CYBER SECURITY POLICY 21/09/22

Approved by	Council
Approval Date and Type	Date 21/09/22 Type Original
Effective Date and Version	Date 01/10/2022 Version 21/09/22
Previous Approval Date(s)	n/a
Date for Next Review	Date: September 2025
Responsible Officer	Governance Officer/Chief Operating Officer
Policy Consultation	Audit Committee MI Principals MI Responsible Officers
Related Documents	Privacy Act 1988 (Cth) Privacy and Personal Information Protection Act 1998 (NSW) Privacy Policy (SCD) Sensitive Information Protocol (SCD Record Keeping Policy (SCD) Code of Conduct (SCD) Student Grievances and Complaints Policy (SCD) Staff Handbook (SCD)
Higher Education Standards (2021)	Section 2.3 Wellbeing and Safety Section 7.3 Information Management
National Code (2018) and ESOS Act	Standard 3: Written Agreements
Student Lifecycle	(If directly relevant)

1. Policy Purpose

This policy is designed to direct the secure use of online resources and the digital storage of all information within the Sydney College of Divinity, including its Member Institutions.

2. Scope

This policy applies to all staff, currently enrolled students and others affiliated with SCD, including committee and Council members, contractors and visitors.

3. Definitions

- *Sydney College of Divinity, SCD, College:* References to Sydney College of Divinity, SCD or College, assumes reference to all Member Institutions, unless otherwise indicated.
- *Cyber security:* Cyber security refers to measures taken to ensure the security of information held by the College in digital form, and to prevent attack, damage, and unauthorised access to the College's electronic systems.
- *Users:* Users are all staff, students or others who use SCD owned and operated electronic systems in the course of their work, study, or responsibility within SCD.

4. Policy Statement

4.1 General

- The College will maintain up-to-date and effective security measures to ensure the security of information, communication, and electronic systems.
- The College will provide appropriate information and training to users to ensure correct use of SCD resources and adherence to required security measures.
- The College will appoint a responsible officer to monitor cyber security and liaise with relevant consultants or contractors in maintaining cyber security. Individual Member Institutions should appoint a responsible officer to monitor their internal cyber security.

4.2 Passwords

- Unique passwords are provided to, or created by, individual users for access to their personal accounts, or for authorised access to portals.
- Personal passwords should not be shared and should be kept in such a way as to prevent others from gaining access to them.
- Users are required to change their personal password at least every 6 months.
- If a user has more than one personal account a different password should be used for each account.

4.3 Emails

- The College will ensure that effective filters are in place to block unwanted emails.
- Users should delete unrecognised or suspicious looking emails and immediately report any suspicious email activity to the responsible officer.
- College email addresses should be used for work and study purposes.

4.4 Websites and Social Media

- The responsible officer will ensure that College websites and social media accounts are protected by appropriate and up-to-date measures.
- The responsible officer will ensure that College websites and social media accounts are regularly checked for possible security threats and appropriate action taken to counter such threats.

4.5 Secure use of Technology

- The responsible officer will ensure that up-to-date anti-virus software and other appropriate protective measures are installed on all College computers.
- Computers are to be shut down, or screen locked, when not in use or left unattended.
- Users are required to use One Drive where it is made available. Any data kept on external storage devices must be password protected.
- Detailed information on use of technology is provided in the SCD *Acceptable Use of Technology Policy.*
- Where multi-factor authentication is available it must be used.

4.6 Sensitive Information

- Sensitive information may only be accessed by those permitted to do so and must not be share without appropriate authorisation.
- Sensitive information must be kept securely and disposed of when no longer needed.
- For further information refer to SCD *Privacy Policy* and SCD *Record Keeping Policy.*

4.7 Response to Incidents

- The College will have in place a risk management strategy for responding to cyber security breaches in line with its *Risk Management Policies and Procedures.*
- The risk management strategy will incorporate procedures for checking for and identifying threats, find the cause and assessing the impact of the threat, limiting the damage, removing the threat, and taking steps to prevent further threats.
- Breaches in cyber security should be reported immediately to the responsible officer who will act accordingly in line with the risk management strategy and the SCD *Critical Incident Policy.*

4.8 Responsibilities

- The SCD Governance Officer is responsible for overseeing all matters relating to cyber security, including risk management. In their absence the SCD Chief Operating Officer will be responsible.
- Saxons IT, or their successor, is responsible for monitoring and updating security measures and implementing risk management strategies.
- Users have a responsibility to comply with all security regulations and protocols. Users must not communicate information about SCD cyber security to others outside of the College except where authorised by the College or required by law to do so.

4.9 Complaints and Grievances

- Complaint or grievances related to cyber security will be addressed according to the *SCD Complaints and Grievances* policies.

4.10 Breach of Policy

- A breach of this policy will occur when a user takes actions, whether deliberate or inadvertent, that threaten or breach the security of SCD computer systems, electronic communication, or electronically stored information.
- Breaches of policy may result in disciplinary proceedings including, but not limited to, warnings, suspension or termination of enrolment or employment, and legal action.

5. Related Policies/Procedures/ Guidance Notes

6. Monitoring and Review

- This policy will be reviewed every three years and will be included in the Council's Annual Workplan Schedule.
- This policy may be amended as required.
- Reviews of the policy will include, if needed, engagement of consultants with expertise in the field, and/or reference to credible sources of information.