



**Birchington Parish Council
Information, Communication & Technology (ICT) Policy**

1. Introduction

1.1 This policy sets out the requirements for the secure, lawful and appropriate use of Birchington Parish Council's Information, Communication and Technology (ICT) systems.

1.2 The Council's ICT systems include desktop computers, laptops, tablets, mobile phones, telephones, email systems, internet access, cloud services and any other digital systems used to conduct Council business.

1.3 ICT systems are provided primarily for official Council business. Limited personal use is permitted in accordance with this policy.

1.4 This policy applies to:

- All Councillors
- All employees
- Temporary staff
- Contractors
- Any authorised third parties with access to Council systems

1.5 Failure to comply may result in withdrawal of access, disciplinary action, or legal action where appropriate.

2. Purpose

This policy aims to:

- Safeguard Council data and digital assets
- Ensure compliance with UK GDPR and the Data Protection Act 2018
- Support compliance with the Council's adopted Data Protection Policy
- Reduce cyber security risks
- Protect the Council's reputation

3. Governance and Responsibility

3.1 Birchington Parish Council, as Data Controller, has overall responsibility for compliance with data protection legislation .

3.2 Day-to-day responsibility for ICT governance and data protection compliance is delegated to the Parish Clerk.

3.3 The Council's IT provider is: TQS Total Quality Systems Limited

3.4 All users are personally responsible for protecting Council data and ICT systems.

4. Acceptable Use

4.1 ICT systems must be used lawfully, professionally and in accordance with this policy.

4.2 Limited personal use is permitted provided that it:

- Does not interfere with Council duties
- Does not incur significant cost

- Does not breach this policy
 - Is conducted during breaks or outside core working hours
- 4.3 Users must not access, create, store or distribute material that:

- Is unlawful
- Is discriminatory, abusive or obscene
- Harasses, intimidates or bullies
- Damages the Council's reputation
- Contains viruses or unlicensed software

4.4 Council business must not be conducted through private email accounts, personal cloud storage services or messaging platforms (including WhatsApp).

5. Passwords and Authentication

5.1 All accounts must use strong passwords in line with National Cyber Security Centre (NCSC) guidance (e.g. three random words).

5.2 Multi-Factor Authentication (MFA) must be enabled wherever available.

5.3 Passwords:

- Must not be shared
- Must not be written down insecurely
- Must not be stored in plain text
- Must be changed immediately if compromise is suspected

5.4 Administrative credentials are securely managed by TQS.

6. Equipment and Asset Management

6.1 All ICT equipment remains the property of Birchington Parish Council.

6.2 Equipment must:

- Be handled with care
- Not be dismantled or altered without authorisation
- Be protected from damage

6.3 An asset register will be maintained.

6.4 Faults, damage or security concerns must be reported immediately to the Clerk or TQS.

6.5 Unauthorised software must not be installed.

6.6 Personal USB storage devices must not be used without prior approval.

7. Portable Devices

7.1 All portable devices used for Council work must:

- Be password or PIN protected
- Use encryption where available
- Automatically lock after inactivity

7.2 Devices must not be left unattended in public places.

7.3 Devices must not be left in vehicles except temporarily and secured in the boot.

7.4 Lost or stolen devices must be reported immediately to the Clerk and TQS.

8. Use of Personal Devices (BYOD)

8.1 Personal devices may be used to access Council systems.

8.2 When using personal devices:

- Council emails must be sent only from Council email accounts
- Secure Wi-Fi must be used
- Devices must be kept updated
- Strong passwords must be used
- Council data must not be permanently stored on the device

8.3 Council data must remain separate from personal data wherever possible.

8.4 The Council reserves the right to remove Council data from personal devices where necessary.

8.5 Users are responsible for the security and maintenance of their own devices.

9. Email Use

9.1 Council email accounts are provided for official Council business.

9.2 Limited personal use is permitted in accordance with Section 4.

9.3 Emails may be subject to disclosure under:

- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- UK General Data Protection Regulation
- Data Protection Act 2018

9.4 Users must not:

- Represent personal views as Council views unless authorised
- Forward confidential or sensitive information to private accounts
- Amend and forward received emails without clearly identifying changes
- Send personal data unless there is a lawful basis to do so

9.5 Authorised Email Signature Block (Mandatory)

All Councillors and staff must use the approved Birchington Parish Council email signature block for all outgoing Council emails.

The signature must include:

- Name
- Official title
- Council name
- Council postal address
- Council telephone number
- Official Council email address
- Council website
- The approved Council email disclaimer

The approved disclaimer wording is:

EMAIL DISCLAIMER:

This email and any attachments are intended for the named recipient(s) only and may contain confidential information. If you have received this email in error, please notify the sender immediately and delete it from your system.

Any views expressed are those of the author and do not necessarily represent those of Birchington Parish Council.

Birchington Parish Council processes personal data in accordance with the UK General Data Protection Regulation and the Data Protection Act 2018. Further information about how the Council manages personal data is available in the Council's Data Protection Policy on our website:

www.birchington-pc.gov.uk

Although reasonable precautions are taken to ensure this email is free from viruses, the Council cannot accept responsibility for any loss or damage arising from its use.

9.6 The authorised signature block must not be altered to include:

- Personal slogans or quotations
- Political messaging
- Links to external organisations
- Personal social media accounts

9.7 The Clerk is responsible for maintaining and updating the standardised signature format.

10. Internet Use and Copyright

10.1 Internet access is provided for Council business.

10.2 Users must comply with the Copyright, Designs and Patents Act 1988.

10.3 Users must not:

- Download copyrighted material unlawfully
- Access inappropriate or illegal content
- Install unauthorised software

11. Monitoring

11.1 The Council reserves the right to monitor:

- Email usage
- Internet access
- Network activity
- System logs

11.2 Monitoring will be lawful, proportionate and conducted in compliance with UK GDPR .

11.3 Monitoring may be undertaken for security, maintenance, audit or investigative purposes.

12. Remote Working

When working remotely users must:

- Not save passwords on shared devices
- Log out after sessions
- Ensure screens cannot be overlooked
- Securely store printed documents
- Avoid unsecured public Wi-Fi
- Use secure connections wherever possible

Sensitive data must not be accessed in insecure environments.

13. Social Media

13.1 Councillors and staff must not claim to speak on behalf of the Council unless authorised.

13.2 Social media must not be used to:

- Disclose confidential information
- Post discriminatory or defamatory content
- Damage the Council's reputation

13.3 Councillors must comply with the Members' Code of Conduct and Nolan Principles.

14. Data Protection and AGAR

14.1 All ICT use must comply with the Council's adopted Data Protection Policy .

14.2 Any suspected personal data breach must be reported immediately to the Clerk.

14.3 The Parish Clerk is responsible for completing AGAR Assertion 10 (Information Governance).

15. Health & Safety

15.1 The Council will comply with Display Screen Equipment (DSE) regulations.

15.2 Users must report workstation concerns to the Clerk.

16. Misuse

Misuse of ICT systems may result in:

- Withdrawal of system access
- Disciplinary action
- Dismissal (employees)
- Legal proceedings

Serious breaches may constitute gross misconduct.

17. Reporting Security Incidents

All suspected security incidents, phishing emails or data breaches must be reported immediately to:

The Parish Clerk

or

TQS Total Quality Systems Limited

Adopted on:

Minute Reference :

Review Date: Annually