POLICY
Cyber Security

NT CHRISTIAN SCHOOLS

DOCUMENT INFORMATION

Document Title:	Cyber Security Policy
Policy Category:	IT - Information Technology Management
Policy Monitor:	IT Manager
Contact:	policy@ntchristianschools.com.au
Approved by:	Board
Approval date:	29 March 2026
Review date:	November 2027
Access Level:	Public

Policy Feedback

AMENDMENT HISTORY

Version	Date	Changes Made
1.0	03/2026	Developed to support operations, risk management and compliance. Supersedes Password Security Policy, with terms included in this policy. Board approved via circular resolution 29/3/26.

1 Preamble

NT Christian Schools is an organisation that exists to advance the Christian religion through the provision of high-quality education and training services and religious instruction. A holistic and relational approach to learning for each individual student, underpinned by a biblical world view provides an education for the whole person, for the whole of life.

We believe that the Christian faith is a life-transforming faith that will be authentically evidenced in a believer's actions. The bible exhorts us to pursue godliness and to model biblical standards of behaviour. Everything we do, our practices, our conduct, our use and stewardship of resources is an act of worship to God and a witness to those around us.

All members of the NT Christian Schools community are to be committed to ensuring a safe and caring environment for students, staff and the whole community in a manner that is consistent with the Christian ethos and beliefs of NT Christian Schools.

Employees and those a policy applies to are fully supported by NT Christian Schools to meet compliance with this policy.

NT Christian Schools is committed to achieving and maintaining workable solutions for our organisation.

We may make changes to this policy from time to time to improve the effectiveness of organisational operation or to meet legislative requirements. Notification of changes will be communicated to those a policy applies to, and it is their responsibility to read updated policies and relevant related documents as soon as reasonably practical. Any NT Christian Schools stakeholder who wishes to provide feedback about this policy may forward their suggestions to the policy monitor or policy@ntchristianschools.com.au.

2 Purpose

This policy articulates NT Christian Schools' foundation for the management and implementation of robust cyber security measures, effective incident response and continuous improvement processes. This aims to protect electronic information, sensitive data, infrastructure and services from theft, unauthorised access or use, disclosure, modification or destruction.

This policy along with the Information Communication and Technology (ICT) policy suite, Privacy Protection Policy, Record Management Policy and Risk Management Policy articulate NT Christian Schools' information governance to meet operational, statutory, legal, audit and moral obligations.

3 Policy applies to

This applies to all users of Information and Communication Technology (ICT) including employees, contractors, consultants, volunteers, students, and other users.

The policy is available to all parents, carers, students, staff, volunteers, and contractors via the NT Christian Schools website and on request in hard copy from the NT Christian Schools Business Services Office as required.

The policy is available to all staff and Board of Directors via the NT Christian Schools Canvas *Policy and Advisory Library*.

4 Policy

4.1 Guiding Principles

All members of NT Christian Schools' community are called to show good character and to act ethically, using their skills for good[1], protecting the vulnerable and showing love and respect to others[2].

As an organisation we must take reasonable action to protect people, prevent harm, steward our resources well and be actively vigilant against our adversaries[3].

It is the responsibility of all users of NT Christian Schools ICT to work together to protect and secure the information held by NT Christian Schools and the ICT infrastructure.

NT Christian Schools endeavours to be an organisation supported by digital solutions that are safe, uphold confidentiality, privacy and integrity, protect against unauthorised access, enable compliance, efficient business operations, and support student development and educational outcomes.

4.2 General Requirements

Operational Directors, ICT Manager, Principals and Line Managers are responsible for implementing the policy.

All users must be aware of and adhere to the control requirements defined in the Cyber Security Policy, Acceptable Use Policy and agreements. By using ICT facilities controlled by NT Christian Schools' or its associated entities, the user is accepting this and other ICT policies and procedures.

All users granted access to NT Christian Schools' ICT systems, infrastructure and services must adhere to instruction, protocols and user agreements as communicated by NT Christian Schools and are accountable for all actions and functions performed on their accounts.

All users are to be educated on the responsible use of technology, the importance of digital wellbeing, and how to engage with technology respectfully to protect themselves, others and the resources.

