Acceptable IT Usage Policy – Information Resources

Policy Code: IT-001 **Version:** 13.0 **Effective Date:** 12 August 2020

Purpose

Information Technology (IT) resources are essential for accomplishing the College's vision. Members of the College community are provided with shared access to these resources, which must be used and managed responsibly to ensure their integrity, security and availability for appropriate educational and business activities. This Acceptable IT Usage Policy provides guidance to authorised users on the appropriate use of the College information technology resources.

Definition of "College" – *The Australian College of Natural Medicine Pty Ltd (ACNM) trades as Endeavour College of Natural Health and FIAFitnation. For the purpose of this policy, any reference to 'College' or 'the College' should be considered a reference to each or any of these respective trading names / entities.*

Scope

- All College staff, students, contract academics, honorary appointees, contractors and guest / visitors of the College plus any authorised users or organisations accessing the College IT resources (collectively referred to as 'Users')

Policy Statement

Within this policy, IT resources include all computers, electronic communication devices and software owned or leased by the College, and network facilities which link technology within the College and which provide external access and communication such as the internet and email.

The policy applies to all personal devices with access to the network, however personal devices are not to be used for work purposes unless approved by senior management.

All Users of the College IT resources, including those who install, develop, maintain, administer and access those systems and applications, irrespective of where College IT resources are accessed and used, and includes use at home.

This policy is intended to operate within, and be consistent with relevant legislation and Federal laws, the College policies and procedures including, but not limited to, areas such as sexual harassment, discrimination, equal opportunity, freedom of information, copyright, defamation, and conduct. It is intended to encourage responsible action and good judgement and to protect privacy.

In the event of a breach of this policy or inappropriate use of the IT resources provided by the College, suspension, termination of employment, legal action, or other disciplinary action may occur, in line with the *Performance Management Procedure*.

1. User Responsibilities

Users must familiarise themselves with rules governing the use of the College's IT resources and systems.

The IT department, Managers and Human Resources should also ensure Users are made aware of the rules governing the use of the College IT resources and have them acknowledge this by signing, or otherwise acknowledging, that they will carry out their responsibilities under these rules.

Users learning of any violation of any of this policy must bring this matter to the attention of their immediate manager or supervisor without delay. All students are required to sign an *Acceptable Student Usage of IT Agreement Form*.

2. Authorised Access

2.1 Users may only make use of equipment, software networks or information for which proper authorisation has been given. In the case of staff, authorisation must be obtained from the person or unit responsible for the facility (e.g. Director or nominee). In the case of students, authorisation occurs automatically upon enrolment at the College.

2.2 Users are responsible for ensuring that passwords, accounts, software and data are adequately secured and that passwords / access codes are not shared. Users will be held responsible for all activities, which originate from their use of the account. To ensure the security of systems, a secure password should be selected in line with these guidelines:

- 2.2.1 User accounts must have passwords
- 2.2.2 Passwords for accounts must not be shared, unless a group account has been specifically authorised in writing
- 2.2.3 Passwords for user accounts have a pre-determined life (e.g. an expiration date of 30 days) as imposed by the IT department
- 2.2.4 To minimise the chance of passwords being discovered, they must use a mix of alpha and numeric characters and, where possible, contain at least 6 characters
- 2.2.5 Passwords to computer and network resources containing computerised College data will not be issued over network media in clear text unless a secondary means of authentication is provided (e.g. smart cards).
- 2.2.6 In the event a User suspects that another User has gained unauthorised access to their account, the IT department must be notified immediately
- 2.2.7 Users must not use any means, electronic or otherwise, to discover others' passwords

2.3 Sharing or obtaining passwords inappropriately is a breach of this policy and may result in disciplinary action.

2.4 Students are permitted only to use student resources available within the College such as computers in the student labs and student wireless networks. Under no circumstances are students permitted to use staff or Contract Academics' computers without prior authorisation and direct supervision by a person able to give authorisation (e.g. Director or nominee). Contract Academics are permitted to use shared resources in the computer labs, e.g. library. Employees are permitted to use any and all available and authorised resources to undertake their duties.

