Electronic Publishing and Resource Use Policy

Fact box

- **Policy owner:** Chief Information Officer
- **Policy category:** Management: IT
- **Policy status:** Approved
- **Approval body:** Executive
- **Endorsement body:** Executive
- **Related policies:**
  - Accessibility and Disability Policy
- **Defined terms:** CIO.
- **Last amended:** 20th Dec. 2022
- **Relevant HESF:**

Purpose

This policy outlines guidelines and procedures for the appropriate publishing and use of Alphacrucis University College (AC) electronic resources, as well as the rights and responsibilities of users.

Scope

All campuses
All users of AC electronic resources

Policy

In support of academic instruction, research, public service, and administrative functions, AC encourages the use of, and provides access to, information technologies and network resources for the conduct of official AC business and for individual professional purposes related to an official AC purpose.

This policy governs the acceptable use of AC ICT resources with respect to: provision of resources; access to resources; responsible, ethical, equitable and legal use of resources; security and privacy; compliance, breaches and responsibilities. Users are responsible for using resources in accordance with the law and with AC policy.

DEFINITIONS

Account/ AC Sign-In - access provided by AC to any ICT resource or any non-AC ICT resource utilised for AC purposes.

ICT - Information Communication Technology products and services, including all types of technology and associated resources which relate to the capture, storage, retrieval, transfer, communication or dissemination of information through the use of electronic media. This includes, but is not limited to, computers, computing staff, hardware, software, networks, computing laboratories, classroom and lecture recording equipment, web-based systems, databases, files, information, software licenses, computing-related contracts, network bandwidth, usernames, passwords, documentation, disks, CD-ROMs, DVDs, magnetic tapes, USB storage, and electronic mail.

User - all staff, students, contractors, visiting faculty, third parties, volunteers, affiliates, alumni and all other people who legitimately access and use computing resources, information technologies and networks owned or managed by AC.

Other Entities - External organisations which may provide cloud solutions (e.g. Microsoft, Amazon Web Services) and host services such as Turnitin.

FREEDOM OF EXPRESSION

AC respects the rights of students and staff to freedom of speech, including academic freedom of artists and scholars. Therefore, AC does not restrict the contents of electronic mail of staff, faculty, and students or the contents of faculty, staff, and student individual web pages, including contents on social media, linked to the official AC web pages beyond the restrictions inherent in complying with the law, AC Code of Conduct and community behavioural expectations.

Individual web pages are the responsibility of their developers. These represent the work of the individual artists, scholars, and authors who created them and not AC. All such pages are required to contain an appropriate disclaimer indicating that AC is not responsible for the creation of, or the content of, these web pages. AC reserves the right to remove from any AC server a web page or resource that is found to be in violation of the law or AC policies.

In general, electronic publications for the purposes of promoting AC are subject to the same AC policies and standards as print publications, and are subject to the discretion of the Director of Marketing.

AUTHORISED AND APPROPRIATE USE

Express permission is required from the Chief Information Officer (CIO) or nominated representative for the following:

- installation of any software on any computer owned or operated by AC;
- removal of AC software from any computer in the network;
- alteration or amendment of settings for AC computer hardware and software.

The CIO or delegated representative will virus check all software using standard testing procedures before being used.

Every user undertakes to indemnify AC against loss, costs or damage that may occur from illegal or improper actions they have performed.

The computer and electronic equipment belonging to AC may not be tampered with, removed or modified in any way except by official AC IT staff or agents engaged by AC for this purpose.

AC makes no warranties of any kind, whether expressed or implied, for the provision of electronic services and will not be responsible for any damage or loss suffered through the use of this system. Damages may include but not be limited to loss of data, non-deliveries, misdeliveries or service interruptions, or errors or omissions by any user. The use of any information obtained by this system is at the personal risk of the user. AC specifically denies any responsibility for the accuracy or application of any information obtained through its services.

Appropriate Use

Only authorised users are permitted access to AC's ICT resources. AC requires all users of its ICT resources to do so in a responsible, ethical, equitable and legal manner and in accordance with the AC Code of Conduct and standards of communication. Legitimate AC purposes include:

- work related to AC courses of study;
- all work directly related to instruction, research, and scholarly, professional, and administrative endeavours related to AC activities;
- adherence to all Australian laws, AC policies and Code of Conduct. This includes, but is not limited to, areas such as copyright, breach of confidence, defamation, privacy, contempt of court, bullying and cyber-bullying, harassment, vilification, anti-discrimination, wilful damage and computer hacking;
- advertising or use of AC logos on web pages with approval from AC Head of Department;
- compliance with relevant copyright legislation.

AC staff may use AC electronic mail system to send personal messages, provided that such messages are insignificant in cost and resource usage, and provided that all such messages comply with the statements in this policy.

Staff members should be aware that offers or contracts transmitted by AC's electronic mail system are as legally binding on AC as those sent on paper.

Inappropriate Use

AC computer resources, information technologies, and networks shall not be used for:

- supporting, establishing, or conducting any private business operation or commercial activity;
- personal activities unrelated to AC;
- attempting to gain unauthorised access to any portion of the system or access to any other unauthorised system or account;
- violating any laws or AC policies and procedures, including the AC Code of Conduct and commitment to protection against discrimination, harassment and bullying, vilification and victimisation, sexual misconduct, and other wrongful, unlawful or inappropriate conduct;
- intentionally disseminating, accessing, or providing a hyperlink to obscenity, as that term is defined by the law, unless such activities are directly related to an employee's legitimate research or scholarship purpose or to a student's completion of an academic requirement;
- sending unsolicited electronic mail (e.g., "spam") in violation of Australian law or in quantities that interfere with AC or other servers, and/or without approval by the appropriate server administrator;
- sending fraudulent or misleading information via AC networks or electronic resources;
- destroying, altering, compromising the integrity or security, or making inaccessible AC computer resources, information technologies, and networks when such uses are not authorised;

- compromising the privacy of users of the computer resources, information technologies, and networks; copying of software in violation of a license;
- online gambling;
- libellous material or information detrimental to any person.

