



Broadmayne Parish Council IT Policy

1. Introduction

Broadmayne 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.

2. Scope

This policy applies to all individuals who use Broadmayne Parish Council's IT resources, including computers, networks, software, devices, data, website and email accounts.

3. Acceptable use of IT resources and email

Broadmayne Parish Council 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

Where possible, authorised devices, software, and applications will be provided by Broadmayne Parish Council to its employees for work-related tasks.

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

Under no circumstances should any non-public meeting or conversation be recorded without the permission of those present. This does not affect statutory rights (under the Openness of Local Government Regulations 2014).

Councillors, staff, and other authorised persons that use council systems are expected to use all devices in an ethical and respectful manner and in accordance with this policy.

5. Data management and security

All sensitive and confidential Broadmayne Parish Council data should be stored and transmitted securely using approved methods. All devices with access to Council data should be kept locked and protected with a PIN code when not in use - to prevent unauthorised access, should not be left unattended when unlocked at any time, and should never be left in parked vehicles. Regular data backups should be performed to prevent data loss, and secure data destruction methods should be used when necessary.

Personal data relating to councillors, staff, and other authorised users, associates, residents, or external stakeholders should not be saved to any personal accounts with third-party storage cloud service providers as this may breach data protection legislation or create a security risk if the device is lost or stolen. This applies especially if the passwords used to store/access data are saved onto the device, or if the service permits councillors, staff, and other authorised users to remain logged in between sessions.

Personal information and sensitive data should never be saved on councillors, staff, or other authorised users own devices as this may breach confidentiality agreements, especially if the device is used by other people from time to time.

6. Network and internet usage

Broadmayne 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 communication

Email accounts provided by Broadmayne Parish Council are for official communication only. Any emails sent from own devices should be sent from a council email account and should not identify the individual's personal email address. Emails should be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless it is encrypted.

Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

8. Password and account security

Broadmayne Parish Council 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.

9. Mobile devices and remote Work

Any mobile devices which may be provided by Broadmayne 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.

The Council recognises that some councillors, staff, and other authorised users may wish to use their own smartphones, tablets, laptops etc to access servers, private clouds or networks for normal council purposes, including, but not limited to, reading their emails, accessing documents or to store data. Any such use of personal devices will be at the discretion of the council, but consent for standard systems (MS Windows, Mac OS X, Linux - in commercial configurations) will normally be permitted. Such devices should be kept up to date so that any vulnerabilities in the operating system or other software on the device are appropriately patched or updated.

In cases of legal proceedings against the council or external stakeholders, the council may need to temporarily take possession of a device, whether council-owned or personal to retrieve the relevant data.

Wherever possible the user should maintain a clear separation between the personal data processed on the council's behalf and that processed for their own personal use, for example, by using different apps for council and personal use. If the device supports both work and personal profiles, the work profile must always be used for work-related purposes.

Councillors, staff, and other authorised users must take responsibility for understanding how their device(s) work in respect to the above rules if they are accessing council servers/services via their own IT equipment. Risks to the user's personal device(s) include data loss as a result of a crash of the operating system, bugs and viruses, software or hardware failures and programming errors rendering a device inoperable. The council will use reasonable endeavours to assist, but councillors, staff, and other authorised users are personally liable for their own device(s) and for any costs incurred as a result of the above.

10. Email monitoring

Broadmayne 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.

Such monitoring and the retrieval of the content of any messages may be for the purposes of checking whether the use of the system is legitimate, to find lost messages or to retrieve messages lost due to computer failure, to assist in the investigation of wrongful acts, or to comply with any legal obligation.

11. Retention and archiving

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

12. Reporting security incidents

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 Parish Clerk immediately.

13 Training and awareness

Broadmayne Parish Council will offer opportunities to access regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will receive training to keep them up to date on email security and best practices.

14. Compliance and consequences

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

15. 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.

16. Contacts

For IT-related enquiries or assistance, users can contact the Parish Clerk, Tim Watton in the first instance.

All staff and councillors, as well as volunteers utilising or supporting IT resources, are responsible for the safety and security of Broadmayne Parish Council's IT and email systems. By adhering to this IT and Email Policy, Broadmayne Parish council aims to create a secure and efficient IT environment that supports its mission and

goals.

Date: Adopted 7th April 2025, reviewed Oct 2026

Signature: *Tim Watton*

Role: Parish Clerk and Responsible Financial Officer

Review date Oct 2027