ICT Acceptable Use Policy

1. PURPOSE

To outline the expected behaviours of users when using, or having access to, Institute owned information technology equipment and information assets (Information, Communications and Technology (ICT) resources.)

2. SCOPE

Applies to all users using, or having access to, ICT resources for business and/or academic use. It also applies to any contractors and consultants who provide work onsite on behalf of Holmesglen Institute.

3. POLICY STATEMENT

ICT resources are provided by the Institute to all users to improve and enhance learning, teaching, and business functions of the Institute. Using information technology, accessing information, and communicating electronically can be cost-effective, timely and efficient and carries with it responsibilities.

4. PRINCIPLES

4.1. Acceptable use

4.1.1. ICT access and usage at Holmesglen must be undertaken in accordance with the principles of acceptable usage and access.
Refer to Appendix 1 Unacceptable Use of ICT Resources and the Institute's Code of Conduct.

4.1.2. Unacceptable use of ICT resources will be treated as a breach of Holmesglen's Code of Conduct and action taken in accordance with the Conduct Rule and Access Control Policy.

4.2. Internet site and content filtering

Holmesglen recognises and respects the need for academic freedom in teaching, learning and applied research when accessing internet sites and content. However, for the purposes of maintaining respect and ensuring acceptable usage, some internet sites and content are filtered and blocked at the discretion of the Chief Information Officer.

4.3. Taking ICT resources off-site

Equipment, information or software, regardless of its form or storage medium, must not be taken off-site without prior permission from the Chief Information Officer. This excludes devices specifically purchased for this purpose – for example, laptops, mobile phones, tablets.

4.4. Passwords

To safeguard the integrity of Holmesglen's employees network, information and systems, Holmesglen enforces access by means of password control. This means that:

4.4.1. Holmesglen implements complex password requirements for all users.

4.4.2. Complex passwords consists of: a minimum of 10 characters; a minimum of one uppercase alpha character (A - Z); a minimum of one numerical character (0 – 9) and a minimum of one non-alphanumeric character (e.g.? # % &).

4.4.3. Holmesglen ensures that the password system remembers the last 8 passwords used and passwords cannot be reused if they are remembered by the system.

4.4.4. Passwords must not be disclosed to other persons, including management and system administrators.

4.4.5. Passwords used for private purposes must not be used for business purposes.

4.4.6. Users must utilise the 'Self-Managed Password' Facility.

4.5. Use of social media

4.5.1 Users of social media must ensure that comments they make are consistent with official Holmesglen's commentary, rules, policies, and procedures.
Refer to Appendix 2 and the Social Media Guidelines.

4.5.2 Holmesglen approved corporate social media channels are managed and all accounts are monitored.

4.6 Use of email and other Institute communication channels

Email, telephony and SMS facilities are provided to users to undertake Institute business activities.

4.6.1 Emails or other electronic communications must not be used for the creation or distribution of any offensive or abusive message. This may include offensive comments about race, gender, age, sexual orientation, pornography, religious or political beliefs, national origin or disability.

4.6.2 Users must be aware of the information classification, as defined in the Information Security Policy, of the messages they send or receive and handle that information appropriately.

4.6.3 Emails are automatically scanned and inspected for viruses or malware upon sending and prior to receiving. Certain emails will be quarantined and released manually if appropriate. Infected, suspicious or blacklisted emails will be deleted.

4.6.4 Users must not solicit emails that are unrelated to the Institute's business activities.

4.6.5 Institute business activity and communications must only occur using the official communication channels provided to users.

4.6.6 Holmesglen Institute reserves the right to monitor, access and inspect user email and other electronic communications. For this reason, communications are not guaranteed to be private.

4.6.7 Reasonable personal use of Holmesglen email accounts is permitted.

4.7 Systems monitoring and inspection

All data which is created, stored, sent or received through ICT resources or other organisational communication systems, including various applications, email, Internet, fax, etc., whether it is personal or not, is subject to system monitoring.

4.7.1 Holmesglen Institute reserves the right to inspect ICT resources. This may include, but is not limited to, individual login sessions, the internet sites visited by users, emails, files stored, downloaded and generated.

5 ACCOUNTABILITIES

Action	Accountability
Identify ICT risks that may affect the ICT Acceptable Use Policy and recommend changes to the Chief Executive.	Chief Information Officer

Action	Accountability
Consider, review and approve requests to take ICT resources off-site.	Chief Information Officer
Consider, review and approve monitoring and access investigations of users or a group of users.	Executive Director Corporate and Commercial Services
Undertake approved monitoring, access and inspection investigations. Rescind, suspend or modify user access to ICT resources on the basis of investigation findings.	Chief Information Officer
Monitor ICT resources from a systems view.	Infrastructure Manager (TSD)
Appoint a person to oversee the approved corporate social media channels for business purposes.	Managers in consultation with Associate Director Brand, Marketing and Student Recruitment
Promptly report any issues to the TSD Helpdesk.	All users

6 DEFINITIONS

Term	Meaning
ICT resources	All IT infrastructure, system and application software, data, and other information assets and components which are owned or used by the Institute. In the context of this Policy, the term information assets is applied to information systems and other information/equipment including paper documents, mobile phones, portable computers, data storage media, Internet access, email, Brightspace LMS, telephony.
Information assets	An identifiable collection of data including, but not limited to paper documents, databases and data files and digital documents. Includes all records created and/or held within Business IT Systems or on approved networks and cloud services.
Holmesglen approved social media channels	Includes Facebook, Instagram, Twitter, LinkedIn and Holmesglen Online Community Platform

THINK principles	'THINK' before posting or commenting.
	T is it truthful;
	H is it hurtful;
	I is it inspiring;
	N is it necessary;
	K is it kind.

