

MELLS PARISH COUNCIL

Information Technology and Email Policy

1. Introduction
2. Scope
3. Acceptable use of IT resources and email
4. Device and software usage
5. Data management and security
6. Network and internet usage
7. Email communication
8. Password and account security
9. Mobile devices and remote work
10. Email monitoring
11. Retention and archiving
12. Reporting security incidents
13. Training and awareness
14. Compliance and consequences
15. Policy review
16. Contacts

Appendix 1: Email Guidelines for Members of Mells Parish Council

This Policy was adopted by Mells Parish Council at its meeting on the 11 August 2026,
Minute ref: 08.08.26 i.

Review date: August 2027

1. Introduction

Mells 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 Mells Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts.

3. Acceptable use of IT resources and email

Mells Parish Council's IT resources and email accounts are to be used for official council related activities and tasks. Limited personal 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 Mells parish council for work-related tasks. Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

5. Data management and security

All sensitive and confidential Mells Parish Council data 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.

6. Network and internet usage

Mells 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 Mells Parish Council are for official communication only. 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

Mells 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

Mobile devices provided by Mells 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.

10. Email monitoring

Mells 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.

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 Clerk for investigation and resolution. Report any email related security incidents or breaches to the Clerk immediately.

13 Training and awareness

Mells Parish 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.

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 at: clerk@mells-pc.gov.uk

All staff and councillors are responsible for the safety and security of Mells Parish Council's IT and email systems. By adhering to this IT and Email Policy, Mells parish council aims to create a secure and efficient IT environment that supports its mission and goals.

Signed: _____

Date: _____

Position: _____

Email Guidelines for Members of Mells Parish Council

- (a) Do not assume that the recipient will read an email immediately, if the matter is urgent follow up the email with a phone call.
- (b) Emails enable clear communication to several people at once, but are subject to the Freedom of Information Act, therefore please ensure that only relevant facts are sent by email.
- (c) Emails should not be used as a deliberate means of avoiding personal contact where one face to face discussion can avoid an exchange of numerous e-mails.
- (d) Limit the number of copies to those that are necessary.
- (e) Do not unnecessarily broadcast information widely. Constant bombardment of individuals by irrelevant or unsolicited email is time wasting.
- (f) E-mails should be checked regularly.
- (g) Reply promptly to all e-mail messages requiring a reply. Where a prompt, detailed, response is not possible, send a short e-mail acknowledging receipt and giving an estimate of when you will provide a detailed response.
- (h) Do not either write in capitals as this can be perceived as shouting, or adopt a more aggressive tone in e-mails than you would in a face to face discussion and abide by the corporate standards for written communication.
- (i) Do not attach long files or include graphics and logos if this is not necessary.
- (j) Summary checklist
 - Is email the best way to communicate this message?
 - Think before you write.
 - Use the spell check facility
 - Check who it is being sent to. Only copy in people who you would be prepared to talk to about the subject.
 - Re-read before you send.