Acceptable Use of Information Technology Policy

1. Scope

This Policy applies to all Holmes Institute (Holmes) staff, students, contractors, visitors and other authorised users of Information Technology (IT) facilities and services. This Policy also applies to all authorised users connecting to IT services from either personal (BYOD) or Holmes owned facilities.

2. Purpose

This policy is in place to ensure that all Holmes' stakeholders understand and use the Holmes' IT facilities and services in a proper and responsible manner.

3. Definition

3.1. IT Facilities and Services include but are not limited to:

a) Computer equipment, software, operating systems, storage media, communication facilities and accessories (voice, video and data), network accounts, network services, email accounts and central archive, web browsing, phones and hand-held devices; and IT equipment and physical infrastructure located in communications rooms, data centres, workspaces, PC laboratories and other locations both within and outside of Holmes; and

b) Bring Your Own Device (BYOD): the use of any electronic device not owned or leased by Holmes, and which is capable of storing data and connecting to a network (e.g. wireless, 4/5G, physical connection), to access or connect to Holmes' IT services, data and networks. This includes but is not limited to mobile phones, smartphones, tablets, laptops, notebooks and portable storage devices.

3.2. Collaboration Services: Include but are not limited to; technologies used to transfer messages, including email, instant messaging, and peer-to-peer exchanges provided by or affiliated with Holmes.

4. Policy Principles

4.1. IT facilities and services are provided for the purpose of academic and Holmes related business.

4.2. Holmes IT facilities and services are provided solely for legitimate Holmes' business and operations.

4.3. Authorised users of Holmes IT facilities and services are responsible for exercising good judgement regarding reasonable personal use with guidance from Teaching staff and Student Services for students; and individual departmental managers and Directors/Deans for staff and other users.

4.4. All Holmes staff, students, contractors, visitors and other authorised users of Holmes IT facilities and services are expected to use these facilities and services in an appropriate and responsible manner.

4.5. It is the responsibility of authorised users of IT facilities and services to familiarise themselves with Holmes' policies, procedures and guidelines related to IT and to conduct their activities accordingly.

4.6. Users may be exempt from aspects of this policy where it is required for their role, studies or research, where written permission from the head of the relevant department and the IT Manager has been obtained.

4.7. Users who choose to BYOD must:

a) assume sole responsibility for the operating system, the device and any personal applications running on the device;

b) ensure that the operating system, firmware and installed software is obtained from an authorised source, is up to date and that required security patches have been applied to protect against known vulnerabilities;

c) employ security solutions where available, including anti-virus, firewall and threat intelligence solutions.

5. Monitoring and Auditing

5.1 All data created on Holmes' systems, including communications infrastructure and desktop computers remains the property of Holmes. This includes emails sent and received from Holmes' staff and student email accounts as well as emails retained in central archive.

5.2 In order to protect the Holmes' network, servers and data and/or to comply with legal or regulatory requirements, Holmes has the right to intercept, interrogate, or otherwise capture data created or received by individual users of IT facilities and services.

6. Personal Use

6.1 IT facilities and services are provided for the purpose of academic and Holmes related business operations. All staff, students, contractors and visitors are to use these facilities and services for their authorised and intended purpose.

6.2 Users are responsible for exercising good judgement regarding reasonable personal use in line with their duties and responsibilities.

6.3 Costs incurred by Holmes through excessive personal use may be recovered directly from the individual concerned, and may lead to further disciplinary/legal actions.

6.4 Users should not allow access to the IT facilities and services to unauthorised users.

6.5 Authorised users of IT will be held responsible for all actions including any infringement carried out by a third party given access to IT facilities and services via their accounts.

7. Unacceptable Use

The following is inappropriate and prohibited when accessing, connecting to or using IT facilities and services:

7.1 Engaging in any activity that is illegal under State, Federal or international law or in breach of any Institute policy.

7.2 Use for the purpose of creating, accessing or transmitting or otherwise dealing with content which is objectionable, obscene or offensive, or in a manner which is contrary to other Holmes' policies or which may otherwise expose Holmes to legal liability.

7.3 Use that violates copyright or intellectual property including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Holmes.

7.4 Use for commercial or private gain unless approved by a management.

7.5 Sending of unauthorised and unsolicited global or commercial messages (spam or junk mail).

7.6 Unauthorised tampering with any part of IT infrastructure or deliberate modification to the current production network.

7.7 Damage or alteration, either wilfully or through negligence, of any hardware, software, physical plan, or communications component without proper authorisation.

7.8 Tamper with, deface or permanently mark Holmes IT equipment in any way.

7.9 Deliberate introduction of malicious programs into the Holmes' IT network.

7.10 Deliberately effecting security breaches or disruptions of Holmes IT network or business systems including, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorised to access, unless these activities are within the scope of regular duties.

7.11 Circumventing user authentication or security of any host, network or account without proper authorisation.

7.12 Interfering with or denying service to any authorised user (e.g. denial of service attack).

7.13 Making fraudulent or unapproved offers of products, items, or services originating from any Holmes IT facility or service is prohibited.

7.14 Making statements about warranty, guarantees, or similar binding commitments on behalf of Holmes, expressly or implied, is prohibited unless it is a part of normal job duties.

7.15 Providing information about or lists of Holmes' staff and students to parties outside of Holmes is expressly forbidden unless it is part of normal job duties.

8. Breaches of the policy

All reported breaches of this Policy will be treated seriously and in accordance with the relevant procedures.

8.1 The consequences for substantiated breaches of this Policy will depend on the seriousness of the case.

8.2 Outcomes may include, but are not restricted to the following:

a) Disciplinary or other appropriate action

b) Withdrawal of access to the Holmes' email system and computer network.

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 Operating Officer
Implementation Officers	IT Manager
Review Date	July 2027
Approved by	
Governing Council	
Associated Documents	
Business Continuity Disaster Recovery Plan IT Code of Conduct Policy Cybersecurity Policy and Procedures – Staff Cybersecurity Policy and Procedures – Students Student Charter and Conduct Policy – Higher Education	

Version	**Brief Description of the Changes**	**Date Approved**	**Effective Date**
1.0	New Policy	2 March 2020	2 March 2020
2.0	Scheduled review by Governing Council	December 2023	December 2023
3.0	Addition of BYOD clauses	12 July 2024	12 July 2024