularly, but not limited to the case of a Freedom of Information request.

IT Security and Online Safety (passwords and remote access)

Passwords should be either a minimum of 20 random letters, numbers or symbols (ideally 24 plus), or four or five random words joined with non-alphanumeric characters. Where a service offers two factor authentication then this must be used, if possible, with a hardware security key or software two factor authentication (e.g. Microsoft authenticator) secured by a strong log-in or password. Where a device is provided for an extended period to a Councillor or employee of the Council and this device offers biometric authentication, then this should be activated and utilised.

Any loss of, or damage to equipment should be reported as soon as possible to the Town Manager and Chair and any criminal damage will be reported to the Police by the Town Manager.

Any loss of personal data as the result of loss or theft of equipment shall be reported immediately to the Town Manager and Chair for action and thereafter Information Commissioner's Office (ICO).

Training

Users will be provided with appropriate and tailored training, both formal and informal, to satisfactorily achieve a level of competence in their use of Council Information Technology.

Dependant on the role and experience of an employee, training and continuous professional development may be necessary in the following areas:

- The legal responsibilities of the employee in processing and controlling personal data under the Data Protection Act and GDPR
- The use of essential software applications
 - Email
 - Email Account Management, including Security and Maintenance
 - Accounting Software
 - Business Banking
 - Password Security Management
 - Cloud Storage of council documentation
 - Office Suite Software
 - Mapping and Asset Management
 - Remote Building Alarm Access
 - Building Access Control System
 - Public Toilet Access Control System
 - Remote Boiler Control Access
 - CCTV image retrieval and retention
 - Task Management
- Performing Firmware and Software updates to IT assets

Review

To accommodate the pace of change in Information Technology, this policy shall be reviewed annually in the month of May ahead of the Annual Meeting of the Town Council.

Breaches of the Policy

Failure to adhere to the requirements of this policy may result in restricted IT access, removal of council issued devices, in disciplinary action or sanctions, or legal action by council or third parties.

On the implementation of this policy and/or on the appointment of a new User, all Users must read and acknowledge the content of this policy in writing to the Town Manager.