All users should use private email services for conducting personal business rather than email facilities provided by NT Christian Schools as all data and communication on NT Christian Schools' provided services remains the property of NT Christian Schools, and for NT Schools accounts, the Department of Education and Training (DET).

NT Christian Schools believes staff have a right to a safe and non-intrusive work environment and will not undertake unreasonable or excessive monitoring of work or communications, beyond what is necessary to meet statutory, compliance or duty of care requirements and to safeguard collected data.

Only use NT Christian Schools' ICT technologies and resources which you have been granted access privileges to and be vigilant in securing all ICT equipment that has been entrusted to you and the information contained therein.

Take all reasonable action to prevent unauthorised disclosure of data.

---

[1] 1 Peter 4:10, Colossians 3:23
[2] Mark 12:31
[3] 1 Peter 5:8

Take all reasonable action to prevent unauthorised access to information on an inactive workstation.

Any suspicion of or known security threats or breaches must be reported:

- Students report to your teacher or Head of School.
- Employees report to your Line Manager or the ICT team.
- Volunteers and contractors report to your coordinator, supervisor, or campus Principal.

Only use NT Christian Schools' and NT Department of Education and Training ICT resources for:

- Work/business and educational purposes,
- Personal use when it is not for commercial gain or in any way counterproductive to the business or policy of NT Christian Schools.

4.3 Security Governance Risk and Compliance

Information security threats and risks to NT Christian Schools' assets must be identified, assessed, appropriately responded to, and monitored through formalised and organisation wide security risk management procedures.

Exemptions requests must be documented, reviewed by appropriate management, and accepted by the accountable organisation manager.

Compliance with policies relevant to information management and cyber security must be measured and monitored to ensure effective implementation and maintenance.

The ICT Manager and ICT Team, operational Directors, Principals, and Line Managers are responsible for conducting audits and reviews at planned intervals to assess and inform data, information, and system security.

NT Christian Schools' must comply with all applicable federal and Northern Territory regulatory requirements. Applicable regulatory and compliance requirements related to cyber security and data protection must be identified, and processes established to ensure requirements are understood and met by all stakeholders.

4.4 Information Classification, Handling and Protection

Inventory or asset registers must be maintained and updated as required on an ongoing basis and retained as per the Asset Management Policy, Record Management Policy, and Record Retention Framework.

All NT Christian Schools information assets and data must be classified, labelled (where applicable), and handled and retained in accordance with NT Christian Schools' Records Management Policy, Record Retention Framework, and Privacy Protection Policy.

A robust data backup and recovery process must be in place for all critical systems to support the integrity and availability of critical information assets.

Processes for disposal of data that is no longer required must be in accordance with the Record Management Policy.

4.5 Identity and Access Management

Access to NT Christian Schools information systems and assets must be securely established and managed.

User access requests (for example system access requests, requests to update access privileges, or requests to revoke user access rights) must be assessed and approved in accordance with defined user access management procedures.

User access must be authenticated, authorised, terminated, and reviewed periodically. User identities (physical and digital), passwords, tokens, tags, and account privileges must be managed to ensure sound authentication, registration, segregation of duties, privileges allocation, and termination of user access where appropriate.

Privileged access rights must be authorised according to the principle of 'least privileged' and authenticated via multi-factor authentication (i.e. smart card, soft token, or PIN). Privileged access is to be reviewed at least biannually, with immediate remediation (for example immediate access revocation) as required.

Processes for acquiring and disposing of assets must be in accordance with the Asset Management Policy.

4.6 Password Security

Password security is a key means for maintaining proper security of information; therefore, password security is to be as strong as practical and commensurate with the information being protected.

It is the responsibility of all users to maintain passwords.

Two-factor authentication or other enhanced security measures are to be available and used to protect sensitive information.

Passwords are to:

- Follow principles established for the relevant entity or information management software,
- Updated regularly,
- Not forwarded to others by email,
- Not disclosed to anybody. Provisions are made for obtaining ICT support from NT Christian Schools ICT staff as defined below.
- Passwords must be kept secure and confidential, using appropriate password management practices.

