Ara Code of Conduct for ICT Users

1 Acceptable Use of ICT Systems at Ara

The Ara ICT facilities will be used only for ethical, authorised, lawful purposes.

1.1 The types of activities that staff and students are encouraged to participate in and considered acceptable practice when using ICT systems include:

a Communication and sharing non-restricted information

b Internet access for research or professional and educational development related to one's position or study at Ara

c Broadening knowledge of the education sector, learning outcomes and applicable news within the context of an individual's assigned responsibilities

d Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities

e Reasonable use of computing facilities for personal correspondence, e.g. sending personal emails, and using internet web sites so long as it does not interfere with staff productivity or consume sustained high-volume traffic

1.2 Users Will:

a Comply with all applicable copyright, intellectual property and software license agreements. Particularly of note is The Copyright (Infringing File Sharing) Amendment Act 2011 which specifically prohibits BitTorrent technology for unlicensed material.

b Respect copyright and intellectual property rights of all Ara teaching materials, including those disseminated via eLearning/mLearning/flexible and/ or distance delivery.

c Respect the privacy of others. This includes (but is not limited to) confidentiality of email, files, data and transmissions. Staff must take necessary precautions to protect the confidentiality of personal or confidential information encountered in the performance of their duties.

d Conduct themselves in a professional and respectful manner

e Use only those facilities for which they have authorisation, whether these facilities are at Ara or at any other location accessible through a network.

f Inform the ICT Service Desk when ICT faults occur, so they can be appropriately dealt with.

g Change passwords regularly in accordance with the Ara ICT Security Policy.

h Ensure all access codes, account numbers, passwords, or other authorisation that have been assigned to them are kept confidential and never shared with others.

i Take due care when using Ara ICT equipment. This includes, but is not limited to:

i Taking all reasonable steps to prevent physical damage (including from foodstuffs or liquid)

ii Ensuring physical security of any ICT device provided to an individual including Laptops, Mobile phones, Projectors etc.

j Ensure that all Ara related files are stored appropriately in an Ara managed storage environment (this does not include local desktop or laptop Hard Drives).

k When sharing information containing personally identifiable records, reasonable steps be taken to ensure that only the intended recipient receives the communication.

l Use of personal cloud services must comply with the ICT Assets and Media standards – reference 4.1 which prohibits the use of personal cloud-based storage and email services for storage and dissemination of Institution documents and communications. E.g., gmail, dropbox, personal OneDrive and google drive should not be used for institutional operations.

m Ensure responsible use of AI services.

i. GenAI tools can consume data from inputs, which could then be used in the tool's responses for others. To help ensure that we do not risk sharing sensitive information, Microsoft Copilot is our only approved GenAI tool for use with institutional information.

ii. AI outputs must be reviewed, by the user, for quality. Consideration needs to be given to ethics, bias, hallucination and audience appropriate exposure of data.

1.3 Staff BYOD:

a Ara staff connecting to Ara approved cloud applications from personal devices will be subject to policies that enable the business to protect the data within. This may include but not be limited to requiring pin numbers or biometric protection, application or device encryption, remote wipe capabilities, data destruction of work information on non-connection time frames and application function restrictions. These functions will require the installation of a management agent and no access will be provided without this agent.

2 Un-acceptable Use of ICT Systems at Ara

2.1 Users are responsible for using the ICT facilities in an ethical, lawful manner. Unacceptable use includes but is not limited to:

a Use of ICT services for illegal or unlawful purposes. This includes, but is not limited to: intentional copyright infringement, software license infringements, obscenity, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation and computer tampering (e.g. spreading computer viruses or destruction of data owned by others).

b Intentionally using ICT services to visit internet sites that contain obscene, pornographic, hateful or other objectionable material, unless explicitly authorised by the ICT Director.

c Attempting to obtain unauthorised access to any other computer system or data stored in a computer system or probing the security mechanisms at Ara or another organisation.

