PROCEDURE C31.0-P31.0

STUDENT USE OF SCENTIA INFORMATION AND COMMUNICATION SERVICES

1.0 INTRODUCTION

1.1 Related Policy

Student Use of Information and Communication Technology (ICT) Services

1.2 Purpose

This procedure provides for the operationalisation of the Student Use of ICT Services Policy.

1.3 Scope

This procedure applies to all students enrolled in the Scentia Group Colleges: the Australian Institute of Management, Education and Training Registered Training Organisation (AIM RTO), the AIM Business School (ABS) and the Australasian College of Health and Wellness. (ACHW)

1.4 Scope Exceptions

This policy does not apply to Scentia staff who should refer to the Scentia Acceptable Use of Information and Communication Technology Facilities for Staff.

2.0 RESPONSIBILITIES

1. All those referred to under the Scope of this policy are responsible for complying with its terms and procedure.

2. The Head of Compliance is responsible for the review of this Policy and Procedure in consultation with the Head of Technology.

3. The Head of Technology has overall responsibility for:

   a. the implementation of this Policy and Procedure; and
   b. providing ICT facilities as required for Scentia.

3.0 PROCEDURE

3.1 General use and ownership

1. Access to Scentia ICT services, particularly its Learning Management Systems, (myAIM, myABS and myACHW) must be authenticated and comply with credentials guidelines set by the Head of Technology. Passwords and access to ICT services must not be shared.

2. ICT services must not be used for unauthorised commercial activities or unauthorised personal gain.

3.2 Use of BYOD devices

1. This procedure and related policy apply to BYOD devices connected to the Scentia network and internet.

2. Students must lock BYOD devices (computers, tablets, mobile phones) when not in use.

3. Students are responsible for the loss or damage of any personal devices and accessories and Scentia is not liable for any costs associated with the repair or replacement of lost / damaged device/s and accessories.

3.3 Internet

1. When using Scentia's ICT services to access and use the Internet, students must act in accordance with the Freedom of Intellectual Inquiry and Expression Policy, Copyright and IP Policy, and other relevant legislation.

2. Students are expected to use the Internet for legitimate learning purposes related to their course. The use of Social Media is governed by the Social Media Policy.

3. The Head of Technology may deny or restrict a student's access to internet sites that are reasonably considered to contain inappropriate or malicious content.

3.4 Unacceptable use

Unacceptable use includes but is not limited to:

a. Engaging in any activity that is in breach of Scentia's policies or procedures, or illegal under local, state, federal or international law;

b. Accessing data, network, a server or an account for any purpose other than engaging in learning at AIM, ABS or ACHW;

c. Circumventing user authentication or security of any host, network or account;

d. Executing any form of network spoofing and monitoring which will intercept data not intended for the user's host;

e. Intentionally introducing any program or device that would degrade Scentia's ICT services;

f. Deliberate, unauthorised corruption or destruction of ICT services (including deliberate introduction or propagation of computer viruses);

g. Using ICT facilities to access, create, store, 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 or research;

h. Transmission or use of material which infringes copyright held by another person or Scentia;

i. Interfering with or denying service to another user;

j. Sending unsolicited email messages, including sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam);

k. Effecting security incident(s) in a manner that negatively impacts Scentia, its staff or students;

l. Providing information about, or lists of, Scentia ICT users to outside parties;

m. Use which deliberately and significantly degrades the performance of ICT services for other users (including the downloading of large video files not related to teaching and learning and research).

3.3 Monitoring and Access

1. The Technology Business Unit will monitor ICT services including but not limited to:

   a. protecting the integrity and security of Scentia 's ICT facilities;
   b. checking network traffic and detecting intrusions;
   c. auditing the ICT assets of Scentia;
   d. aggregating activity and usage patterns;
   e. investigating and repairing system malfunctions;
   f. policy and procedure compliance.

3.4 Reporting Security Incidents or Potential Breaches

1. Students must immediately report to the Student Support Team any ICT security incidents including but not limited to:

   a. suspicion their myAIM, myABS or myACHW account has been accessed by someone else;
   b. unauthorised access to a secure area by a third party;
   c. illegal material accessed on Scentia ICT Services; or
   d. communication with sensitive information.