3. Responsible Use of Resources

3.1 Internet and email services can only be used for:

- 3.1.1 College purposes
- 3.1.2 Limited personal use

3.2 College purposes includes any activity that is conducted for purposes of accomplishing College business related to research, teaching and learning, course of study, College administrative activities, and professional development.

3.3 In the spirit of abundancy and in line with other organisational values, limited personal use is allowed. This is use that is infrequent and brief and should be structured to occur during personal time such as lunch breaks. This should not include uses:

3.3.1 that require substantial expenditure of time

3.3.2 that are for private business, personal gain or profit

3.3.3 that support political campaigns, candidates, legislation or ballot issues

3.3.4 that contain inappropriate content/materials

3.3.5 that impede the efficiency of intranet, internet or email services

3.3.6 that clog mailboxes with large numbers of messages

3.3.7 that waste College resources, such as playing games or social media activities (e.g. Facebook, Instagram, Twitter, etc.)

3.3.8 that would violate or breach the College's *Employee and Contractor Code of Conduct* or the *Acceptable IT Usage Policy - Information Resources*

3.3.9 that would violate or breach any State or Federal legislation

3.3.10 that would violate or breach any the College policies, regulations or harm the College image or reputation

3.4 As a guide, use that occurs more than a few times per day and/or periods longer than a few minutes would exceed what is considered personal use.

3.5 College electronic mailing lists and distribution lists should be used for business purposes only. It is inappropriate to:

3.5.1 mass email messages of a commercial, political, lobbying or fundraising nature

3.5.2 forward chain letters or electronic "petitions", or to ask recipients to forward messages

3.5.3 'Reply to All' unless it is essential all recipients see the reply

3.5.4 send anonymous mailings

3.5.5 solicit support (financial or otherwise) for charity, or special causes not connected with the College effort

3.5.6 send unverified public service announcements (such as virus alerts, unsafe products, lost and found, etc.)

3.5.7 A message sent to the College electronic mailing list must be relevant to the membership of the list.

3.6 College work should not be sent to personal email addresses. If work needs to be accessed offsite, a secure drop box will be created by the IT department.

3.7 Users should not use the College network, whether at a College campus or another site including at home, to access inappropriate Internet sites. Inappropriate Internet sites include, but are not limited to:

3.7.1 sites that are illegal or hold illegal content

3.7.2 sites that are pornographic or contain inappropriate sexual material

3.7.3 sites that advocate hate or violence

3.7.4 sites that offer games, gambling or software that are unrelated to academic programs.

3.8 Users must not download, distribute, store or display offensive or pornographic graphics, images or statements or other material obtained from inappropriate Internet sites.

3.9 Users must not download, distribute, store or display material that could cause offence to others, for example offensive material based on gender, ethnicity and political beliefs.

3.10 Users must not attempt to email "spoof", i.e. construct electronic communication so it appears to be from someone else.

3.11 Accessing inappropriate sites is considered serious misconduct and may result in disciplinary action up to and including termination of employment.

3.12 Where representing the views of the College, prior approval must be obtained from the office of the CEO, and the communication must identify the user's position within the College. Where the view expressed is the 'official' College view, the authorised source and author of that view should be identified.

3.13 Users must not express views on behalf of the College without prior and official authorisation from the office of the CEO to do so, or to allow another person to reasonably misconstrue that a personal view represents the official position of the College. In circumstances where readers might reasonably conclude a personal view is representative of the College, the user must clearly state that the opinion expressed is that of the writer and not necessarily that of the College, or words to that effect.

3.14 The College logos and designs are the property of the College and may only be used for approved College documents.

3.15 Users must take reasonable steps to ensure physical protection including damage from improper use, food and drink spillage, electrical power management, anti-static measures, protection from theft, and sound magnetic media practices.

3.16 Ensure computers are not left unattended without first locking the systems and/or securing the entrance to the work area – particularly if the computer system to which they are connected contains sensitive or valuable information.

3.17 Users must ensure resources are at all times physically secure including during travel keeping items in safe and secure areas or not leaving them unattended.

3.18 Users must not install software or hardware, or change the standard PC configuration in any way without the express permission of the Director IT, or authorised nominee.

