EDITH COWAN COLLEGE AUSTRALIA

Internet and Digital Communications Policy

Policy Owner:	Regional IT Service Delivery Manager, SA/WA
Contact Officers:	Regional IT Service Delivery Manager, SA/WA
Policy Number:	QHRPO008
Approved by:	Senior Management Group
Date Approved:	16 February 2009
Last Reviewed:	August 2016
Related Policies:	Bullying, Harassment and Discrimination Policy Navitas Acceptable Use Policy Navitas Disciplinary Policy for Operations based in Australia Navitas IT Security User Awareness Policy Navitas Social Media Policy Privacy Policy Student Misconduct Policy
Related Documents:	Navitas Facebook Guide Navitas IT File and Folder Security Standard Navitas IT User Access Form

1. Overview

1.1 The purpose of this policy is to ensure that staff and students of ECC use ECC's Digital Communications systems in an appropriate manner. This policy is designed to ensure that the integrity of the ICT system is maintained whilst allowing appropriate management of each individual workstation and terminal.

1.2 ECC provides access to the vast information resources and facilities of the Internet to help staff and students complete tasks faster, more efficiently and to assist them in using the latest available data and technology.

1.3 The facilities represent a considerable commitment of resources in respect of telecommunications, networking, security and software – at significant costs to ECC and therefore needs to be treated accordingly.

2. Organisational Scope

2.1. This policy applies to all staff and students of ECC and its partner providers.

3. Definitions

3.1. **Digital Communications:** includes digital messages sent from one person to one or more recipients via electronic systems. In the context of this policy, it can include messages sent via email, Facebook, Twitter, LinkedIn, YouTube, social media, wikis, blogs, etc. It uses Internet as a method to enable communication and distribute information

3.2. **ICT:** Refers to Information and Communication Technologies.

3.3. **Internet:** The world-wide network linking together thousands of computer networks and many millions of users through public and private telecommunications lines; a global system of computer networks that are interconnected to deliver a range of electronic, wireless, audio-visual technologies.

4. Policy Principles

4.1. Use of Digital Communications and Internet by staff is permitted and encouraged where such use is suitable for teaching or ECC business purposes and supports the goals and objectives of ECC.

4.2. All network, Digital Communications, Email and Internet accounts maintained on ECC computing systems are the property of ECC and Navitas, and all users must comply with relevant policies and user access permissions

4.3. As stated in the *Navitas IT Acceptable Use Policy*, any user who breaches Australian legislation relating to discrimination, censorship, copyright, privacy, spam or any other related laws will be held personally liable for that breach.

4.4. Mitigation of Risk:

- Image - ECC must take care to maintain the clarity, consistency and integrity of our image and reputation. Anything an employee writes in any Digital Communication in the course of acting for ECC, could be construed as representing our position. This presents some significant risks to ECC and to staff and students.
- Legal – there is a danger that, if Digital Communications access is abused, ECC may be found to have broken the law, resulting in criminal action or civil penalties
- Cyber-attack**–** ECC takes precautions to prevent cyber-attacks (eg. hacking, identify theft, malware, phishing, spam, Trojans, spyware, viruses, etc.) of ECC systems or hardware

5. Policy Content

5.1 Access and Security

ECC's position in connection with access to, and downloading from, the Internet on ECC computers:

- Security must be a key concern for everyone. As use of the Internet and Digital Communications expands within our organisation, it is essential that you are fully aware of your responsibilities and what restrictions are placed on its use.
- This Policy is intended to clearly define the conditions of use of the Internet and Digital Communications. All employees and students authorised for Internet and/or Digital Communications access will be provided with access to this policy
- This policy will be subject to amendment in response to changing circumstances as Internet and Digital Communications facilities develop, whether operational or legislative. ECC will inform staff and students of changes.
- If you breach of any of the provisions of this Policy, then it is likely to lead to action being taken against you under the Navitas IT-related policies or the ECC Student Misconduct Policy.
- If you have any queries regarding access to the Internet and/or Digital Communications, then please contact Student and Academic Services or IT Support.

5.2 Navitas and ECC Rights

5.2.1 All use of the Internet and Digital Communications systems through ECC network connections will be monitored, logged and retained. Details are also recorded of Internet sites visited (or attempted to be visited), pages accessed, files downloaded, graphic images examined and all email correspondence.

5.2.2 If ECC have reasonable grounds for believing that you are guilty of breaching any of the rules in this Policy, ECC reserves the right to do any or all of the following:

- Monitor staff and students Digital Communications traffic
- Retrieve and consider the contents of messages sent or received by you for the purpose of determining whether the use of the Digital Communications system is legitimate, to assist in the investigations of wrongful acts, or to comply with any legal obligations
- Find lost Digital Communications or retrieve Digital Communications lost due to computer failure

5.2.3 ECC may from time to time monitor Digital Communications traffic randomly to ensure that the rules contained in this Policy are being followed. The confidentiality of any personal message seen by ECC when carrying out that monitoring exercise will be maintained unless, ECC reasonably believe that the message contains evidence that the rules in this Policy may have been breached. In that case, ECC reserve the right to use that message as part of an investigatory or disciplinary procedure.

5.3 DIGITAL COMMUNICATIONS

5.3.1 General

Messages sent on Digital Communications systems are to be written in accordance with the standards of any other form of written communication. The content and language used in the message must be consistent with our best practice.

- Always remember that staff and students' Digital Communications could be read out in court as part of court proceedings. Therefore, you should write them as carefully as if you were writing a letter. Also, you should avoid obscene or defamatory language.
- The printing or forwarding of any Digital Communications which breach any of the standards set out in this Policy will also constitute a breach of these rules.

