Cybersecurity Policy and Procedures - Students

1. Scope

This Policy and Procedure applies to Holmes Institute (Holmes) and to all its current, prospective and former students. This Policy applies to all information assets that are owned and/or operated by Holmes and/or registered in any Domain Name System (DNS) domain owned by Holmes, being used on campus or off-site, and any devices that are present on Holmes' campuses, but may not be owned or operated by Holmes. This Policy also covers any information assets outsourced or hosted at external/third-party service providers, if that asset resides in a Holmes domain or appears to be owned by Holmes.

2. Purpose

2.1. This document sets out Holmes' policy on cybersecurity.

2.2. Cybersecurity is about defending IT Facilities and Services and stored data from unauthorised access, use, disclosure, disruption, modification and destruction. It is concerned with ensuring integrity, availability, confidentiality and safety of data and services and ensures controls are proportionate to risk.

2.3. Holmes recognises the importance of cybersecurity. It is committed to ensuring all Institute activities involving Information Technology are appropriately defended against cybersecurity threats.

2.4. Holmes recognises that successful implementation of cybersecurity relies on having a well-informed user community combined with effective management procedures. This overarching policy is supported by this recognition and it provides principles for Holmes' continuous enhancement in terms of operational practice, action plans, technology controls and education programs around the concern of cybersecurity.

2.5. Holmes is committed to the appropriate use of Information Technology and Services to support its learning, teaching, research, administrative, and service functions. The Acceptable Use of Information Technology Policy defines acceptable behaviour expected of Users of Holmes' IT Facilities and Services.

2.6. This policy aims to protect Holmes' information from unauthorised access, loss or damage, intentional or otherwise, while ensuring seamless access to academic resources by students.

3. Definitions

3.1. **IT Facilities and Services** means Information Technology facilities operated by or on behalf of Holmes. This includes services and systems and associated computing hardware and software used for the communication, processing and storage of information.

3.2. **Cybersecurity** means the practice of defending computing devices, networks and stored data from unauthorised access, use, disclosure, disruption, modification or destruction.

3.3. **Holmes' network** means the network infrastructure used by the Institute including all network services all campuses and associated businesses or companies with trusted access to Holmes' services.

3.4. **Information Asset** means any information that is of value to the organisation. This term also includes the underlying supporting infrastructure such as business processes,

hardware, networks, storage, applications, third-party providers and storage amongst others.

3.5. **Information Security** means the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity and availability.

3.6. **Authentication Information / Credentials** means any form of authentication used to validate the identity of an individual. Common authentication information are: passwords, private keys, tickets, tokens, etc.

3.7. **Account** means a way to identify and authenticate individuals to a system.

4. Policy Principles

4.1. Internet Filtering

a) The Internet has become an essential tool in education, however, some information and sites on the Internet condone or promote matters which are illegal in Australia or directly contravene Holmes' values, standards and policies.

b) Internet Filtering can reduce the risk to Holmes from those who practise antisocial behaviour such as creating viruses, distributing spyware, attempting to break into computer networks and/or sending unsolicited commercial emails.

c) Holmes subscribes to a Web Content Filtering service. This service has been employed to block access to Internet sites with particular categories of content as well as sites which may threaten Holmes' security.

d) Students may request the blocking of sites they have good reason to believe are in contravention of legislation or Holmes' policies and values.

e) In accordance with the principles of academic freedom, students may request to be excluded (in part or in whole) from web filtering if their Holmes-related work or studies requires access to these sites.