3.19 The installation and use of personal networks including wireless networks is prohibited. Network access is to remain wired within the College via the provided wireless network unless authorised by the Director IT.

3.20 The use of peer to peer software (including, but not limited to, Limewire, BitTorrent, Azureus, Kazaa, etc.) for downloading is specifically prohibited.

3.21 Portable methods of storage, such as USB Drives and portable hard disks are permitted for use but must not be used to copy/use information considered as confidential or College intellectual property for personal use. However, users are encouraged to create a file on the device that stores personal identification (student / staff ID, first name, surname, email address) in order to identify the owner of the device should it be lost.

3.22 The College accepts no responsibility for the loss or damage of any portable storage medium. Should the device be lost on College premises then handed in, attempts will be made to identify and contact the owner.

3.23 Hardware remains the property of the College. On cessation of employment/association, all College hardware must be returned in a clean, tidy, working and prompt fashion. The College notebooks and desktop computers are issued for use by the College staff only. Notebooks and accessible College resources (e.g. internet access) are not provided for non-College staff members to use (i.e. friends, family etc.).

3.24 Where possible, hardware shall be purchased from the College's preferred suppliers. Where this is not possible, hardware shall be purchased in Australia to ensure that any warranty is easily claimable.

3.25 Software remains the property of the College. On cessation of employment / association, all College software must be returned in a prompt fashion. Failure to comply may result in Users being held personally responsible for any data loss or penalties imposed for breach of copyright.

3.26 All software purchases must go through the IT Department. This is to ensure that:

- 3.26.1 Software is correctly added to the asset register upon purchase and receipt
- 3.26.2 Software is allocated against the asset in the database
- 3.26.3 Audits of software on computers can occur against a reliable account of owned software
- 3.26.4 Site licence price savings can be achieved through a coordinated approach to purchasing software
- 3.26.5 Upgrades of software can occur, generally business wide, to ensure minimum confusion between versions
- 3.26.6 Areas are not disadvantaged by not having access to upgraded software if appropriate/suitable for position and hardware
- 3.26.7 All instances of licence documentation, software media and copies of delegation/invoice details for the software are held and accounted for.

4. Mobile Devices

The College provides mobile phones and other mobile devices to nominated staff to facilitate business communications. The College accepts that a small proportion of calls may be for reasonable private use (for example contacting family members) and reserves the right to recover costs that are deemed to be excessive or unsuitable. This includes costs associated with data transmission and internet usage.

The College will ensure that:

4.1 There is a genuine business need for an individual to be allocated a mobile device prior to its allocation.

4.2 The staff member provides a written authorisation for any deduction in the event that the equipment is not returned in good order upon termination of employment.

The staff member is responsible for the proper use, care and maintenance of College mobile devices and must:

4.3 Not use the device for any unlawful activity, personal financial gain or for commercial purposes outside of College operations unless authorised.

4.4 Keep private use to a minimum and restrict mobile calls to local and mobile – mobile numbers only.

4.5 Fully reimburse the College for the cost of any private International Direct Dial (IDD) calls made within Australia, or made to Australia when travelling overseas.

4.6 Report any faults, damage, theft or loss to mobile devices immediately to the line manager and IT department in order for a replacement to be ordered and the service provider notified.

4.7 Not use mobile devices whilst driving unless secured in a commercially designed holder fixed to the vehicle OR not touch any part of the phone whilst driving. All state law must be adhered to at all times.

4.8 Pay any fine incurred when using a mobile device whilst driving.

4.9 Return the mobile device in good working order on the cessation of their employment with the College or when the device is no longer applicable to the position held by the staff member.

Further details of staff responsibilities when issued with a College mobile device can be found in the *Mobile Device Usage Policy*.

5. Respect for Other Users of Resources

Successful use of College IT resources depends upon a spirit of mutual respect and co-operation to ensure that everyone has equitable privileges, privacy and protection from interference or harassment.

To this end:

5.1 Users must respect the privacy of other users and thus not intentionally seek information on, obtain copies of, or modify files, tapes, passwords or any type of data belonging to other Users unless specifically authorised to do so.

5.2 Users must not intentionally disrupt or damage the academic, research, administrative, or related pursuits of others.

