1.15

MERCY EDUCATION POLICY

1.15 CYBERSECURITY

Introduction

Mercy Education Ltd (Mercy Education) is committed to protecting its people, assets and recognises the importance of protecting the organisation's sensitive data, intellectual property and Information Technology (IT) infrastructure from cyber incidents and threats.

Mercy Education strives to develop and embed a culture of cyber(?) security awareness across all aspects of its governance and operations.

Purpose

This Policy outlines the responsibilities of all authorised users of Mercy Education networks and systems and provides guidance for the management of cybersecurity risk for Mercy Education and its schools

Definitions

Board: the Board of Mercy Education Limited

Cyber-attack: an attempt by hackers to damage or destroy a computer network or system

Cybersecurity: the state of being protected against the criminal or unauthorised use of electronic data, or the measures taken to achieve this

Cyber threat: the possibility of a malicious attempt to damage or disrupt a computer network or system.

Clergy: any cleric, member of religious institute or other persons who are employed or engaged by a Church body, or appointed by a Church body to voluntary positions, in which they work with or are near children or young people or are engaged in other forms of pastoral care or chaplaincy.

Mercy Education Limited
ABN 69 154 531 870
PO BOX 5091
ALPHINGTON VIC 3078

NB: Whilst specifically the definition of the word 'clergy' is for ordained persons who are religious leaders serving the needs of their religion and its members, for the purpose of this document, it includes other professed religious personnel providing pastoral care or chaplaincy services.

Director: a person who is a director for the time being of the Mercy Education Ltd Board

Employee: an individual working in a school environment or school boarding environment who is:

- Directly engaged or employed by a school governing authority
- Contracted service provider (whether a body corporate or any other person is an intermediary) engaged by the school governing authority to perform child-related work; or
- A minister or religion, a religious leader or an employee or officer of a religious body associated with the school

Information Communication Technology (ICT/IT): all hardware devices (laptops, workstations, mobile phones, associated portable devices, interactive whiteboards, etc.), networking services, and all software resources (applications, databases) locally or remotely accessible made available and administrated by Mercy Education and its schools

Mercy Colleges/Schools: any of the 13 schools governed by Mercy Education.

School environment: any of the following physical, online, or virtual places, used during or outside school hours:

a) A campus of the school
b) Online or virtual school environments made available or authorised by the school governing authority for use by a child or student (including email, intranet systems, software applications, collaboration tools, and online services); and
c) Other locations provided by the school or through a third-party provider for a child or student to use including, but not limited to, locations used for:
   (i) camps
   (ii) approved homestay accommodation
   (iii) delivery of education and training such as registered training organisations, TAFEs, non-school senior secondary providers, or another school; or
   (iv) sporting events, excursions, competitions, or other events.

Student: means a person who is enrolled at or attends the school or a student at the school boarding premises. This may include a young person over the age of 18 years

Volunteer: an individual (including College Advisory Council Members) who is engaged by Mercy Education or its schools and performs work without renumeration or reward for the school environment or school boarding environment.

What about Director definition?

Policy Coverage

All authorised users who may include Board Directors, employees, students, volunteers, clergy, third parties, suppliers, contractors who have access to Mercy Education's ICT systems, networks, and data

Policy Statement

Mercy Education is committed to the protection and safety of all employees, students, volunteers, and the wider school community and to the security of handling and storing all data including personal and sensitive information in both the short and long term.

Mercy Education believes that Cybersecurity is an individual and collective responsibility for all authorised users of Mercy Education networks and systems.

The Mercy Education Board will ensure that:

01 Mercy Education's and each school's policies and procedures are consistent with applicable national, state and territory laws and policies and that online incidents are reported as part of the overall legal and policy framework of Mercy Education and its schools

02 the Board Risk and Compliance Committee (RISKCOM) oversees the risk management for cybersecurity to ensure that controls are in place to protect the National Office and its schools, employees, and communities

03 the Mercy Education Code of Conduct for Employees and Volunteers provides guidance on the appropriate use of digital devices, online platforms and social media for school purposes or provides procedures to inform and educate the school community

Mercy Education and its schools must:

04 develop and implement risk mitigation procedures to protect against cyber threats

05 implement minimum standard requirements to protect all electronic information, infrastructure and services from theft, unauthorised access, use, disclosure, modification or destruction during the information lifecycle

06 require all authorised users to acknowledge and agree to protocols regarding acceptable use of networks, hardware and software

07 ensure that all authorised users must only use the ICT resources to which they have been granted access or rights

08 ensure that all authorised users of Mercy Education and school networks have secure password (or passphrase) access or multi-factor authentication, including direction on creation of strong and unique passwords / passphrases, appropriate storage and capacity procedures and processes for update of hardware and software

09 maintain a level of cybersecurity which ensures the confidentiality, integrity and availability of digital services for authorised users

10 ensure that all individuals prevent the unauthorised disclosure of data via unauthorised access to information on an unattended workstation or device

11 ensure that all authorised users (where relevant) receive relevant training in cybersecurity and privacy, on induction, annually and when otherwise required, according to their role

12 develop and maintain email security protocols including but not limited to:
- when it is appropriate to share a work/school email address
- opening email attachments from trusted contacts and unknown senders

- blocking junk, spam and fraudulent emails
- identifying, deleting and reporting suspicious emails

13 Applying and maintaining security controls on (but not limited to):
- firewall (including whitelisting)
- blocking of websites
- blocking of application installations
- anti-virus software
- automated spam and phishing detection
- password strength
- multi-factor authentication
- identification and management of technical vulnerabilities
- awareness information
- monitoring of logs

14 work with employees, students and the wider community to regularly identify emerging online safety issues and evaluate against current policies and procedures

15 include clear incident response pathways and processes so that authorised users can respond confidently to inappropriate behaviour or security breaches

Related Documents:

Australian Signals Directorate
- *https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight*

Mercy Education Ltd (MEL)
- *Mercy Education Limited Governance Statement*
- *1.05 Records Management*
- *1.07 Policy: Privacy*
- *6.09 Child Safety*
- *10.08 Operational Instructions – Data Breach Response Plan*

Review History:

Version	Date Released	Next Review	Author	Approved
1.0	May 2023	March 2024	Head of People & Culture	MEL Board
1.1	May 2024	March 2025	Head of People & Culture	MEL Board