4.6.1 Provisions for ICT Team to Access Passwords

In the event that the ICT Team are required to access an individual's account, or a generic account others are responsible for; to resolve or assist with technical issues, a temporary password will be set by ICT Team if you are unable to enter the password yourself.

At the conclusion of and resolution of works, the temporary password will be reset by the user or by the ICT Team to ensure ongoing security of account.

It should be noted that while staff on the ICT Team have full system access to provide support to the organisation as required and are authorised to access all user data when required to provide necessary supports, they are held accountable by NT Christian Schools Policies, protocols, user agreements and Codes of Conduct in the same manner as all other users.

4.7 Use of Artificial Intelligence (AI) and Generative Artificial Intelligence (GenAI)

Artificial intelligence (AI) offers valuable opportunities to enhance productivity, streamline workflows, and support innovative teaching and learning practices. NT Christian Schools is committed to embracing these technologies to enrich and strengthen business operations.

The use of AI must be managed carefully to protect the security, accuracy, and intellectual property of NT Christian Schools' data, private information, ICT infrastructure, and other assets.

AI tools are to be used in a safe, ethical, accountable and legally compliant manner serving as supportive tools that enhance, rather than replace professional judgement in teaching, learning and administration.

All staff have a responsibility to protect NT Christian Schools confidential, sensitive and private information (identifying data)[4], intellectual property, workplace values and ethos.

When utilising AI, only input the minimum data required. Use de-identified data for prompts and testing, and do not enter information considered confidential, sensitive and private information or high-risk personal data into public AI tools.

If AI use contributes to or suffers a data breach, the school must assess, and if required, make required notifications in accordance with Privacy Protection Policy and Privacy Breach Reporting, Investigating, Responding Form.

Where possible, use approved enterprise AI tools that keep prompts and outputs within NT Christian Schools' tenant and apply existing identity, permissions, auditing and retention, and Design Law Treaty (DLT) policies (eg: Microsoft 365 Copilot with Enterprise Data Protection).

Example of acceptable uses of AI

- Drafting routine communications;
- Summarising non-confidential policies;
- Assistance to draft lesson plans and assessments
- Formatting rubrics;
- Assisting with non-sensitive analysis or admin workflows;

Examples of prohibited uses of AI

- Entering student, parent, or staff personal/sensitive information into public AI tools;
- Uploading or prompting with confidential school intellectual property, or unlicensed third-party content to public AI tools;
- Automated decision-making about students or staff with significant effects (discipline/performance management);
- Circumventing copyright/licensing, including mass reproduction of learning materials beyond permitted licences.

All staff must independently verify the accuracy of AI-generated content before relying on content to avoid potential harm, risk, embarrassment and reputational damage from using 'hallucinated' AI output and to ensure there has been no violation of relevant regulations.

Where AI materially contributes to learning activities, assessments, parent communications, or

[4] Privacy Protection Policy

decisions, the use of AI should be disclosed and the nature of human review. Cite sources for factual claims and transparency.

Student's original work must not be uploaded to public AI tools without consent and pedagogical justification. If there is a justification to do so, it should only be on approved platforms and anonymised where feasible.

Staff are to seek permission from ICT Manager before utilising non-enterprise-protected AI tools for security of data and ICT Infrastructure.

4.8 End User Security

All staff and users must undergo security awareness training upon induction and at regular intervals as made available to them.

All staff and users must report any observed or suspected security incidents as per NT Christian Schools' Privacy Breach Reporting, Investigating, Responding Form and/or Cyber Security Incident Response Plan.

DO NOT open any emails or attachments or open links within emails if you are not familiar with the sender or the domain name sending it to you. If an email is received containing information that you are unsure or concerned about, please contact the ICT Team and follow the advice provided. Do not interact with the email until advised otherwise.

If an email is received notifying the receiver of a 'virus', DO NOT forward to anyone, or interact with the email or attachments. Contact the ICT Team to determine validity and further action.

4.9 Vendor and Third-Party Security

Security risks associated with contracted third parties (i.e. suppliers, vendors, cloud service providers, etc.) who maintain direct or indirect access to NT Christian Schools systems and data, must be operationally and contractually controlled.

