

IT Policy

1. Purpose and Scope

- 1.1 This policy sets out how Honeybourne Parish Council (the Council) uses information technology (IT) to conduct its business securely, efficiently, and in compliance with legal requirements.
- 1.2 This policy applies to the Clerk/RFO, all Councillors, and any contractors who access Council IT systems.

2. Council IT Infrastructure

2.1 Equipment

The Council provides the Clerk with a laptop, a mobile phone and a printer for Council business. The Clerk does not use this equipment for personal purposes. Councillors are provided with a dedicated Council email address but use their own personal devices (phones, tablets and computers) to access Council business; the Council does not provide IT equipment to Councillors.

2.2 IT Support

The Council has contracted IT support for technical assistance and maintenance. All IT issues should be reported to the Clerk, who will coordinate with the IT support provider.

2.3 Data Storage

All Council documents, records, and data are stored securely on cloud-based storage. The Council also uses cloud-based specialist software for financial management and cemetery records management. Regular backups are maintained by the cloud providers. Access to financial and cemetery software is restricted to the Clerk. The Clerk is responsible for maintaining organised file structures.

2.4 Website and Social Media

The Council's website is professionally hosted. All content on the website belongs to Honeybourne Parish Council. The Clerk is the only person with access to upload and manage website content. Any technical issues with the website are reported to the Clerk, who will coordinate with the website host.

The Council's social media accounts are administered by the Clerk. Social media is used for information sharing only; comments are disabled. This is covered in detail by the Council's Social Media Policy.

3. Security Measures

3.1 Password Protection

The Clerk's computer is password protected. Passwords must be strong, containing a minimum of 12 characters with a mix of letters, numbers, and symbols. Passwords must not be shared with anyone and should be changed every 6 months, or sooner if a compromise is suspected.

3.2 Physical Security

The Clerk's computer is secured when not in use. No unauthorised persons have access to the Clerk's computer. Councillors should ensure their personal devices are password or PIN protected.

3.3 Access Control

Only authorised persons have access to Council IT systems. Councillor email accounts are set up by the Council's IT support provider, with each Councillor setting and managing their own password; neither the Clerk nor the IT support provider holds or has access to Councillors' passwords. The IT support provider can, however, suspend or restrict access to an account administratively (for example, if instructed to do so by the Council) without needing to know the password. The Clerk maintains a list of all Council email accounts. When a Councillor leaves the Council, the IT support provider will deactivate or reassign their email account as appropriate.

4. Email Use

4.1 Council Email Addresses

The Council provides dedicated email addresses for the Clerk and all Councillors using the domain @honeybourne-pc.gov.uk. The Clerk's email is clerk@honeybourne-pc.gov.uk and Councillors' emails follow the format firstname.surname@honeybourne-pc.gov.uk. Personal email addresses such as Gmail, Hotmail, or other free services must NOT be used for Council business.

4.2 Email Acceptable Use

Council emails must only be used for Council business. Users must not send offensive, discriminatory, or defamatory content, share confidential information without authorisation, use Council email for commercial or political campaigning purposes, or open suspicious attachments or links.

4.3 Email Retention

Emails containing Council business are subject to Freedom of Information Act requests. Important emails should be saved to the cloud storage system. The Clerk is responsible for maintaining email records in accordance with the Council's retention schedule.

4.4 Protection of Personal Information in Emails

When circulating emails to Councillors that contain personal information of third parties, the Clerk will redact personal details of senders to protect their privacy. The Clerk will seek permission from senders before sharing their contact details with Councillors unless there is a legitimate reason to do so without consent.

5. Use of Personal Devices (BYOD — Bring Your Own Device)

5.1 Councillor Devices

Councillors may access Council emails and documents on their personal devices including phones, tablets, and computers. Councillors are responsible for the security of their own devices.

5.2 Device Security Recommendations

Councillors are responsible for ensuring their devices have appropriate security measures. It is strongly recommended that devices have up-to-date security software or antivirus protection where applicable, password or biometric protection enabled, and automatic updates enabled. The Council does not provide or fund security software for Councillors' personal devices.

