BRACEBRIDGE HEATH PARISH COUNCIL

The Heath: Village Hall & Library, Red Hall Lane, Bracebridge Heath, LN4 2LB
07899 888530 – clerk@bracebridgeheath-pc.gov.uk

IT Policy

Contents

1. Introduction

1.1. Bracebridge Heath Parish Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications.

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

1.3. The aims of this policy are to:

- facilitate the ongoing development of the efficient management and delivery of the Council's services.
- provide opportunities for staff to acquire and develop core ICT competencies.
- ensure that the Council's ICT systems are reviewed regularly and adjusted to meet new or changing need.

2. Scope

2.1. This policy applies to all individuals who use Bracebridge Heath Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts. This includes but is not limited to:

- employees
- elected members (councillors)
- members of the public
- other people, companies, contractors and organisations in contact with Bracebridge Heath Parish Council.

3. Acceptable use of IT resources and email

3.1. Bracebridge Heath Parish 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.

4. Device and software usage

4.1. Where possible, authorised devices, software, and applications will be provided by Bracebridge Heath Parish Council for work-related tasks.

4.2. Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

5. Data management and security

5.1. All sensitive and confidential data held by or belonging to the parish council 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. The council currently uses Microsoft Office Sharepoint for data storage.

5.2. All 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.

5.3. In line with the council's Data Protection policy, all suspected security breaches or incidents should be reported immediately to the clerk to council for investigation and resolution

5.4. All members, employees or volunteers must report any incidents which could pose a risk to the council's systems or data security to the Town Clerk without delay. This includes but is not limited to:

- Lost devices
- Potential risk arising from phishing emails/websites
- Passwords having been shared
- Unauthorised access to systems

6. Network and internet usage

6.1. Bracebridge Heath Parish 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.

7. Email communications

7.1. Bracebridge Heath Parish Council provides a separate email account for all employees and members of council using the bracebridgeheath-pc.gov.uk domain. The email accounts are hosted through Microsoft. The clerk (or other designated person) will set up a new email accounts as required.

7.2. Councillors and employees are not permitted to use any other private or personal email account for council business.

7.3. A Council email account may not be used for personal purposes. Any email account used for council business should be accessed only by the member to whom it belongs.

7.4. When councillors or employees, cease to be part of the Parish Council, their email account will be closed down and all emails (sent or received) will be archived or deleted in accordance with Council's Document Retention Policy.

7.5. All users should regularly review and delete unnecessary emails to maintain an organised inbox. Emails should be retained and archived in accordance with legal and regulatory requirements.

7.6. The following disclaimer should be appended to all outgoing emails:

This email, content and any files transmitted with it are confidential and intended solely for the use of Bracebridge Heath Parish Council and the individual or entity to whom they are addressed. If you have received this email in error please forward it to the sender and delete it from your system. Thank you

8. Inappropriate use

8.1. Users must not use email to abuse or inflame others or to harass or threaten anyone. Responding to abuse, harassment or threatening will not be accepted as an excuse for inappropriate language and/or behaviour. Users must not send emails containing obscene, abusive or profane language.

8.2. Recipients of abusive or threatening emails related to the business of the Council must immediately inform the clerk or chairman.

8.3. Users must not send, access, display, download, copy or circulate information to containing stories, jokes or anecdotes that contain:

- pornography or sexually orientated images
- gambling
- gaming (playing computer games)
- promotion of unlawful discrimination of any kind
- promotion of racial or religious hatred
- threats including the promotion of violence
- fraudulent or illegal material promotion of illegal and/or unlawful acts
- information considered to be offensive, inappropriate or disrespectful to others
- unauthorised and copyrighted material including music.

8.4. Bracebridge Heath Parish Council will report to the police all known incidents in which users intentionally send or receive emails containing the following:

- Images of child pornography or child abuse (i.e. images where children are or appear to be under the age of 16 and are involved in sexual activities or posed to be sexually provocative)
- Adult material/pornography that breaches the Obscene Publications Acts (1959 & 1964)
- Criminally racist material

8.5. Users must not send, receive or disseminate proprietary data or any confidential information belonging to Bracebridge Heath Parish Council to or from a third party unless authorised.

9. Email monitoring

9.1. Bracebridge Heath Parish 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.

9.2. On the receipt of a Freedom of Information request or Subject Access Request it may be necessary for a member of staff to be given access to employee or councillor email accounts allocated by the Council. You will be informed if this is necessary to allow the Council to fulfil the request.

10. Mobile devices and remote work

10.1. 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.

11. Training and awareness

11.1. The council will provide regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will receive regular training on email security and best practices.

12. Compliance and consequences

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

13. Contacts

13.1. For IT-related enquiries or assistance, users can contact the clerk – clerk@bracebridgeheath-pc.gov.uk / 07899 888530.

13.2. All staff and councillors are responsible for the safety and security of the council's IT and email systems. By adhering to this IT Policy, Bracebridge Heath Parish Council aims to create a secure and efficient IT environment that supports its business activities.

14. Responsibilities & review

14.1. The clerk, on behalf of the Council, is responsible for the administration of this policy and will report breaches to the Full Council for advice about further action.

14.2. The Full Council is responsible for reviewing this policy. This policy will be reviewed every three years or in response to changes in the law.

