THE HUTCHINS SCHOOL

Digital information and communications policy

Relevant legislation	Copyright Act 1968 (Cth) Criminal Code Act 1995 (Cth) Electronic Transactions Act 1999 (Cth) Privacy Act 1988 (Cth) Spam Act 2003 (Cth)
Commencement date	01 August 2014
Last review date	01 August 2023

1. Purpose

This policy outlines the principles and guidelines for the appropriate use of the School's network, apps, services and communication systems. It aims to ensure that staff, students, and School community members use digital resources responsibly, ethically, and securely, in a manner that aligns with the School's values of humiliity, kindness, courage and respect, and protects the integrity of the School's operations.

The policy provides a framework for safeguarding privacy, maintaining security, and upholding high standards of professionalism in all digital communications and transactions within the School environment.

2. Scope

This policy applies to staff, students and School community members who are provided with access to apps, services and/or the School network. It scaffolds expectations for the use of the network, apps and services, outlines expectations for all electronic communications and regulates access to digital information created within, transferred to, transmitted by or stored in the School's systems and infrastructure.

3. Objectives

The objective of this policy is to inform employees, students and community members with access to Hutchins accounts and resources of the School's standards and expectations for digital information and communications and to provide structure and regulation around School access to records generated by staff members, students and community members, whether past or present.

4. Definitions

Digital information	Documentation in digital form, whether created directly in electronic apps and services, or converted from physical formats. This includes all electronic communications, as defined below, and all information generated via electronic apps and services.
Electronic apps and services	Includes all digital tools and platforms provided by the School to facilitate educational, administrative, and communicative functions. These encompass (but are not limited to): • productivity tools (e.g., Microsoft Office 365); • communication apps (e.g., email services, instant messaging services, video conferencing tools, such as Microsoft Teams, Zoom, Slack, Google Meet); • learning management systems (e.g., Synergetic, EduPlanet21); • data storage and sharing platforms (e.g., SharePoint, OneDrive); and • any other software, mobile applications, or online services utilsed in School operations.
Electronic communications	Communication through digital or online systems, including (but not limited to) email, messages, documents, files, or any other electronic media.
ELMO	ELMO is a cloud-based Human Resources (HR) and payroll software platform used to manage various HR functions, including recruitment, onboarding, performance management, learning and development, payroll processing, and compliance tracking. It provides an integrated system to streamline HR operations, improve workforce engagement, and ensure compliance with organisational policies and regulatory requirements.
Electronic mail (email)	Messages distributed by electronic means from one computer user to one or more recipients via a network.
School network	All hardware, software and services provided or managed by the School in respect to ICT.
The Hutchins School community	The Hutchins School community (or 'The School community') refers to parents, carers, alumni, associations (including, but not limited to, the Hutchins School Old Boys' Association and the Parents' Association), governing bodies (such as The Hutchins School Board), volunteers, contractors and sub-contractors of the School.

5. Policy statement

Access to the School network is provided primarily to conduct school business and to complement and facilitate the studies of students. Staff, students and members of the School community using the School's network generate digital information that is subject to the policy body of the School, primarily the Code of Conduct, Privacy Policy, Social Media Policy and Commitment to Kindness. The School encourages the productive, legal and ethical use of electonic apps and services in accordance with the terms outlined in these documents.

The School recognises that inappropriate or excessive use of electronic apps and services may jeopardise its operations and expose the School to unnecessary risk. Their use is subject to laws relating to copyright, freedom of information, confidentiality, privacy and anti-discrimination. All users of the School's network and services are expected to maintain high standards of professionalism in their communications and in their app and service use in line with the School's values of humility, kindness, courage and respect.

Network, app and service provision

Staff and students at the School are provided with access to the School's network. Community members may be provided with network access at the School's discretion.

Students are provided with an email account and access to School-approved apps and services for the duration of their education. This access is subject to the Student ICT Agreement, which students and their parents/carers must read, sign and return on an annual basis.

Staff at the School are provided with an email account with access to School-approved apps and services for the duration of their employment. This access is subject to the Staff ICT Agreement, which staff are required to read, sign and return on an annual basis (via ELMO).

Community members may be provided with an email account and/or accounts for apps and services at the discretion of the School. Such users will be provided with a copy of or link to this policy and are expected to adhere to the requirements and obligations laid out within it.

Electronic communications

Electronic communicaions are an inherently vulnerable method of communication, and should not be considered private. All communication by staff, students, and community members using School resources (whether that communication is internal or external) must be in keeping with The Code of Conduct, Privacy Policy and Commitment to Kindness, and must reflect the School values of humility, kindness, courage and respect.