4.2. IT Security Audit

a) The IT Manager has the authority to conduct a security audit on any system at Holmes at any time.

b) IT security audits may be conducted on all computers and communication devices owned or operated by Holmes as well as any computer and communication devices that are present on Holmes premises, but may not be owned or operated by Holmes.

c) IT Security audits may be conducted to:

i. Ensure integrity, confidentiality and availability of information and resources.
ii. Investigate possible security incidents.
iii. Investigate possible violations of laws applicable in any Australian state, the Commonwealth of Australia and any international jurisdiction in which Holmes conducts operations.
iv. Ensure that Holmes complies with relevant legislation.
v. Monitor user or system activity where there is a legitimate concern that one or more of the above conditions is not being met.
vi. Ensure resources are used appropriately and for study-related purposes in accordance with policy.
vii. Facilitate the recovery of Holmes' information stored on individual desktop PCs, laptops or devices etc.

4.3. User Access Management

a) All Holmes equipment, networks and business systems must identify and authenticate users by an approved authentication service.
b) Student access to Holmes' information systems and services may be suspended or cancelled in the case of misconduct in accordance with the Student Charter and Conduct Policy and Procedures.
c) Students will continue to have access to their student accounts for a period of 12 months after the end of their enrolment.

4.4. Virus Protection

a) Antivirus software is employed by Holmes to protect against the damage caused by virus attacks.
b) The IT Manager will respond to any detected, likely or imminent attack to Holmes' network as he/she sees appropriate.
c) A PC, laptop or another device that has been infected will be disconnected from Holmes' network. The infected device will need to be cleaned and cleared of any threat to Holmes' network. The device may be required to be presented for inspection by the IT Manager before reconnection to the network is permitted.
d) If an infection to a file occurs, the following steps apply:
    i. If a file can be cleaned, it is cleaned.
    ii. If it cannot be cleaned, and the file is recoverable from backup, it is deleted.
    iii. If it cannot be cleaned, and the file is not recoverable from backup, it is quarantined off the network.

5. Students Roles and Responsibilities

This section outlines the roles and responsibilities of Holmes students towards cybersecurity. All students are required to follow these procedures.

5.1. Password Management

a) It is important that students use strong passwords to access their Holmes' accounts. It is recommended that you use a password that is at least 8 characters in length and one that is a combination of numbers, letters and special characters.
b) Passwords must be changed every 60 days, or as soon as you suspect that your password may have been compromised.
c) You cannot reuse any of your previous 10 passwords.
d) Avoid adding serial numbers to your old password when changing your password.
e) Your password should be unpredictable, i.e. it should not contain any part of your name, email address, phone number, birth date, etc.
f) Do not use the same password across multiple accounts.
g) Do not share your password with anyone, not even staff from Holmes.
h) Holmes staff will never ask for your password, not in person, not over the phone.
i) Do not write or print your password on a piece of paper or stick it to your laptop or PC.
j) Do not write your password in a text file and store it in your computer.
k) Your password must be memorable, but only to you.

5.2. Email Security

Emails are a major source for computer malware. Thus vigilance is required, especially when receiving an email from an unknown source.

a) Do not click on links or download attachments contained in a suspicious email. A suspicious email is one that is unexpected, coming from unknown source or is out of context. If the suspicious email seems to be coming from a Holmes' staff member, verify the authenticity of the email via other means, for example, talk to the alleged sender in person or over the phone.

b) Do not forward suspicious emails to others.
c) Do not open emails from unknown sources.
d) If you receive a suspicious email, delete it immediately.
e) Be aware that email communications via Holmes' network may be monitored. Holmes emails should only be used for course-related purposes.
f) Do not forward confidential information to unauthorised parties.
g) If you receive confidential information that is not intended to you, delete it immediately.
h) You are encouraged to add a signature to your email to properly identify yourself.
i) Double check prior to hitting replay-all in your response to emails, especially if your response contains confidential information.

5.3. Device Security

It is important to maintain the security of all devices used to access Holmes' network. This includes personal computing devices such as laptops, tablets and smartphones, used to access Holmes' network or storing course-related data.

a) All computing devices connected to Holmes network must be password-protected. Smartphones can either be PIN-protected or using biometrics.
b) Regularly update your operating system, software, browser and antivirus.
c) Do not leave your laptop, tablet or phone unattended.
d) Lock your screen before leaving your computer, even when leaving for a short period of time.
e) If you have to leave your laptop behind, you are encouraged to physically lock it.