2. Students must immediately report any suspected breach of the Use of ICT Services policy or this procedure, to the Student Support Team.

3. Where there is an allegation of non-compliance and the Head of Technology considers it necessary to act immediately to prevent the business from being disrupted, the Head of Technology (or delegate) may:

   a. remove or disable a student's access to a Scentia location and/or
   b. restrict or remove a student's access to Scentia's ICT services pending further investigation, disciplinary and/or judicial action.

4. The Head of Technology (or delegate) will inform the student of any action in writing within ten (10) working days of the action being taken.

3.5 Failure to comply with this procedure

Failure to comply with this procedure will be dealt with the *Student Code of Conduct* Policy.

4.0 DEFINITIONS

- **myAIM -** Learning Management System for students enrolled in the Australian Institute of Management Education and Training (AIM) Registered Training Organisation (RTO) offering vocational education and training (VET) courses

- **myABS** - Learning Management System for students enrolled in the Australian Business School (ABS), a higher education provider

- **myACHW** - Learning Management System for students enrolled in the Australasian College of Health and Wellness (ACHW) , a higher education provider

- **ICT Services**– Any information, communications technology or audio-visual service, equipment or facility owned leased or contracted by the Scentia group that hosts, stores, transmits or presents digital information for the business and purpose of Scentia. This may include, but is not limited to:

  - messaging and collaboration applications;
  - any cloud-based facilities associated with the delivery of ICT activities;
  - all hardware and infrastructure (e.g., servers, workstations, voice and data network, wired and wireless networks, audio visual equipment, printers, and portable storage devices);
  - videoconferencing and web conferencing systems, services and applications; and
  - all software and applications, and services (including but not limited to internet access), and data contained or stored in any ICT facility.

- **Data** – individual facts or items of content, including symbolic representations that may form the basis of information (e.g., a date, a name, a number).

- **Information** – a collection of data in any form, which may be transmitted, manipulated, and stored, and to which meaning has been attributed. Information may include, but is not limited to: a written document, an electronic document, a webpage, an email, a spreadsheet, a photograph, a database, a drawing, a plan, a video, an audio recording, a label or anything whatsoever on which is marked any words, figures, letters or symbols which are capable of carrying a definite meaning to one or more persons or information systems.

- **File Share** - centrally provided disk space for organisational units, projects and other groups to facilitate storage, sharing and protection of electronic material associated with work activities.

- **Spam** - Spam is irrelevant or unsolicited (unwanted) messages sent over the internet often in the form of emails, typically to a large number of users, for the purposes of advertising, phishing, spreading malware, etc.

5.0 REFERENCES AND ASSOCIATED INFORMATION

- Social Media Policy (Staff and Students)
- Staff Use of Information and Communication Technology Services Policy
- Information Management Policy and Procedure
- Information Cyber Security Policy and Procedure
- Student Code of Conduct
- Privacy of Student Information and Records Policy and Procedure
- Crimes Act 1914 (Cth Australia)
- Cybercrime Act 2001 (Cth Australia)
- Copyright Act 1968 (Cth Australia)
- SPAM Act 2003 (Cth Australia)
- Privacy and Personal Information Protection Act 1998 (NSW)

6.0 POLICY/PROCEDURE OWNERSHIP

Policy Owner	Head of Technology
Status	New
Approval Authority	Scentia Corporate Board with endorsement of the ABS Corporate Board and ACHW Corporate Board.
Date of Approval	26/04/2023
Effective Date	01/05/2023
Implementation Owner	Head of Technology
Maintenance Owner	Head of Compliance
Review Due	1 April 2025
Content Enquiries	Mike Kumar- Head of Technology Email: mkumar@scentia.com.au

7.0 AMENDMENTS

Version	Amendment Approval (Date)	Amendment Made By (Position)	Amendment Details
C31.0-P31.0	26 April 2023	Head of Technology	New Procedure