Users must not transmit (via any electronic means) material that could be considered:

- discriminatory (e.g., on the basis of age, race, gender, religion, etc.);
- offensive (harassing, bullying, defamatory, sexually explicit, obscene or pornographic);
- contrary to the values of the School;
- promoting violence or threats;
- 'spam'; or
- forged or disguised identies.

The School values privacy and confidentiality. Users must ensure that their electrionic communications:

- are not forwarded or copied without careful consideration or the original author's permission;
- carefully consider the need to send sensitive or copyrighted material;

- are sent and received only by the account owner (except where authorisation has been given; e.g., the Principal's Executive Assistant may send and receive electronic communications on behalf of the Principal); and
- are appropriate for the individual, audience, group, mailing or distribution lists or teams to which they are sent.

While using School-provided networks, users may also not:

- send electronic communications to any media organisation, journalist or person associated with the media or public relations organisations without the express consent of the Principal (or delegate);
- use electronic communications for advertising or other commercial use that is not associated with the School; or
- forward (without authorisation) branded material or photographs of:
  - school events;
  - students;
  - members of the School community at school or in social situations; or
  - the School grounds, or any part of the School; or
  - any other media that could be misused.

Generative AI Usage

The School acknowledges the potential benefits of Generative AI (GenAI) tools for enhancing learning and operational efficiency while emphasizing the importance of ethical, fair, and compliant use. In accordance with the School's Generative AI Policy, staff and students must ensure that personal, sensitive, or confidential information is never shared with an AI tool unless explicitly approved by the School's ICT team.

GenAI tools are considered unregulated third parties unless designated otherwise, and their use must align with privacy, data security, and academic integrity protocols. Staff are required to critically evaluate AI-generated content and maintain accountability for decision-making. Any breach involving personal or identifiable sensitive data must be reported immediately to the School's privacy officer. For further guidance, refer to the full Generative AI Policy.

Email provision and retention

The School's email service provider retains copies of email sent and received through the server. Even where the user has deleted an email, or where the user has left the employment of the School, access is retained.

The School will discontinue user access to an email account when a staff member's employment ceases with the School or when a student is no longer enrolled at the School. An email account may be kept active for a period of time following the departure of an email account user at the School's discretion.

Non-staff and non-student email accounts will have access withdrawn when the individual is no longer affiliated with the School. All email accounts managed by the School are retained by Microsoft after their access is withdrawn from the user and are managed according to the Records Management Policy.

Appropriate presentation of email

Staff are required to ensure that their email presentation is professional at all times. Email stationery is not permitted, while signatures are automatically applied when an email account is created and must not be user-defined. This ensures a professional appearance that is consistent within the School's Brand Style Guide.

Staff should sign off email with an appropriate salutation such as 'Kind regards' or 'Yours sincerely' to ensure professionalism and consistency with the School's Commitment to Kindness.

Reasonable personal use of electronic apps and services

The School's network, apps and services are provided primarily for education, research and work purposes; however, a reasonable amount of personal use is considered acceptable. When considering reasonable personal use, the use of school resources must:

- adhere to this policy and its supporting guidelines;
- not interfere with work; and
- not involve the forwarding of any content that may otherwise breach the requirements and expectations of this policy.

If at any time a Hutchins email account user is not clear or has concerns about what may be considered personal use, he/she should discuss the matter with their supervisor or the ICT Team.

- Users should consider that digital information sent or received via the School's networks is retained and will remain accessible to the School (or to law enforcement) even after they have ceased their association with the School. This may include information generated by personal use.

The School may (under specific conditions, see 'Privacy and confidentiality of digital information') access, review or take action upon any and all digital information created, sent or received by users during the course of their employment or engagement with the School.

Privacy and security of electronic communications

The School is committed to maintaining the security of digital information across the School network - whether those communications are of a business, educational or personal nature – to the highest possible standard. Some electronic communications platforms are neither secure nor encrypted, and should not be considered private. Users are therefore encouraged to:

- avoid sending personal, commercial, educational or reporting information via email;
- avoid sending messages to open groups or using distribution lists where users' email addresses may become public;

- avoid opening sensationalist content or email;
- verify the authenticity of sensitive email where required (seeking ICT support if needed);
- maintain the security of their own account usernames and passwords; and
- use alternative, secure methods (e.g., sharing a document via OneDrive or SharePoint) to transfer private, sensitive or confidential data.

Many online services used by staff and the School community are secured behind Multi-Factor Authentication (MFA), which is specifically designed to hinder adversarial access to Hutchins accounts. Multi-Factor Authentication requires all Hutchins staff and community members to verify their accounts periodically using the Microsoft Authenticator app on their phones. MFA is not enabled for students.

