

BARLBY and OSGODBY TOWN COUNCIL

IT and SOCIAL MEDIA POLICY

Introduction

Barlby and Osgodby Town Council (the Council) recognises the importance of effective and secure information technology (IT), Email and Social Media 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 Employees, Councillors, Volunteers and Contractors. This policy applies to all individuals who use the Council's IT resources, including computers, networks, software, devices, data, and Email accounts.

Communication

All communications from the Council will meet the following criteria : be professional, relevant and respectful in tone and not contain content that is unlawful, libellous, obscene, harassing, defamatory, abusive, offensive or threatening. Communications should not contain un-necessary personal information, political information or known copyrighted material. Caution must be used with Email attachments and links to avoid phishing and malware.

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.

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. 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.

Data Management and Security

All sensitive and confidential 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.

Password and Account Security

IT 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.

Security, Training and Awareness

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. The Council will provide training and resources to educate users about IT security best practices, privacy concerns, and technology updates.

Monitoring

The Council Manager is responsible for approving and moderating publication of content to the Website and Social Media pages to communicate with residents, local groups and organisations and external bodies. Any monitoring to ensure compliance with this policy and relevant laws will be conducted in accordance with the Data Protection Act and GDPR.

Retention and Archiving

Emails should be retained/archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an organised inbox.

Acceptable Use of IT Resources and Email

The Council's IT resources and email accounts are to be used primarily 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.

Compliance

Confidential or sensitive information must comply with the Confidential Information Policy. Breach of this IT and Social Media Policy may result in the suspension of IT privileges and further consequences as deemed appropriate. All Staff and Councillors are responsible for the safety and security of the Council's IT and email systems to create a secure and efficient IT environment. This Policy will be reviewed regularly to ensure relevance and add updates to address emerging technology trends/security measures.

May 2025

Reviewed : May 2026