IT Policy

Policy Statement

Bearsted Parish Council 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.

Scope

This policy applies to all individuals who use Bearsted parish council's IT resources, including:

- Computers, laptops, tablets, and smartphones
- Email and internet usage
- Data protection and storage
- IT security and software
- Social media and online communication

Responsibilities

The Clerk is the designated IT lead.

Bearsted Parish Council outsource IT responsibility for maintaining council owned devices, systems and access to third parties, namely Parish Council Websites, Computer 4U and Secure Tech Systems Ltd.

Councillors and staff are responsible for using IT systems responsibly and in accordance with this policy.

Acceptable use of IT resources and email

All Staff and Councillors are required to read and comply with the conditions of this policy in respect of the way in which the communications mechanisms are utilised. The policy includes computers and all other electronic media.

1. The Council recognises that reasonable use of e-mail facilities to communicate brief personal non offensive messages is acceptable and is a privilege that the Council is prepared to allow, but the amount of time spent must not be abused or it will be stopped.
2. The Council recognises that access to professional information by e-mail or through web sites is a necessary requirement of the job of the Clerk to the Council, other staff and Councillors, therefore this is permitted.
3. Staff and users are expected to use technology in a courteous, reasonable and responsible manner. The following activities are not acceptable, and anyone found to be involved in them may face disciplinary action. In certain instances, the matter will be considered to be gross misconduct:

- Receiving, sending or displaying messages or pictures that are offensive or may be construed to be offensive in nature.
- Using obscene language.
- Improper use of e-mail and internet.
- Damaging computers, computers systems or computer networks.
- Violating copyright laws.
- Using others' passwords and identities.
- Issuing of passwords to third parties unless authorised to do so; trespassing in others' folders, works or files.
- Intentionally wasting limited resources.
- Employing the system for commercial purposes.
- Employing the system for illegal activities.
- Downloading any commercial software.
- Use of personal mobile phones in meetings and during any other Council business (unless authorised).

Potential abuse of the Parish Councils IT equipment or systems should be referred to the Parish Council's HR Committee in the first instance for investigation. Please refer to the BPC Disciplinary Procedure Policy.

1. The Council encourages electronic communications with local, national and international organisations.
2. The computer equipment and software must be used as installed. Staff and users may not install/uninstall, delete or change anything on Council computers. Any requirements to change anything should be authorised by the Clerk to the Council and/or the Chairman of the Council.
3. Access to chat rooms, gaming and other associated sites are not permitted on Council computers.
4. Councillors should only initiate and respond to council business using their assigned @bearstedparishcouncil.gov.uk domain email address. Passwords to this account should not be shared.
5. Emails sent to and from Councillors should be kept for a maximum of 6 months. Emails sent to and from the Parish Office that are deemed routine shall be kept for 6 months with any email sent to or from the Parish Office that are deemed important will be kept indefinitely.

Email and Other Communication

- Official communication should be conducted through parish council email addresses.
- Users must not open suspicious attachments or links.
- Emails should be written professionally and archived as appropriate.
- You Should not forward emails with personal data or links to papers to 3rd parties.
- WhatsApp: no personal data regarding residents or 3rd parties are to be shared on the Council WhatsApp group.
- Information containing personal data should be downloaded or printed unless absolutely necessary. Print outs should be returned to the office to be destroyed confidentially. Stored data must be password protected or encrypted.

Please refer to BPC Email Etiquette Policy

Data Protection and Privacy

- Personal data must be processed fairly and lawfully and only used in line with the UK GDPR and the Data Protection Act 2018 regulations.
- Devices should be password-protected.
- Confidential data should not be stored on personal devices unless encrypted.

Please refer to BPC Privacy Policy

Social Media

When staff and Councillors are using social media sites they should always follow these guidelines:

- Posts on official platforms must reflect council decisions and policies.
- No personal opinions should be shared on behalf of the council.
- Access to accounts should be restricted to authorised individuals only.
- Information published on social media should be deemed relevant to the Parish Council or the community that it represents.
- Information should be accurate, fair, thorough and transparent.
- It should be noted that what is published will be in the public domain indefinitely.
- Compliance with data protection, intellectual property and copyright laws should be ensured.
- Details about customers, partners, or suppliers should not be referred to without their prior written approval (ensuring no advertisement of the services or goods of third parties).
- Staff and Councillors must refrain from promoting themselves as working for the Council in a way which has, or may have, the effect of bringing the Council into disrepute.
- Staff and Councillors must not disclose personal data or information about the Council or its service users, employees or Councillors that could breach the Data Protection Act 2018 (e.g. Photographs, images).
- Staff and Councillors must not make any defamatory remarks about the Council, its service users, employees, Councillors, members of the public or conduct themselves in a way that is detrimental to the Council.

Please refer to the BPC Publicity Policy

Security and Updates

- Antivirus software must be installed and regularly updated.
- Software and devices should be kept up to date.
- Lost or stolen devices must be reported immediately to the Clerk.

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

Bearsted parish council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others. Passwords should be changed if you believe your password has become known to someone.

Back Ups & Records

- Key data (e.g., meeting minutes, financial records) must be regularly backed up.
- Cloud storage may be used, provided it meets UK data protection standards.

Mobile devices and remote Work

Mobile devices provided by Bearsted parish 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.

When using own devices to access Council emails and papers, Cllr's must ensure:

- The access to Council emails, data and information is password protected and not accessible to others.

- The device is still supported by the manufacturer and still receives operating system updates to ensure protection against unauthorised access.
- 2 step authentication is recommended for accessing Council emails.

Breaches and Misuse

Bearsted 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.

Breaches of this policy may result in removal of IT access or further action by the council.

Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the designated IT point of contact for investigation and resolution.

Training and awareness

Bearsted parish council will provide training and resources to educate users about IT security best practices, privacy concerns, and technology updates.

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.