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

b) IT equipment and physical infrastructure located in communications rooms, data centres, work spaces, PC laboratories and other locations both within and outside of Holmes.

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 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.

4.2 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.

4.3 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.

5. Procedure Principles

Provision of IT

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

Personal Use

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

5.3 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.

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

Monitoring and Auditing

5.5 All data created on corporate 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.

5.6 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.

Unacceptable Use

5.7 Under no circumstances are Holmes owned or managed resources to be used to engage in any activity that is illegal under state, federal or international law.

5.8 Holmes IT facilities and services must not be used by staff and students for the purpose of creating, accessing or transmitting or otherwise dealing with content which may reasonably be regarded as objectionable, obscene or offensive, or in a manner which is contrary to other Holmes' policies or which may otherwise expose Holmes to legal liability.

5.9 Any person utilising Holmes IT facilities and services, must do so in accordance with the Copyright and Intellectual Property Laws and policy. This includes, but is not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Holmes.

5.10 The use of Holmes IT facilities and services for unauthorised commercial gain is strictly prohibited.

Access to IT facilities and services

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

5.12 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.

Collaboration Services

5.13 Users of the Holmes' email and other collaboration services are prohibited from engaging in any activity that is illegal under state, federal or international law or against any Holmes policy when using these services.

5.14 A disclaimer will be automatically attached to all outgoing emails sent from Holmes email accounts. This disclaimer must not be altered or interfered with in any way.

5.15 The following is disallowed for all emails sent from Holmes' email accounts:

a) Creating or exchanging messages that are offensive, harassing, obscene or threatening;
b) Exchanging proprietary information, trade secrets, or any other privileged, confidential or sensitive information outside Holmes, or outside a defined privileged group;
c) Creating or exchanging advertisements, solicitations, chain letters and other unsolicited email, unless valid within the context of the person's employment;
d) Reading or sending messages from another user's account, except under proper delegated arrangements;
e) Altering or copying a message or attachment belonging to another user and sending it to others without the express permission of the originator; and
f) Using the Holmes email system for non-Holmes related commercial purposes.

5.16 All email records from Holmes email accounts that have been moved to the central archive will be retained.

Network and Internet

5.17 Deliberate modifications to the current production network are prohibited without proper authorisation.

5.18 Deliberate introduction of malicious programs into the network or server (e.g. Viruses, worms, Trojan horses, e-mail bombs, etc) is strictly prohibited.

5.19 Deliberately effecting security breaches or disruptions of network communication is prohibited. Security breaches include, 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.

5.20 Port scanning or security scanning including the execution of any form of network monitoring is prohibited unless prior approval has been granted by ITS.

5.21 Circumventing user authentication or security of any host, network or account is prohibited without proper authorisation.

5.22 Interfering with or denying service to any authorised user (e.g. denial of service attack) is prohibited without proper authorisation.

5.23 Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, any authorised user's terminal session, via any means, locally or via the external Web is prohibited. This applies to sessions anywhere on the Web (i.e. including hacking sessions on external Web addresses).

5.24 Any devices (including desktops and laptops) connected to the Holmes network, whether owned by the staff member or Holmes, must have the current operating system patches applied to them and be equipped with the latest antivirus software, either by automated download or manual update.

Security and Proprietary Information

5.25 Staff are responsible for considering the sensitivity of any information or data transmitted across the internal and external network, and ensuring that it is treated appropriately according Holmes policies. Examples of confidential information include but are not limited to:

a) Examination results;
b) Confidential senior management communications;
c) Specifications of commercialised Holmes developments or patents;
d) Vendor lists;
e) Details of commercial contracts and agreements; and
f) Research data restricted by privacy and ethical concerns.

5.26 Staff should take all necessary steps to prevent unauthorised access to confidential information and use secure modes of communication.

5.27 Sensitive information held on desktops or transmitted across the Internet should be encrypted and sent over a secure network connection. Because information contained on laptop computers is especially vulnerable, additional special care should be exercised.

5.28 Making fraudulent or unapproved offers of products, items, or services originating from any Holmes' IT facility or service is prohibited (e.g. offering access to Holmes' services for personal benefit).

5.29 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.

Breaches of the policy

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

5.31 The consequences for substantiated breaches of this Policy will depend on the seriousness of the case. Outcomes may include, but are not restricted to the following:

a) Disciplinary or other appropriate action in the case of visitors, consultant or other external users.
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	May 2022
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	New Policy	2 March 2020	2 March 2020
1.1	Added the Cybersecurity Policies in the Associated Documents		