



middle level
commissioners

IT Policy

June 2026

1. Introduction

Middle Level Commissioners recognises the importance of effective and secure information technology (IT) and email usage in supporting their business, operations, and communications.

This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by employees.

Middle Level Board Members and administered Internal Drainage Board members, employees or officials are not provided IT resources by the Middle Level Commissioners and have no access into MLC IT systems. They are expected to act responsibly and securely, using either their personal devices and software, or that provided by their business, employer or appointing authority.

2. Scope

This policy applies to all individuals who use Middle Level Commissioners IT resources, including computers, networks, software, devices (tablets and smart mobile phones), data, and email accounts.

3. Provision of IT Resources

Employees will each be provided with the IT resources they need to undertake their work at their contracted base of employment. For office-based staff this will be a laptop (desktop by exception) with associated peripherals (e.g. keyboard, mouse, monitor). A tablet and/or mobile phone may be provided depending upon role. For field-based staff a tablet and/or mobile phone will be provided. All employees will have an MLC email address and MS365 access. Different/additional items may be justified via DSE assessments and/or as part of any reasonable adjustments.

To enable office-based staff to work flexibly, employees may be provided with an additional laptop power cable and mouse. Additional IT resources, for example, monitors, webcams, keyboards and docking stations to enable improved ability to work from home will not be provided by the employer, except if justified through formal home-working requests, DSE assessment and/or reasonable adjustments.

4. Acceptable use of IT resources and email

Middle Level Commissioners' IT resources and email accounts are to be used for official work-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 and professional

standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

Personal IT resources, including computers, software, devices (tablets and smart mobile phones), data, and email accounts must not be used for work-related purposes unless otherwise agreed.

5. Device and software usage

Where possible, authorised devices, software, and applications will be provided by Middle Level Commissioners for work-related tasks.

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

6. Data management and security

All sensitive and confidential Middle Level Commissioners owned or controlled data should be stored and transmitted securely using appropriate methods (eg encryption, password protection or controlled/limited access SharePoint). Regular data backups are performed to prevent data loss, and secure data destruction methods should be used when necessary, considering as defined within the data retention policy.

7. Network and internet usage

Middle Level Commissioners network and internet connections should be used responsibly and efficiently for work purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited.

8. Email communication and document classification

Email accounts provided by Middle Level Commissioners are for official communication only. Emails should be professional and respectful in tone. Confidential or sensitive information must be labelled as such (refer to government [guidelines](#)).

Employee must be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links. Report any issues immediately to our IT service provider.

9. Password and account security

Employees 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.

Laptops, desk-tops, mobile phones and tablets must not be left unlocked when unattended.

10. Mobile devices and remote work

Mobile devices provided by Middle Level Commissioners should be secured with passcodes and/or biometric and/or two-factor authentication. When working remotely, users should follow the same

security practices as if they were in the office. Equipment should not be left unattended and must be left out of sight and secure if temporarily left in vehicles for example.

11. Artificial Intelligence

Employees can use emerging AI tools and software to help with their work. However, employees and Middle Level Commissioners/Middle Level Board Members must not upload Middle Level Commissioners owned or controlled data and information to either closed or open AI models or software.

Employees must also respect this position with external data they or the organisation may have been provided by any 3rd parties. i.e. do not upload another organisation's information into closed or open source AI tools.

An Artificial Intelligence Policy will be drafted in due course.

12. Monitoring

Middle Level Commissioners reserves the right to monitor IT usage and email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR.

12. 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.

14. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to your line manager, Lead Clerk and/or a Chief Officer for investigation and resolution. Report any email-related security incidents or breaches to our IT Service Provider, your line manager and/or a Chief Officer immediately.

15 Training and awareness

Middle Level Commissioners will provide appropriate training and resources to educate employees about IT security best practices, privacy concerns, and technology updates.

16. Compliance and consequences

Breach of this policy may result in the suspension of IT privileges and consideration within capability and/or disciplinary procedures outlined within the Employee Handbook.

17. Policy review

This policy will be reviewed routinely to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.