15. Related legislation, policies and guidance

15.1. This policy is not a substitute for legislation, regulations and codes of practice but defines how the Council will apply the relevant legislation. Related legislation, policies and guidance are listed below:

- General Data Protection Regulations (GDPR) 2018
- Freedom of Information Act 2000

Bracebridge Heath Parish Council internal documents:

- Data protection policy
- Subject Access Request procedure
- Privacy notices
- Document Retention policy

16. Version control and amendment history

Date approved	Version Number	Revision / amendments made	Review date
June 2025	1.0	New policy. Replaced email and internet usage policy.	June 2028
February 2026	2.0	Addition of appendices – IT security briefing and acceptable use of AI	June 2028

Appendix A: IT Security Briefing: Essential Guidance for Staff & Councillors

This briefing supports the Council's IT Policy by providing practical, everyday advice to help protect council systems, data, and email accounts. All users of council-provided IT equipment and accounts are expected to follow these good-practice guidelines.

1. Password management and resets

Strong passwords are one of the simplest and most effective ways to protect council data.

Good practice

- Use long passwords or passphrases (e.g. "GreenHedgeHorse92!").
- Avoid using personal information such as birthdays, names, or pets.
- Use a different password for each account.
- Change passwords immediately if you suspect they've been shared or compromised.
- Never write passwords on paper or store them in unsecured documents.
- Enable multi-factor authentication (MFA) wherever available.

Warning signs of a compromised password

- Unexpected login alerts
- Emails sent from your account that you didn't write
- Files moved, deleted, or shared without your knowledge

Resetting your password

- If you have forgotten your password or need to reset it, please contact the Clerk by telephone or by coming into the parish office.
- Password resets will be performed using the Microsoft 365 Admin account and the Clerk will advise you of the temporary password.
- The Clerk will never reset your password without your request to do so and will never send an email for you to reset your password via a link.
- Report any concerns to the Clerk immediately.

2. Cyber security basics

Council devices and accounts must be used responsibly to reduce the risk of cyber-attacks.

Keep devices secure

- Lock your device whenever you step away.
- For staff, install only authorised software — never download apps or tools without approval.
- Keep systems updated; install updates when prompted.
- Use council-approved storage only (e.g., SharePoint). Avoid USB sticks unless authorised.

Safe browsing

- Only access trusted websites.
- Avoid clicking pop-ups or "free download" offers.
- Do not use public Wi-Fi for council work unless using a secure connection.

3. Identifying scams and phishing attempts

Phishing is one of the most common threats to councils. Attackers often impersonate trusted organisations or colleagues.

Common signs of phishing

- Unexpected emails asking you to click a link or open an attachment

- Messages claiming “urgent action required”
- Poor spelling, unusual formatting, or unfamiliar sender addresses
- Requests for passwords, bank details, or personal information
- Emails pretending to be from Microsoft, HMRC, Royal Mail, or an officer or another councillor

If you receive a suspicious email

- Do not click links or open attachments
- Do not reply
- Report it to the Clerk immediately
- Delete it once advised
- If you accidentally click something, report it straight away — early reporting reduces risk.

4. Mobile devices & remote working

- Keep devices locked with a PIN, password, or biometric security
- Never leave devices unattended in vehicles or public spaces
- Be mindful of who can see your screen
- Store all council information in SharePoint, not on personal devices
- Lost or stolen devices must be reported immediately.

5. Stay vigilant

Everyone plays a role in keeping the council’s systems secure. If something feels unusual, unexpected, or “not quite right”, trust your instincts and check before acting.

For advice or to report an issue, contact:
clerk@bracebridgeheath-pc.gov.uk / 07899 888530

Appendix B: Acceptable use of AI

This appendix supports the Council's IT Policy. By outlining safe, responsible, and practical ways to use Artificial Intelligence (AI) tools when carrying out council business.

DO:

Use AI to support routine council work

- Draft non-confidential emails, letters, reports, or summaries
- Generate ideas, templates, agendas, or training materials
- Rewrite text for clarity, accessibility, or plain English
- Summarise publicly available information
- Use AI to improve efficiency — not to replace your judgement

Protect council data

- Use AI only on secure council devices and accounts
- Review all AI-generated content before sharing
- Check for inaccuracies, missing context, or invented details
- Ask the Clerk if you're unsure whether something is appropriate

Stay transparent and accountable

- Treat AI as a tool — you remain responsible for the final output
- Be open about using AI where appropriate (e.g., "draft prepared with AI assistance")
- Follow all council policies, including Data Protection and IT Security

DON'T:

Enter personal or confidential information. AI tools must not process personal data unless explicitly approved and compliant with GDPR.

- Never input into AI tools: names, contact details, case information, complaints, safeguarding concerns, financial details, internal or unpublished council documents

Rely on AI for decisions

- AI must not make decisions affecting residents, staff, or council operations
- Do not use AI to interpret legal, HR, or safeguarding matters
- Always apply human judgement and follow proper procedures

Don't use AI for inappropriate or risky content

- No political messaging or campaigning
- No discriminatory, defamatory, or misleading content
- No content that could damage the council's reputation
- No bypassing of established approval or governance processes

Don't assume AI is correct

- AI can produce inaccurate or fabricated information
- Never copy and paste outputs without checking
- Don't share AI-generated content externally without review

If in doubt, ask the Clerk before using AI for council business.
Contact: clerk@bracebridgeheath-pc.gov.uk / 07899 888530