5.3 Users must not use e-mail, discussion forums or web pages under their control, to provide or communicate obscene materials, or that threatens, harasses, intimidate or single-out individuals or groups for degradation or harassment in violation of federal or state law, and other College policies and regulations.

- 5.3.1 All activity must be factual, consistent, respectful and in line with the College's organisational values and any need for confidentiality.
- 5.3.2 Any identifiable and inappropriate activity that connects an individual to their employment with the College and has an impact of the College, it's interests and reputation may result in disciplinary action.
- 5.3.3 If activity is considered defamatory it may result in disciplinary action, a defamatory claim and personal liability considerations.

5.4 Users must not display on screens images, sounds or messages, which could create an atmosphere of discomfort or harassment to others.

5.5 Users must not knowingly create or propagate a virus, worm or any other form of malicious software.

5.6 Users must not tamper with hardware components or hardware configurations without the express permission of the person/s responsible for that particular item of equipment. This includes:

- 5.6.1 workstation, monitor, keyboard and mouse
- 5.6.2 printers and other peripherals
- 5.6.3 network outlets, cabling and other components
- 5.6.4 phones
- 5.6.5 any part of a lab or other installation used by the general population of the College

5.7 Users must respect the integrity of the system and not use College resources to develop or execute programs that could infiltrate the system, tamper with or attempt to subvert security provisions, or damage or alter the software components of the system. This also applies to systems maintained by others outside of the College that users access electronically or physically.

6. Privacy

The College network, systems and facilities are the property of the College. Anything sent or received using the network, systems and facilities of the College are to remain the property of the College and will therefore be transmitted and stored on College property.

Accordingly use will regularly be reviewed by the College on an ongoing basis. This applies whether Users use the College resources at a College campus, at home, or any other location.

6.1 The College therefore reserves the right to monitor and conduct audits on both usage and content of email messages, discussion forums and visits to Internet sites using College resources to:

- 6.1.1 Identify inappropriate use
- 6.1.2 Protect system security
- 6.1.3 Maintain system performance
- 6.1.4 Protect the rights and property of the College
- 6.1.5 Determine compliance with policy and state and federal legislation.

6.2 The College also reserves the right to monitor, audit and record network traffic including:

- 6.2.1 email and internet sites accessed
- 6.2.2 usage data such as account names, source and destination accounts and sites
- 6.2.3 dates and times of transmission or access
- 6.2.4 size of transmitted material
- 6.2.5 other usage related data.

This continuous and ongoing surveillance is conducted by the IT department through various monitoring software and programs and the information is used for accounting purposes, troubleshooting and systems management and to monitor appropriate usage.

6.3 The College reserves the right to inspect, copy, store and disclose the contents of the electronic communications of its employees and other authorised Users (e.g. students), for the purposes of conducting an audit, identifying inappropriate use (upon receiving a complaint, investigation request or allegation of misuse, and following authorisation from the appropriate College managers, the Police or other law enforcement agencies) and to assist in the investigation of an offence. The contents of electronic communications, properly obtained for legitimate business purposes, may be disclosed without permission of the employee or authorised user.

6.4 Monitoring, inspection and auditing can apply to personal and business use of intranet or internet services and personal and business related email messages.

6.5 Users should always assume that everything sent by e-mail, posted to a newsgroup or posted via a web site is in the public domain and might be read by people other than expected recipients. Any email messages, whether personal or business, may be accessed as ‘documents’ under the Freedom of Information Act and may also be tendered in court as evidence, in line with this policy.

6.6 Users should be aware that Internet content can remain available, even after deletion for a significant period of time, perhaps indefinitely.

6.7 The College may use and disclose an employee’s social media posts where that use or disclosure is:

- 6.7.1 for a purpose related to the employment of any employee or related to the College’s business activities
- 6.7.2 use or disclosure to a law enforcement agency in connection with an offence
- 6.7.3 use or disclosure in connection with legal proceedings

6.7.4 use or disclosure reasonably believed to be necessary to avert an imminent threat of serious violence to any person or substantial damage to property.

Users should always assume that any website visited will at least know the Internet address being used and that the same is true for email that is sent.