All third-party services, including Cloud services must be consumed following a formalised risk assessment to identify the necessary security controls that must be implemented by the third party / Cloud Service Provider, and formally documented to manage security risks to an acceptable level. Third parties must be reviewed periodically to assess compliance with contractual cyber terms.

4.10 Patch and Vulnerability Management

NT Christian Schools' IT systems are subject to defined security patch management processes to identify, prioritise, and remediate security weaknesses.

NT Christian Schools' vulnerability management processes must be documented and implemented to identify, prioritise, and remediate security weaknesses. The remediation must be prioritised based on the potential business impact and available mitigation options. Where appropriate, technical solutions and tools must be leveraged and adopted on an ongoing basis to ensure that NT Christian Schools is conducting effective vulnerability scanning and decommissioning of out-of-band legacy systems across its critical IT infrastructure.

4.11 Network Security

NT Christian Schools networks must have appropriate controls in place to protect the network,

information, and assets.

The ability to connect unauthorised devices to the network (wired or wireless) must be controlled, and remote access must be managed, and access secured via use of multi-factor authentication.

4.12 Application Security

End user desktop computers, mobile computers (for example laptops, tablets), must be protected with adequate security mechanisms to prevent the unauthorised disclosure and / or modification of data.

Staff responsible for the administration or subscription management of any application or platform used by entities of NT Christian Schools are required to regularly monitor the privacy, moderation and safety settings to ensure they are active and set up to ensure appropriate protections, particularly after application or platform updates.

Cryptography must be used for protecting sensitive data during its transmission and storage. Data masking must be used to obscure (mask) sensitive information in non-production environments.

4.13 Infrastructure Security

All devices must be securely protected in accordance with approved standards to adequately protect IT systems that support NT Christian Schools' processes and services. Desktop computers, mobile phones, mobile computers (for example laptops, tablets), as well as portable computing devices (for example portable hard drives, USB memory sticks, etc.), must be protected with adequate security mechanisms to prevent the unauthorised disclosure and/or modification of NT Christian Schools data. Baseline configurations must be maintained and reviewed on an annual basis.

All NT Christian Schools building facilities, including office spaces, conference rooms, visitor lounges, and schools must have appropriate security measures in place, (for example CCTV monitoring systems, controlled entry and exit points) to support the safety and security of employees, contractors, visitors, students, other users and assets.

The IT facilities (for example data centers, computer rooms, etc.) that store and process critical information must be constructed, maintained, and monitored in a way that data is adequately protected from physical and environmental threats.

Data must be backed up on a regular basis, protected from unauthorised access or modification during storage, and available to be recovered in a timely manner in the event of incident or disaster.

4.14 Detection and Incident Response Management

Key security related events, such as user privilege changes, must be recorded in logs and protected against unauthorised changes. Logs must be analysed on a regular basis to identify anomalous or potential unauthorised activity and facilitate appropriate follow-up action.

Potential security incidents must be handled appropriately through NT Christian Schools' Privacy Breach Reporting, Investigating and Responding Form and Cyber Incident Response Plans as applicable at school level or enterprise level.

Security incidents must be reported to regulating authorities and necessary bodies as specified in local regulations and legislations for security breach incidents. Security incidents must be

prioritised based on their impact, reported accurately, and handled appropriately in accordance with NT Christian Schools' Privacy Breach Reporting, Investigating, Responding Form and/or Cyber Security Incident Response Plan, and used as future references for resilience against similar security incidents.