As part of its commitment to securing digital records, the School provides storage and transmission through SharePoint, OneDrive and Rory (Schoolbox). If you are unsure of the most appropriate mechanism to use, or require further support, please contact the ICT Service Desk or email service.desk@hutchins.tas.edu.au.

The School will never ask you to disclose usernames and/or passwords for any online services via email. If you have doubt about the veracity or authenticity of an email, please contact the ICT Service Desk.

Privacy and confidentiality of digital information

The School reserves the right to monitor, review, access and take action upon the basis of any digital information created, sent or received by users of its networks, systems and resources. With that said, the School is committed to privacy and confidentiality, and as a general rule, does not wish to be the arbiter of users' electronic communications nor supervising their digital information. As a result, the School will only permit searches for or the disclosure of digital information generated by a user *without consent* where:

- disclosure is requested by Tasmania police, or warranted or required by law;
- reasonable suspicion exists that a member of staff or a student has breached a policy or procedure;
- the information requested is required for school-related business, and is to be provided either to a staff member internally or to an external source with appropriate authority to receive it (e.g. Tasmania Police);
- access to the information is required for business operations (for example, retrieval of a School document or information from a specific point in time that cannot be accessed by other means);
- a staff member is no longer employed by the School but access to digital information, documentation or electronic communication(s) generated, sent or received while in the employment of the School is required for school-related business; or
- in exceptional cases, and to meet time-dependent critical operations needs, reasonable attempts at obtaining consent have failed.

All other requests for access to electronic communications must be approved by either the Principal, Chief Operating Officer or their delegate according to the protocol below.

Protocol for accessing digital information

Where the School becomes aware of a potential breach of a policy or law, or where a legal request is made for digital information about, generated, sent or received by a member of School staff (whether past or present), an investigation will be instigated.

Due to the nature of digital information, this investigation may require access to a user's records and data, and may produce digital information related to other users (e.g., an email sent to the user under investigation by another member of staff or an external party). Due to the added sensitivity around such requests, the following protocols will be followed:

1. The person who becomes aware of a potential breach (often Human Resources or the employee's supervisor) will consult with the Principal or Chief Operating Officer.
2. Where warranted, the Principal and/or the Chief Operating Officer will confer to determine the appropriateness and necessity of accessing the user's electronic communications.
3. Where the Principal or Chief Operating Officer determine that it is appropriate and necessary to access a user's electronic communications, they will inform the Head of Information and Communications Technology (ICT) or ICT Infrastructure Manager, who will facilitate the appropriate search and access.

Non-compliance with this policy

Serious or continued breaches of this policy may be subject to disciplinary action, including dismissal. In the first instance the matter may be taken up by a staff member's manager or supervisor. If required, the matter may be referred to the Principal or Chief Operating Officer for action.

Student breaches will be addressed by their Head of School, who may refer to other staff members in consultation with the Head of Information and Communications Technology (ICT) or the ICT Infrastructure Manager.

Training and support

The School is committed to providing staff and students with assistance to ensure that this policy is successfully implemented. Assistance may include (but is not limited to) the development of this Email Policy and supporting guidelines, access to ICT training and access to ICT support.

Should a staff member feel they need further ICT training, a request can be made following established Staff Training and Professional Learning Procedures.

6. Supporting/related documents

Commitment to Kindness

Complaints and Grievances Policy

Harassment, Bullying and Discrimination Policy

Privacy Policy

Safeguarding Children & Young People Policy

Social Media Policy

Practice and Behaviour Standards

The Hutchins School Code of Conduct

7. Record keeping

This policy is to be kept for three (3) years until review except where legislative or organisational change demands otherwise. The master copy is kept in SharePoint Online in read-only PDF form. All printed copies are uncontrolled.

8. Policy owner

Principal

9. Version Control

Version Number	Author	Purpose/Change	Date
2.0	Policy & Compliance Manager	Full review and update; complete rewrite from 2018 version.	1/7/2020
2.1	Policy & Compliance Manager	Minor amendments only.	27/10/2020
2.2	Policy & Compliance Manager	Full textual review; text simplified in numerous locations. Change to 'Principal' rather than the outdated 'Principal'.	01/07/2023
3.0	Policy & Compliance Manager	Policy broadened to include all electronic communications – renamed from 'Email Policy' to 'Digital Information and Communications Policy'. Significant textual review and rewrite. Inclusion of new definitions to support the expanded scope of the policy.	03/2025