d Using ICT services to reveal or publicise restricted or proprietary information which includes, but is not limited to financial information, new product ideas, intellectual property, academic strategies and plans, databases and the information contained therein, student details, academic product information, computer software and code, computer network and access details and business relationships

This includes input of these types of information into unapproved AI tools.

e Use of the ICT equipment at Ara for any unauthorised commercial purposes unrelated to Ara operations.

f Unauthorised distributed computing applications E.g. – Mining activities, tor network bridges and hosts.

g Configuring, deploying or installing any remote access software onto any ICT computer system unless explicitly authorised by the ICT Director.

h The storage of Ara corporate data on staff personal devices is prohibited. Ara data that has been synced to these devices may be remotely wiped when an individual leaves the organisation.

i Staff sharing OneDrive, SharePoint or Teams files and sites to their personal cloud accounts is prohibited, e.g. using Microsoft 365 sharing OneDrive files to their personal Gmail account.

j Staff emailing Ara documents and information to their personal email accounts is prohibited.

2.2 Prohibited activities include, but are not limited to:

a Destruction or alteration of data owned by others

b Interference with legitimate access to ICT facilities

c Harassment of other users

d Intentional damage

e Disabling other people's computers

f Compromising security

g Disabling or corrupting software systems

h Destroying, altering, or compromising information integrity (e.g. student records, personnel information)

i Email spamming

j Sending of threatening or intimidating email or social media postings

k Service attacks (e.g. making it difficult or impossible for others to use the network effectively and efficiently)

l Initiating or passing on computer chain letters or electronic junk mail

m Maltreating hardware

n Interfering with hardware (this includes printer and video settings)

o Accessing pornographic material or any other objectionable material from or to any Ara computing system

p sharing any authentication information E.g., user and password details written and in plain sight

q logging on to a computer with your own authentication details for someone other than yourself to use. This specifically includes multiple logins of a staff ID to facilitate student access in a learning space as well as sharing user access with any other person.

r Any and all forms of crypto currency mining.

s Installing any VPN, backdoor or any other remote access software.

2.3 Recreational Use:

a **Students:** Recreational use of ICT facilities by students is supported within operational, legal and ethical standards outlined in this document. This use is however limited to facilities not required for legitimate study or Ara sponsored activities on a case-by-case basis. In practice this means that any user engaging in such recreational use may be asked to make those facilities immediately available to another party with teaching and learning or other Ara related needs.

b **Staff:** Reasonable use of ICT facilities for personal use is supported such as correspondence e.g. sending personal emails and using internet web sites so long as it does not interfere with staff productivity or consume sustained high-volume traffic.

2.4 **Privacy:** Users of Ara ICT facilities have a right to a reasonable expectation of privacy; however, system failures or design faults may compromise this. Users should also recognise that authorised Ara personnel may have access to personal data and software stored on Ara ICT facilities while performing routine operations or pursuing system problems. As specified in the relevant administrative policies at Ara, authorised Ara personnel are obligated to take reasonable and appropriate steps to ensure the integrity of the computing facilities and to ensure that this Code is observed.

2.5 **Student Charges:** There will be charges for Student printer usage. These will be detailed in the student handbook. Students are responsible for all print charges associated to their user ID.

2.6 **Penalties for Breach of the Code of Conduct**: Violation of this Code of Conduct is classified as 'unacceptable behaviour' (refer 'Student Rights and Responsibilities' policy and 'Code of Professional Practice' staff policy). Complaints about the misuse of Ara computing facilities may be referred to the staff member's Director and in the case of a student to the Head of Department or Programme, ICT Director or ICT Service Desk Manager.

a **Students:** Serious or repeated infringement of this Code may lead to student probation, suspension, or cancellation/refusal of current or future enrolments, as set out in the relevant policy.

b **Staff:** Infringement by staff may lead to suspension of access to computing facilities/services or referral to the HR Manager for action.