CYBER SECURITY POLICY

Version	3.00	**Number of pages**	6
Responsible officer	Chief Operating Officer		
Contact	National IT Manager – itmanager@morling.edu.au Ext: 110 Senior Systems Administrator – snr.sys.admin@morling.edu.au Ext: 109		
Approving Authority	Morling College Board		
Keywords	Security; IT; Malware; IT protection; Email; Data; Password		
Access level *Select from the drop-down menu*	Public		
Dissemination Range	Staff and students		
Approval date	19 February 2024		
Effective date	13 February 2024		
Review date	20 February 2025		
Superseded documents			
Compliance References	HES_7.3.3.b		
Document classification *Select from the drop-down menu*	Admin, Information Management and Infrastructure		

1. PURPOSE

Data theft, scams, and security breaches can have a detrimental impact on our organisation's systems, and reputation. As a result, Morling College has created this policy to help outline the security measures put in place to ensure information remains secure and its integrity protected.

The purpose of this policy is to outline:

- means of protection of Morling College's data and infrastructure
- protocols and guidelines that govern cyber security measures
- rules for the organisation and personal use, and
- the organisation's disciplinary process for policy violations.

As well as providing assurance of risk management at a governance level, this is also provided as a guide to expectations of end users in contributing to cyber security.

2. DEFINITIONS

Key Term or Acronym	Definition
Confidential data	Includes, but is not limited to: • Unreleased and classified financial information. • Customer, supplier, and stakeholder information. • Customer leads and sales-related data. • Patents, business processes, and/or new technologies.

	• staff/volunteers' passwords, assignments, and personal information. • Organisation contracts and legal records.
MC	Morling College
Staff	Academic, administrative, adjunct or casual employees, whether working in the office or remotely.

3. SCOPE

This policy applies to all individuals with access to Morling College's electronic systems, information, software, and/or hardware. Individuals may include Morling College (MC) staff, students, volunteers, vendors, contractors, or any approved user.

4. POLICY STATEMENT

All those accessing MC data and systems are obliged to:

- to protect confidential data
- ensure the security of all MC devices and information,
- ensure personal device use conforms to this policy when used for MC purposes
- protect the security of the MC email and other business systems
- maintain high security passwords, and keep them secret
- protect the security of data when being transferred
- securely back up data
- securely dispose of devices
- complete cyber security training.

5. PRINCIPLES

Device Security

Organisational Device Use

5.1 To ensure the security of all organisation-issued devices and information, MC staff/volunteers are required to:

5.1.1 Keep all organisation-issued devices, including tablets, computers, and mobile devices, password-protected (minimum of 8 characters).

5.1.2 Secure all relevant devices before leaving their desk/work area.

5.1.3 Obtain authorisation from the Chief Operating Officer or National IT Manager before removing devices from organisation premises.

5.1.4 Refrain from sharing private passwords with co-workers, personal acquaintances, senior personnel, and/or other stakeholders.

5.2 When new staff receive organisation-issued equipment they will be issued instructions for:

- system access
- password management

- software updating requirements.

They are obliged to follow these instructions to protect their devices. The IT team will be available to assist.

Personal Device Use

5.3 MC recognises that staff/volunteers may be required to use personal devices to access MC's systems. In these cases, users must report this information to management for record-keeping purposes.

5.4 To ensure MC's systems are protected, all users are required to:

5.4.1 keep all devices password-protected

5.4.2 ensure all personal devices used to access organisation-related systems are password protected

5.4.3 install full-featured antivirus software

5.4.4 regularly upgrade antivirus software

5.4.5 lock all devices if left unattended

5.4.6 ensure all devices are protected at all times

5.4.7 always use secure and private networks

5.4.8 not store organisational data on personal devices.

Email Security

5.5 MC requires all users to:

5.5.1 Verify the legitimacy of each email, including the email address and sender name.

5.5.2 Avoid opening suspicious emails, attachments, and clicking on links.

5.5.3 Look for inconsistencies or give-aways (e.g. any significant grammatical errors, capital letters, excessive number of exclamation marks.)