PRIVACY

AC is bound by the National Privacy Principles as set out in the Privacy Amendment (Private Sector) Act 2000. In protecting the privacy of personal and health information entrusted to it, AC will meet its statutory requirements under the Privacy and Personal Information Protection Act 1998 (PPIPA), the Health Records and Information Privacy Act 2002 (HRIPA), and the **Privacy Amendment (Notifiable Data Breaches) Act 2017**. Where relevant AC will also meet its compliance obligations with the EU General Data Protection Regulation 2016/679 (GDPR).

System users are responsible for maintaining appropriate access restrictions for their files, as well as protecting their passwords. An AC staff member or student who knowingly allows another person to use his or her username or password may be found responsible for any inappropriate use on the part of that person.

Distribution of name lists, e-mail addresses, home addresses or other means of contact must not be provided without the express permission of the persons involved. Neither shall the security codes or passwords of any other staff member or student be divulged to others.

The invasion of the privacy of any person by the use of AC equipment or services is prohibited. Notwithstanding, AC reserves the right to supervise the entire network in order to preserve the security of AC and all users.

AC respects the privacy of users and does not routinely inspect or monitor use of computing and networking resources. However, AC does not guarantee the security and privacy of any and all data created, stored, or transmitted upon its ICT systems, including any user's electronic mail and/or electronic files. Information reports will be available to AC which can subsequently be used for matters such as system performance and availability, capacity planning, cost re-distribution and the identification of areas for personal development.

Authorised AC staff may access electronic mail or files in a number of situations, such as:

- legal request for public disclosure of public records (which may include material that continues to exist on a hard drive, or on another computer);
- AC record retention requirements;
- routine system maintenance;
- AC staff who have received formal permission by the owner, or with a supervisor's approval, when that employee is unavailable for legitimate business purposes and in a manner that is consistent with any research and/or confidentiality agreements which may apply to those files;
- investigations of misconduct, consistent with all legal requirements and with the approval of the appropriate Department Head, Head of School or next-level administrator. This provision applies to monitoring of employee accounts when the monitoring is done because of suspected illegal activity or policy violations;

- monitoring of AC accounts.

Information automatically logged:

AC may make a record of all visits to AC websites and log any of the following information for statistical and business purposes - the user's address, the user's domain name, IP address, the date and time of the visit, the pages accessed and documents downloaded, the previous site visited and the type of browser used. Identification of the user may also be requested and logged. If the person is not an AC student or staff member, the email address of sent messages will be recorded.

Security information:

AC websites have security measures in place against the loss, misuse and alteration of information. Generally, a login and password are required to visit secure areas. This is to ensure that information is displayed only to the intended person. Individuals are responsible to keep their password secure at all times.

Cookies:

The computer of a visitor to AC websites may be issued with a cookie. The information the cookie contains is set by the AC server and it can be used by that server whenever the website is visited. Cookies may also be used for authentication purposes and to improve security during a visitor's session online.

External links:

Where an AC website contains a link to an external site, AC accepts no responsibility for the privacy practices or the content of such websites.

Public forums:

Some AC courses and/or units require the use of forums, on-line teaching environments, message boards and/or news groups. Any information that is disclosed in these areas becomes public information and it is the responsibility of the user to exercise caution when deciding to disclose personal information.

STORING STUDENT RECORDS

AC maintains proper records of student information by storing all information in a central system. All student records and files are managed by the Student Experience Department. The Student Experience Department is responsible for ensuring the safety, accuracy and orderliness of records, and protecting the privacy of all personal information kept therein. Electronic storage is password protected and hard copy information is filed securely. The CIO is responsible for protecting against the loss of electronic student records by ensuring appropriate backup of data.

There is only one file for each student of AC. These files are kept in a secure location and can only be accessed by authorised personnel. That is, relevant AC academic and administrative staff.

Student files are archived at the AC Sydney campus in Parramatta.

Students can access their personal information by making this request to the Student Experience Department. Students can request to have incorrect personal information corrected by contacting the Student Experience Department and providing documentation to support the change.

Students are provided with accurate information about the use and disclosure of their student records, which includes the disclosure of information to external parties, such as the Commonwealth, tuition assurance scheme operators and accreditation bodies.

STORING RESEARCH DATA & INFORMATION

In accordance with the Australian Code for the Responsible Conduct of Research, Research Data (broadly defined as progressive or final data/information gathered in the course of formal research activities by AC staff and students) requires special protection to guard from accidental or malicious manipulation or loss. AC will implement specific, risk-based protections for this data/information, including regular testing of retrieval and retention for at least five years.

Responsible for implementation

Chief Information Officer
Department Heads

Key stakeholders

All users of AC electronic resources

Related documents

Data Privacy Guidelines

Procedures

Electronic Publishing and Resource Use Procedure

NOTIFYING AND HANDLING OF BREACHES

Users who become aware of possible breaches of this policy must report it to either:

- their supervisor or manager;
- their Head of Department or School; or
- Chief Information Officer (CIO)

The CIO is responsible in the first instance for handling potential breaches for Users other than students or staff. This could result in revocation of access.

Formal disciplinary action for staff and/or students will occur in accordance with AC misconduct policies. AC will report illegal activities and corrupt conduct to appropriate authorities.

Penalties for misuse of ICT resources may range from loss or restriction of access to accounts, to formal disciplinary action up to and including dismissal, or in some more serious instances criminal or civil proceedings.
