THE HUTCHINS SCHOOL

Cyber Security Policy

Relevant legislation	Australian Communications and Media Authority (ACMA) Spam Act 2003 (Cth) Electronic Transactions Act 1999 (Cth) Personal Information Protection Act 2004 (Tas) Privacy Act 1988 (Cth) Telecommunications (Interception and Access) Act 1979 (Cth)
Commencement date	01 March 2024
Last review date	01 March 2024

1. Purpose

The purpose of this policy is to outline the Hutchins School's commitment to providing a secure Information Security Management System (ISMS). The ISMS is designed to mitigate risk and protect sensitive and personal information in accordance with the Privacy Act.

The key components of the School's ISMS are:

- the Cyber Security Framework;
- the Cyber Security Policy; and
- supporting policies, procedures and systems.

The Cyber Security Policy is reviewed and ratified on a two year cycle by the School Board, the Principal and the Chief Operating Officer.

2. Scope

This policy applies to all software, hardware, systems, processes and data within the School's Information Security Management System (ISMS), and to all users (including employees, volunteers, contractors and third-party service providers) who have access to the School's information technology assets.

3. Objectives

The primary objective of this policy is to:

- establish an Information Security Management System (ISMS) at the School that is compliant with ISO 27001;

- provide structure and process to ensure that information is classified, managed and made accessible in a manner consistent with its sensitivity and required confidentiality level;
- establish the need to maintain an inventory of all information assets, and regularly assess them using for vulnerabilities and risk exposure;
- implement physical security measures to protect information assets;
- establish procedures (under the Cyber Security Framework) to govern, protect, manage and respond to risks that threaten information security at the School;
- establish business continuity plans that ensure that critical information assets are protected and essential business operations can continue with as little impact upon the School and its students as possible;
- comply with all applicable state and federal laws, regulations and standards relating to information security; and
- establish a body of protocols and systems designed to ensure that all employees, contractors and third-party service providers are aware of their obligation toward ensuring the security of the School's assets.

4. Definitions

Assets	In the context of this policy, 'assets' (msot often 'information assets') refers to any and all software, hardware, systems, processes and data owned, controlled, maintained or otherwise used by the School.
Information Technology (IT)	'The science and activity of using computers and other electronic equipment to store and send information (Cambridge University Press. Information Technology. In Cambridge Dictionary. https://dictionary.cambridge.org/dictionary/english/information-technology)
ISMS	Information Security Management System. This term refers to the entire suite of policies and procedures that support the security of systems and data at the School. The School's ISMS is known as the 'Cyber Security Framework', which this policy sits within.

5. Policy statement

The School recognises the importance of maintaining the confidentiality, privacy, integrity and availability of its information technology assets. This policy outlines the measures and controls that the School has in place to govern and protect those assets and to detect and respond to threats to their security.

The Cyber Security Framework

The School's ISMS (known as the 'Cyber Security Framework') is based upon and compliant with ISO 27001. The framework consists of:

- The Cyber Security Policy (this policy);
- Cyber Security Management Systems;
- Complementary policies and procedures:
    - Email Policy
    - Privacy Policy
    - Social Media Policy
    - Records Management Policy
    - Working from Home Guidelines – supported by:
        - Working from Home Checklist
        - Working from Home Request Form
- Supporting agreements:
    - Co-operating Schools Data Sharing Agreements:
        - St Michael's Collegiate
        - The Fahan School
    - Student ICT Agreements:
        - Junior ICT Agreement
        - Senior ICT Agreement

Cyber Security Management Systems

The School has in place a number of systems that are designed to limit and regulate external access and monitor potential threats across networked resources. These systems work together to produce a level of security that is assessed through a series of tests and regular audits.

These systems likewise limit the ICT ecosystem available within the School, which allows the ICT Team to regulate the range of services used by staff and ensure that applications support the integrity and security of data assets across the School and limit exposure to risk.

The School's ICT Team administer annual audits of these systems (and many other sub-systems) in order to support best-practice across the board. Knowledge Base (KB) information is made available to staff in order to support safe systems management and access.