5 Roles and Responsibilities

Roles	Evidence of Compliance
ICT Manager & ICT Team Staff	
Implementation of Policy	
Conduct audits and reviews at planned intervals to assess and inform data, information, and system security.	Appropriate documentation that can be audited. Audit and review records.
Ensure regulatory and compliance requirements related to cyber security and data protection is identified, and processes are established to ensure requirements are understood and met by all relevant stakeholders.	
Ensure Privacy and Security Breaches are reported, investigated and responded to appropriately and reported to relevant authorities when required.	Privacy Breach Reporting, Investigating and Responding Forms Cyber Incident Response Plans Critical Incident Response records
Operational Directors	
Conducting audits and reviews at planned intervals to assess and inform data, information, and system security	Audit and review records.
Ensure Privacy and Security Breaches are reported, investigated and responded to appropriately and reported to relevant authorities when required.	Privacy Breach Reporting, Investigating and Responding Forms Cyber Incident Response Plans Critical Incident Response records
Principals, ELC Directors and Line Managers	
Implementation of Policy	
Ensure employees, and other users of ICT infrastructure are made aware of the requirements of the policy.	ICT Acceptable Use Agreements Communication records IT and online safety curriculum
Conduct audits and reviews at planned intervals to assess and inform data, information, and system security	Audit and review records.
Ensure Privacy and Security Breaches are reported, investigated and responded to appropriately and reported to relevant authorities when required.	Privacy Breach Reporting, Investigating and Responding Forms Cyber Incident Response Plans Critical Incident Response records

Roles	Evidence of Compliance
All Users of NT Christian Schools ICT facilities	
Follow policies, procedures and protocols as communicated by NT Christian Schools and Line Managers.	ICT Acceptable Use Agreements Privacy Breach Reporting, Investigating and Responding Forms

6 Definitions and acronyms

The following terms used throughout this policy are defined as follows:

Term	Definition
Administrator Account	An administration account is a user account with high-level privileges to make changes to a computer that will affect other users of the computer. Administrators can change security settings, install software and hardware, access all files on the computer, and make changes to other user accounts.
Applications / Apps	Digital applications or Apps are software designed to perform a particular function on digital devices. They may be linked to a digital program or platform.
Artificial Intelligence (AI)	Using machine learning to create digital content such as text, images, audio and video using technology platforms such as but not limited to: ChatGPT, Google Bard, Copilot, Atlassian, Leonardo.AI
Contractor	A person or organisation who undertakes to provide supplies or a service for a particular project on a contracted term.
Corporate Information Systems	Digital systems that contain data shared among two or more agency organisations used by or are of benefit to more than one organisation to create, update, or delete corporate data. For example, Schools Online.
Data	A subset of information in an electronic format that allows it to be retrieved or transmitted.
DAM	Department of Education Account Manager (DAM) administrators use the DAM tool to give schools, business areas, employees and visitors access to online services in accordance with their employment position or agreed contract access requirements.
Employee	A person employed by NT Christian Schools
Enterprise Data Protection	A systems approach through policy, processes and technologies designed to safeguard the organisations data while ensuring it remains accessible for business operation.
Generative Artificial Intelligence (GenAI)	GenAI term is used to describe the process of using machine learning to create digital content such as new text, images, audio, video and multimodal simulations of experiences. GenAI models can create new outputs instead of just making predictions and classifications like other machine learning.
Generic Email Accounts	An email address generated to support a function of NT Christian Schools or its entities which may have access delegated to one or more team members to monitor and use. These accounts therefore

	may not be directly attributed to single user. For example, admin front desk, admin temp, temp technician and temp teacher.
ICT	Information and Communication Technology
ICT Infrastructure	All physical, virtual and cloud-based infrastructure and software owned or leased by NT Christian Schools including physical or logical connection to the network, including use of Corporate Information Systems – this may include, but not limited to: • Desktop computers, • Mobile computing devices (such as laptops and tablets) • Portable hard drives, USB memory sticks • Mobile phones • Digital programs /platforms such as Compass, Microsoft Teams, Owna, Tech1, Canvas, SeeSaw, Facebook. • Internet access
Intellectual Property (IP)	All content, data, lesson materials, assessments, documentation and works created by staff in the course of employment with NT Christian Schools, except where otherwise agreed, is the Intellectual Property of NT Christian Schools.
Platforms	Web-based software packages/programs that allow sharing information, purchasing products and services, and innovation. Some examples are Uber, LinkedIn, Amazon, social media platforms, and Microsoft.
Risk	Risk is often characterised by reference to any event that will have an impact on the Company or any of its activities. Risk is measured in terms of the consequences that could arise from an event (including changes in circumstances), and the likelihood of that particular consequence occurring. Risks to the NT Christian Schools are generally assessed in terms of their people, reputation, business operations, governance, financial and educational/ academic outcomes respectively
Risk Management	Protecting NT Christian Schools people, and its valuable assets inclusive of processes, property, products and reputation from the impact or consequences of an event by identifying potential impact or hazards by implementing controls and mitigation or minimisation actions that reduce unacceptably high risk.
Personal or Sensitive Information	is personal information or an opinion about an individual such as: • Behavioural and welfare records, • Racial or ethnic origin, • Professional history, • Academic records, • Professional registration details, • Political opinions or associations, • Religious or philosophical beliefs, • Trade union membership or associations, • Sexual orientation or practices, • Criminal records, • Health or genetic information, • Some aspect of biometric information, • Teacher notes,