5.4. Portable Storage Media

Portable storage media refers to external storage devices such as thumb drives, external hard drives and Micro SD Cards. Computer malware can easily spread via portable storage devices.

a) Scan storage devices before connecting them to your machine.
b) Remove storage devices once no longer in use. You are encouraged to copy the materials you need and unplug the storage device immediately. If the materials are copied to a public machine, make sure to permanently delete the copied materials when no longer needed.

5.5. Confidential Information

For the purpose of this policy, confidential information refers to: personal information such as date of birth, home address or phone number; sensitive information such as financial transactions, health records, assessment materials and exam results; and Intellectual Property such as formulas and inventions.

a) When no longer needed, taking into account privacy requirements, confidential documents in physical form must be disposed of in a safe manner.
b) Confidential documents in physical form, must be kept in a secure location, while those in digital form must be kept in a secure machine.
c) Confidential information should only be disclosed to the intended parties.
d) If you receive confidential information that is not intended to you, delete it immediately.

5.6. Social Media Websites

This policy applies to formal use of social media on behalf of Holmes or the personal use of social media when referencing Holmes Institute. Social media refers to social networking websites, vlogs, forums and any public digital platform which enables sharing of ideas, photos, audio or video. Students should be aware of the potential reputational damage of posts on social media to them and Holmes as an organisation. Examples of prohibited media posting include defamatory, discriminatory or harassing posts.

a) Refrain from sharing confidential information on social media platforms.
b) Use of social media on Holmes' network or computers should be limited to study-related purposes. Use of social media on Holmes' network or computers for personal purposes is prohibited.
c) Minimise the amount of personal information (e.g. birthdate, contact information, home address) you share on social media and the Internet. The more personal information you make public, the more susceptible you are to spear-phishing attacks and/or identity theft.
d) Avoid accessing or downloading materials from suspicious websites while using Holmes' network and/or computing devices.
e) If you receive a suspicious web-link through social media, do not click on it. Instead, consider typing company/service name in a search engine and go to their website.

5.7. Physical Security

Physical security is a critical component of the overall cybersecurity ecosystem. There is generally a higher chance for a compromise to succeed if the attacker gains physical access to targeted machines.

a) Do not hand over your student ID/access card to someone else (including staff).
b) Students are no allowed to enter lecturers' rooms or other administrative areas (other than reception) unless authorised by staff.
c) Do not leave confidential information (e.g. assessment papers or personal information) on printer's tray or scanner's lid or any common area.
d) For your safety, familiarise yourself with the emergency procedure for the lift. Also, familiarise yourself with the evacuation procedure of the building.

5.8. Incident Response

The overall security framework at Holmes can only be successful if everyone paid their share in securing the system. Should you detect a spam, security intrusion or any suspicious activity, notify Holmes IT Helpdesk immediately. Examples for suspicious system activities include:

a) Your account becoming inaccessible.
b) The computer becoming too slow, running out of memory or frequently freezing.
c) Frequent pop-ups on the screen; and
d) Receiving spams appear to be coming from your machine.

Version Control and Accountable Officers

It is the joint responsibility of the Implementation Officer and Responsible Officer to ensure compliance with this policy.

Responsible Officer	Chief Executive Officer
Implementation Officers	IT Manager
Review Date	July 2027
Approved by	
Governing Council	
Associated Documents	
Academic Freedom and Freedom of Speech Policy Acceptable Use of Information Technology Policy Privacy Policy and Procedure Student Charter and Conduct Policy and Procedures Student Deferral, Suspension and Cancellation Policy and Procedures	

Version	Brief Description of the Changes	Date Approved	Effective Date
1	New Policy	26 March 2021	26 March 2021
1.1	No change scheduled review	Not required	12 July 2024