Roles, responsibilities and accountabilities

Users

End-users are responsible for reporting any potential cyber security incidents or breaches to IT support. This includes the loss or compromise of devices.
All staff, volunteers and contractors are responsible for:

- participating in training provided by the School as required;
- incorporating safe online and cyber security practices into their work;
- managing their documents in accordance with the Records Management Policy;

- operating in a manner that respects the Privacy Policy, safeguarding private, confidential and sensitive information; and
- complying with any additional policies and procedures that are intended to protect information security assets.

IT Management and Staff

IT managers are responsible for managing cyber security risks across the school, and are accountable for compliance with ISO27001 and this policy. They are also responsible for:

- ensuring that key information security assets are managed via the Cyber Security Management Systems;
- supporting compliance across the School with relevant IT policies and procedures, cyber security standards and local operating procedures;
- monitoring IT systems and services for potential cyber security risks and threats.

IT Managers are expected to be both proactive and responsive toward emerging threats or concerns regarding cyber security, and are responsible for ensuring that systems are in place to detect, mitigate and respond to the risks that such threats present.

Chief Operating Officer

The Chief Operating Officer is responsible for:

- promoting the importance of cyber security risk management to School staff and leadership;
- communicating with the School Board and its subcommittees regarding cyber security threats, risks, detections and mitigations; and
- providing adequate resourcing for the management of cyber security risk across the School.

The Principal

The Principal is responsible for:

- promoting the importance of cyber security risk management among School staff and leadership;
- engaging with the School Board and its subcommittees to consider cyber security threats, risks, detections and mitigations; and
- ensuring that School staff are provided with training opportunities to upskill in respect to cyber security.

Payroll, Human Resources, Safety & Risk and the Enrolments Office

Payroll, Human Resources, Safety & Risk and the Enrolments Office have the greatest access to staff and student data across the School. As a result, staff in these areas must consider cyber security more carefully than the average end-user. In addition to the requirements listed under ‘Users’, staff working in these areas are required to:

- be mindful of cyber security risks and take steps to mitigate them within the scope of their work;

- report any data breaches or concerns in respect to data security to the Chief Operating Officer as soon as practicable; and
- take steps to ensure that their higher level of access to School data is not shared or left vulnerable on their devices.

Reporting cyber security breaches

Under the Privacy Act 1988 (Cth), the School must report to the Australian Information Commissioner breaches of private data that is likely to cause serious harm unless remediation occurs. Staff, volunteers and contractors are required to report any potential or confirmed data breaches as soon as possible to the Chief Operating Officer.

6. Supporting/related documents

Internal documentation

Policies and procedures:

- Email Policy
- Privacy Policy
- Social Media Policy
- Records Management Policy
- Working from Home Guidelines – supported by:
  - Working from Home Checklist
  - Working from Home Request Form

Supporting agreements:

- Co-operating Schools Data Sharing Agreements:
  - St Michael's Collegiate
  - The Fahan School
- Student ICT Agreements:
  - Junior ICT Agreement
  - Senior ICT Agreement

External documentation and legislation

- ISO 27001 standard

- Privacy Act 1988 (Cth)
- Australian Cyber Security Centre (ACSC) Essential Eight
- Australian Privacy Principles (APPs)
- Australian Signals Directorate (ASD) Information Security Manual (ISM)
- Notifiable Data Breaches (NDB) scheme
- Australian Communications and Media Authority (ACMA) Spam Act 2003 (Cth)
- Electronic Transactions Act 1999 (Cth)
- Telecommunications (Interception and Access) Act 1979 (Cth)

7. Record keeping

This policy is to be kept for two (2) years until review, unless there is a significant legislative or organisational change requiring earlier review.

The master copy is kept in SharePoint Online in read-only in PDF form. All printed copies are uncontrolled.

8. Policy owner

The Principal.

9. Version Control

Version Number	Author	Purpose/Change	Date
1.0	Policy & Compliance Manager	Initial release	03/2024