7. Copyright Compliance

7.1 The Copyright Act sets out the exclusive rights of copyright owners and the rights of Users. In addition, certain uses may be covered by licence agreements to which the College is party.

7.2 It is illegal to place on a Web page any pictures or videos of people without the permission of the people in the picture or video and / or the copyright owner.

7.3 Software programs are protected by the Copyright Act. Users do not have the right to make and distribute copies of programs without specific permission of the copyright holder.

8. Confidential Information

Authorised Users have a duty to keep confidential both during the course of employment and following:

8.1 All College data unless the information has been approved for external publication; and

8.2 Information provided in confidence to the College by other entities.

Each staff member is under a duty not to disclose the College business information unless authorised to do so. Breach of confidentiality through accidental or negligent disclosure may expose a User to disciplinary action.

Company and/or sensitive information includes, and will include, all trade and business secrets and other confidential information and documents relating to the affairs or business of the College or any person with whom Users come into contact as a result of their employment or study with the College or who may come into the User's possession in the course and by reason of their employment or studies, whether or not the same were originally supplied by the College.

Please note that under no circumstances can confidential information be taken off site without prior written authorisation from relevant manager. Breach of this condition may result in disciplinary action which may include termination of employment.

Confidential information includes any information (written or verbal) of a commercial, technical or financial type which is not publicly available. Users must not make unauthorised copies of any material (original or not) such as correspondence, company manuals, computer printouts, customer lists, diaries, file notes or any other material, whether or not compiled or made by the User, or to which the User has access as part of their employment. All such material is and remains the property of the College. All the College property must be returned upon termination of employment.

9. What happens if Users don't act responsibly?

9.1 The College considers any breach of a User's responsibilities to be a serious offence and reserves the right to copy and examine files or information resident on or transmitted via the College IT resources. Students deemed to be in breach of the above principles or guidelines are subject to disciplinary action, which may include suspension or expulsion. Staff deemed to be in breach of these principles or guidelines are subject to disciplinary action up to and including termination of employment. Severe staff breaches, such as accessing

pornographic material, will result in instant termination of employment. Offenders may also be prosecuted under State, Federal and International laws.

The College reserves the right to temporary or permanently remove material from web sites, close or suspend any account that is endangering the running of the system or that is being reviewed for inappropriate or illegal use. Users' access will be terminated on cessation of employment.

Definitions

User - a User is a person, organisation, or other entity that employs the services provided by a telecommunication system, or by an information processing system, for transfer of information. In the College environment users include but are not limited to staff, lecturers and students.

Student/Learner - is an individual person who is formally enrolled to study at the College. The individual person is that who appears on the College's documents such as enrolment, admission and payment documents, and who is assigned an individual student ID.

Related Procedures

Performance Management Procedure

Further Information

Related Policies

Employee and Contractor Code of Conduct

Mobile Device Usage Policy

Related Documents

Acceptable Student Usage of IT Agreement Form

Guidelines

Not Applicable

Benchmarking

Not Applicable

Supporting Research and Analysis

Australian Business Lawyers

Related Legislation

Copyright Act 1968 (Cth)

Privacy Act 1988 (Cth)

Equal Opportunity Act 1992 (QLD)

Sex Discrimination Act 1984 (Cth)

Disability Services Act 2006 (QLD)

Disability Discrimination Act 1992 (Cth)

Racial Discrimination Act 1 975 (Cth)

Classification of Publications Act 1991 (QLD)

SPAM Act 2003 (Cth) and

Other relevant Commonwealth and/or State laws such as those relating to the transmission of offensive material and Telecommunications.

Review and Approval

Policy Author

Director, Student Retention and Systems

Policy Owner

Head of Technology and PMO, Technology Services

Contact

Head of Technology and PMO, Technology Services

Ganesh.jagtap@endeavour.edu.au

Recommending Body

Chief Executive Officer

Approval Body

Chief Executive Officer

25 November 2014

Policy Status

Revised

Responsibilities for Implementation

- Head of Technology and PMO, Technology Services

Key Stakeholders

- Head of Technology and PMO, Technology Services
- National Human Resources Manager
- College staff, contractors
- College Students