Term	Meaning
Reasonable personal use	Holmesglen's systems must generally be used only for business activities. Reasonable personal use is permissible as long as: a) It does not consume more than a trivial amount of resources. b) It does not interfere with an employee's productivity. c) It does not pre-empt any business activity. d) It is not used for commercial purposes outside of the Institute.
Social media	Includes but is not limited to Instant Messaging and Chat streams, Short Message Service (SMS) and SnapChat, professional networking sites such as LinkedIn, blogs on social networking sites such as Twitter, Facebook, Google+, 'comments' on online newspapers, photo and video sharing sites such as YouTube, Instagram, Flickr, wikis such as Wikipedia, forums and discussion boards.
Self-Managed Password Facility	A facility to enable users to manage their own passwords. This includes changing passwords and unlocking a locked account once the user verifies their identity.
Users	Any employee or learner, or any other person who uses Holmesglen's facilities, including a contractor and any employee or agent of a contractor.

7 CONTEXT AND/OR REFERENCED DOCUMENTS

Internal

Access Control Policy

Information Security Policy

Conduct Rule

Code of Conduct

Social Media Guidelines

External

Privacy and Data Protection Act 2014 (Vic)

8 REVIEW

This policy must be reviewed no later than three years from the date of approval.

The policy will remain in force until such time as it has been reviewed and re-approved or rescinded. The policy may be withdrawn or amended as part of continuous improvement prior to the scheduled review date.

9 VERSION HISTORY

Version Number	Date	Summary of changes
1	November 2017	New Policy incorporating and replacing: ▪ Electronic Code of Practice ▪ Employee Code of Conduct – Social Media

Version Number	Date	Summary of changes
		▪ Rule for Password
2	August 2018	Minor changes to arrange some content into two appendices.
3	October 2019	Inclusion of Holmesglen approved social media channels and its management.
4	July 2023	Scheduled review, minor changes to reflect current practices and protocols.

APPENDIX 1 – UNACCEPTABLE USE OF ICT RESOURCES

Unacceptable use includes, but is not limited to, the following:

1) Storing information assets in locations other than the network drives or approved systems and cloud services;
2) Using ICT resources excessively for non-educational and training activities or non-Institute business;
3) Revealing or publicising personal or proprietary information not specifically marked for disclosure;
4) Downloading, uploading or otherwise transmitting commercial software or any copyrighted material not licensed for use at Holmesglen;
5) Using ICT resources to access, create, transmit or solicit material which is obscene, defamatory, discriminatory in nature, or likely to cause distress to some individuals or cultures, where such material is not a legitimate part of teaching and learning;
6) Visiting Internet sites that contain obscene, hateful or other objectionable materials
7) Send or receiving material that is obscene, defamatory or which is intended to annoy, harass or intimidate another person;
8) Tampering with hardware components or hardware configurations without the express permission of the person/s responsible for that particular item of equipment. This includes workstation, monitor, keyboard and mouse; printers and other peripherals; network outlets, cabling and other components; telephones; any part of a computer lab or classroom equipment;
9) Attempting to gain unauthorised access to ICT resources;
10) Removing or interrupting authorised access to information assets and other ICT resources, including removing access to shared information assets, deleting assets or moving assets into unauthorised locations;
11) Making use of unauthorised data or information obtained from the use of ICT resources;
12) Attempting to identify or exploit weaknesses in ICT resources;
13) Using ICT resources to gain unauthorised access to third party IT facilities;
14) Using ICT resources in unauthorised attempts to make third party IT facilities unavailable;
15) Attempting to defeat the cyber or information security measures implemented by the Institute including, but not limited to, firewalls, proxy avoidance and virus protection measures;
16) Intentionally interfering with the normal operations of the Institute network including the propagation of computer viruses and sustained high volume network traffic which substantially hinders others in their use of the network;
17) Examining, changing or using another person's files, output, or login credentials for which they do not have explicit authorisation from the Chief Information Officer; and
18) Performing any other inappropriate use as identified by the Technology Services Department.

APPENDIX 2 – ACCEPTABLE SOCIAL MEDIA USE

Users must follow the Social Media Guidelines and the following protocols for acceptable social media use:

1) Observe the requirements for privacy and copyright, including related issues for copyright of images and videos, publicly available information and the making of public comments.
2) Where an employee posts a comment directly related to their field of expertise, the employee may use Holmesglen's name and their position title to establish their credentials. Comments of this nature should be limited to the individual's area of expertise and should not affect Holmesglen's brand or reputation in any way.
3) Faculties/Departments using private groups in social media for business purposes must oversee the social media tools with the express purpose of maintaining a professional communication stream.
4) The 'digital citizen' THINK principles must be used when making comment on social media.
5) Personal social media accounts must not be used to communicate with, friend or follow learners.
6) The personal use of social media during work hours must be limited to official breaks.
7) Personal use of social media must never have an adverse effect on Holmesglen's brand or reputation and users must minimise the risk of this occurrence.
8) Users posting comments or other artefacts in a personal capacity are personally responsible for their published content.