5.5.4 Avoid clickbait titles and links (e.g. offering prizes, advice).

5.5.5 Contact the IT department regarding any suspicious emails.

Manage Passwords Securely

5.6 Passwords should be secure, so they won't be easily hacked, and remain secret.

5.7 Users are required to:

5.7.1 choose secure passwords (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays)

5.7.2 either remember passwords or store the paper or digital record securely, keeping them confidential. Destroy the record when the work is done.

5.7.3 all system-level passwords (e.g. Root, enable, application administration accounts, and so on) must be changed on a quarterly basis.

5.7.4 all user-level passwords (e.g. email, web, desktop computer, etc.) must be changed at least every six month.

Report Security Breaches Immediately

5.8 Immediately alert the IT team of any breaches, malicious software, and/or scams.

5.9 This includes perceived attacks, suspicious emails, or phishing attempts. Our IT team must investigate promptly, resolve the issue, and send an alert to all relevant users if necessary.

Remote Access

5.10 Remote users must comply with this policy. Since they will be accessing our organisation's accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

5.11 Seek advice from our IT team to assist ensuring a safe set-up.

Data Backup

5.12 Backups help protect MC from loss of information and damage to its reputation by protecting against phishing, ransomware, etc, and insider threats.

5.13 Our IT team manages the backups for all MC servers and cloudbased data (e.g. Google Drives and emails). All organisation-related data is to be stored using these systems.

Disposal

5.14 In order to protect our organisation's data, all storage mediums (including USB drives) must be properly erased before disposal, and physical records disposed of appropriately.

5.14.1 Some methods of disposal to ensure that the information cannot be practicably read or reconstructed include:

5.14.2 burning, pulverizing, or shredding of papers containing confidential information

5.14.3 a procedure to ensure the destruction or erasure of electronic media

5.14.4 sending out for proper disposal those technology assets that have reached the end of their useful life

5.14.5 removing all data from equipment using disk sanitizing software that cleans the media overwriting every disk sector with zero-filled blocks.

Disciplinary Action

5.15 Violation of this policy can lead to disciplinary action, up to and including termination.

5.16 MC's disciplinary protocols are based on the severity of the violation.

5.17 Unintentional violations may only warrant a verbal warning, frequent violations of the same nature may lead to a written warning, and intentional violations may lead to suspension and/or termination, depending on the case circumstances.

Review and Respond

Periodic Cyber Security Assessments

5.18 MC will conduct periodic assessments (at least annually) to detect potential system vulnerabilities and to ensure that cyber security procedures and systems are effective in protecting confidential information.

Response to Cyber Security Incidents

5.19 MC will respond to data breaches depending on the type and severity of the incident. In doing so the organisation will:

5.19.1 Contain and mitigate the incident/ breach to prevent further damage

5.19.2 Evaluate incident and understand potential impact

5.19.3 Implement a disaster recovery plan (if needed)

5.19.4 Determine if personal information was compromised and notify affected persons of the date the organisation becomes aware of this breach.

5.19.5 Enhance systems and procedures to help prevent the recurrence of a similar breach

5.19.6 Evaluate response efforts to the update response plan to address any shortcomings.

6. RELATED DOCUMENTS AND LEGISLATION

- ICT Disaster Recovery and Business Continuity Plan
- Privacy Policy
- Staff Code

7. REFERENCES

Nil

8. VERSION HISTORY

Version	Approved by	Approval Date	Effective Date	Changes made
X.XX	MC Board	19 February 2024	13 February 2024	Updated contacts and minor edits. Transferred into an updated document template.
2.00	MC Board	20 February 2023	23 January 2023	Streamlining
1.00	MC Board	7 October 2020	7 October 2020	New policy

Download this policy anew with each use, as it may have changed.