	Generally sensitive information requires a higher level of privacy protection than other personal information.
Public AI Tools	Any AI applications that are available for public use, often through web platforms or standalone applications. (eg: ChatGPT, DALL-E)
Service Account	A service account is a user account that is created explicitly to provide a security context for services running Windows Server operating systems. The security context determines the service's ability to access local and network resources. The Windows operating systems rely on services to run various features.
Site Manager	Officers, including principals, site managers and line managers, who have executive responsibility for overall management and control of any Department workplace.
Student	A person enrolled in a school or early learning service or programs delivered by NT Christian Schools
User	The individual operating NT Christian Schools' ICT system, resource or infrastructure.
Volunteer	Those who willingly give of their time, knowledge, skill or support NT Christian Schools, without financial gain, either in formal or informal arrangements.

7 Early Learning Compliance

QUALITY AREA 7: GOVERNANCE AND LEADERSHIP		
7.1.1	Service philosophy and purpose	A statement of philosophy guides all aspects of the service's operations.
7.1.2	Management Systems	Systems are in place to manage risk and enable effective management and operation of a quality service.
7.1.3	Roles and Responsibilities	Roles and responsibilities are clearly defined and understood and support effective decision making and operation of the service.
7.2	Leadership	Effective leadership builds and promotes a positive organisational culture and professional learning community.
7.2.1	Continuous Improvement	There is an effective self-assessment and quality improvement process in place.

EDUCATION AND CARE SERVICES NATIONAL LAW AND REGULATIONS	
S.165	Offence to inadequately supervise children.
S.167	Offence relating to protection of children from harm and hazard.
R.84	Awareness of child protection laws
R.145	Staff record
R.147	Staff members

R.168	Education and care services must have policies and procedures.
R.170	Policies and procedures are to be followed
R.181	Confidentiality of records kept by approved provider
R.183	Storage of records and other documents

8 Related legislation and policy

8.1 NT Christian School policies and procedures

- ICT Acceptable Use Policy and relevant agreements.
- Mobile Device Policy
- ICT Continuity and Disaster Plan
- Privacy Protections Policy
- Privacy Breach Reporting, Investigating, Responding FORM
- Record Management Policy and Record Retention Framework
- Reporting and Investigating Incidents Policy
- Risk Management Policy
- Asset Management Policy
- Stewardship Policy
- Child Protection Policy
- Staff and Board Code of Conduct
- Parent, Visitor, Volunteer and Contractor Code of Conduct
- Student Code of Conduct
- Protected Disclosures (Whistleblower) Policy
- Critical Incident Response Plan
- Working Remotely Policy

8.2 Legislation

- Cyber Security Act 2024
- Non-Government Schools Registration Standards, Std: 3.3, 3.4, 8.2
- National Principles for Child Safe Organisations, Ppl: 1.5, 8.2
- Privacy Act 1988 (Cth)
- Workplace Surveillance Act 2005
- Copyright Act 1968
- Criminal Code Act 1995 (Cth)
- Spam Act 2003 (Cth)
- Telecommunications (Interception and Access) Act 2017 (Cth)
- Telecommunications Act 1997 (Cth)

8.3 Other relevant resources

- Australian Cyber Security Center (ACSC) – Essential Eight
- Notifiable data breaches | OAIC
- Online safety | eSafety Commissioner
- Australian Privacy Principles (APP 1-13)