5.3 Data Protection on Personal Devices

Councillors must not store confidential Council documents permanently on personal devices. If documents are downloaded for meetings, they should be deleted afterwards or stored securely. Lost or stolen devices must be reported to the Clerk immediately.

5.4 Responsibility for Information Sharing

Once documents are sent to Councillors' official email addresses or provided in printed form, Councillors are personally responsible for maintaining confidentiality and complying with the Council's Code of Conduct.

Councillors must not share confidential information with unauthorised persons. The Clerk is not responsible for Councillors' actions regarding information sharing after it has been properly distributed through official Council channels.

5.5 Use of Council Email for Council Business

Councillors must use their Council email addresses for all Council business. Personal email addresses must not be used for Council matters.

Councillors are reminded that if they conduct Council business using personal email addresses, those personal emails become subject to Freedom of Information requests. This could result in personal email accounts being scrutinised and private correspondence being disclosed. To protect personal privacy and ensure proper record-keeping, all Council business must be conducted using the Council-provided email addresses.

All Council email correspondence is subject to Freedom of Information requests and must be retained in accordance with the Council's document retention policy.

6. Data Protection and Data Breaches

6.1 All users must comply with the Council's Data Protection Policy. Personal data must be processed lawfully, fairly, and transparently, and must be kept secure and not shared inappropriately.

6.2 Users must not share passwords or login credentials. Confidential documents must not be forwarded to personal email accounts. Screens should be locked when away from devices. Confidential information must not be discussed in public places.

6.3 Any suspected data breach or security incident must be reported immediately to the Clerk, or in the Clerk's absence to the Chair of the Council. The Council's Data Breach Policy sets out the full process for assessing, recording, and where necessary reporting a breach to the Information Commissioner's Office and to affected individuals, and should be followed in full.

7. Internet and Social Media Use

7.1 Internet access should be used responsibly and primarily for Council business. Users must not access illegal, offensive, or inappropriate content. Downloading unlicensed software is prohibited.

7.2 Social media use on behalf of the Council is covered by the Council's Social Media Policy. Personal social media use must not bring the Council into disrepute. Councillors must make clear when expressing personal views online that they do not represent the Council.

8. Software and Licensing

8.1 Only properly licensed software may be used on Council devices. The Clerk maintains a list of all software licenses. Installation of unauthorised software on Council devices is prohibited.

8.2 The Clerk is responsible for ensuring Council devices have up-to-date software. Security updates must be installed promptly. The IT support provider assists with major updates and technical maintenance.

9. Backup and Business Continuity

9.1 The cloud storage providers maintain automatic backups. The Clerk should verify backups are functioning periodically. Critical documents should be saved in the appropriate cloud folders promptly.

9.2 In the event of IT failure, the Clerk will contact IT support immediately. Cloud access ensures continuity, as Council data can be accessed from any device with an internet connection. Emergency contact procedures are maintained by the Clerk.

10. Reporting IT Issues

10.1 IT issues should be reported to the Clerk. The Clerk will coordinate with the IT support provider to resolve technical issues and logs all IT incidents and resolutions.

10.2 Report immediately to the Clerk if a device is lost or stolen, you suspect unauthorised access to your account, you receive a suspicious email or phishing attempt, you accidentally share confidential information, or any other security concern arises.

11. Awareness

11.1 The Clerk and Councillors will be provided with a copy of this IT Policy upon adoption. Updates to IT security practices will be communicated as needed. Councillors should raise any IT security concerns at Council meetings.

12. Policy Review

12.1 This policy will be reviewed every three years or sooner if there are significant changes to IT infrastructure, changes to relevant legislation, a serious IT security incident occurs, or best practice guidance changes.

13. Related Policies

13.1 This policy should be read in conjunction with the Council's Data Protection Policy, Data Breach Policy, Social Media Policy, Risk Assessment (including IT and cyber security risks), and Freedom of Information Publication Scheme.