5.3.2 Defamation and Libel

For many purposes, Digital Communications have the same effect as if they had been typed on notepaper. This means that you should never under any circumstances make derogatory comments about anyone in any Digital Communications that you send or post, whether internally or externally.

5.3.3 Harassment and Bullying

- ECC will not tolerate the use of Digital Communications systems for the harassment or bullying of any person — whether on the grounds of disability, gender, sexual orientation, marital status, race, colour, religious belief, and age, national or ethnic origins or for any other reason whatsoever. Any allegations of such harassment will be dealt with under the ECC *Bullying Harassment and Discrimination Policy*
- Harassment in this context includes sending Digital Communications to unwilling recipients.

5.3.4 Internal Digital Communications

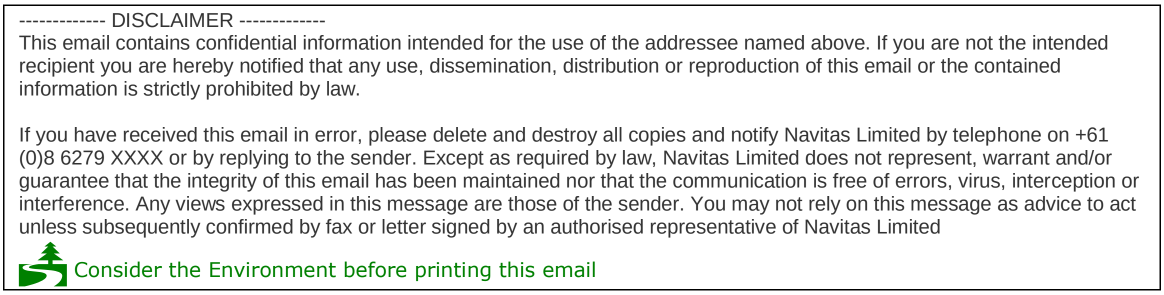
- Staff are asked to limit the distribution of comic material. Use alternatives such as the business Unit Intranet.
- Do not send materials of an offensive, obscene or malicious nature to colleagues — as staff and students risk offending others.
- Breach of this rule will be dealt with under the relevant policies.

5.3.5 Opening/Downloading Digital Communications and Attachments

- ECC needs to keep control over all Digital Communications and attachments received by ECC systems because:
  - Opening or downloading these may risk a breach of the copyright laws.
  - Digital Communications or attachments may contain viruses that could corrupt our computers and computer systems.
- To prevent these risks from happening, staff and students should never open or download any Digital Communications unless you are absolutely certain that you can verify its source.
- As a general rule, if you receive an unsolicited Digital Communications from an organisation that you do not recognise and suspect may be suspicious, you should contact IT support for guidance.
- Under no circumstances should staff or students import any programs or other software that has not first been approved in advance by IT Support and or a ECC Line Manager.

5.3.6 Sending external Emails

Whenever ECC employees send emails, the following wording will appear automatically:



------------- DISCLAIMER -------------
This email contains confidential information intended for the use of the addressee named above. If you are not the intended recipient you are hereby notified that any use, dissemination, distribution or reproduction of this email or the contained information is strictly prohibited by law.

If you have received this email in error, please delete and destroy all copies and notify Navitas Limited by telephone on +61 (0)8 6279 XXXX or by replying to the sender. Except as required by law, Navitas Limited does not represent, warrant and/or guarantee that the integrity of this email has been maintained nor that the communication is free of errors, virus, interception or interference. Any views expressed in this message are those of the sender. You may not rely on this message as advice to act unless subsequently confirmed by fax or letter signed by an authorised representative of Navitas Limited

Consider the Environment before printing this email

5.4 Confidential Information

Much of the information that staff and students have access to is confidential. Under the terms of your employment contract, you are required to keep such information confidential and not to pass it on to third parties. ECC wish to make it clear that that requirement extends to the use of Digital Communications. Therefore, staff or students must not send or post confidential information to any third party — without prior permission of an ECC Line Manager.

5.5 Security

- Staff and students are personally responsible for the security of their computer account. You must not allow the terminal to be used by any person — unless you have expressly authorised them to use it.
- Staff and students must keep their password confidential – it must not be shared or disclosed to others.
- To help prevent unauthorised users from using a ECC computer, network connections must be locked if left unattended for any length of time.

5.6 Unacceptable Use of the Email System

- Abuse of Digital Communications systems by transmission of any unsuitable material is likely to constitute misconduct for the purposes of relevant ECC policies.
- Unsuitable material includes but is not limited to material which is:
  - Defamatory
  - Offensive or obscene
  - Untrue or malicious
  - Of a political nature
  - In breach of copyright
  - In breach of any relevant Navitas or ECC policies
  - In breach of any legislation relevant to ECC industry sectors

5.7 Management of Digital Communications

- Staff and students should make sure that they regularly delete all Digital Communications that are no longer needed to avoid overloading servers. Training on how to do this can be provided by IT Support.
- Stand-alone computer users must manage their Digital Communications accounts to the same standards

5.8 Personal Use

ECC will allow reasonable personal use of Digital Communications systems — as long as the following applies:

- All of other rules in this Policy are followed when using the system
- Personal use does not interfere with your working day or ECC organisational needs.

5.9 Cyber Attacks

- ECC network includes scanning software which is designed to intercept any cyber-attack embedded in Digital Communications attachments and files downloaded from the Internet. Whilst the user is informed of the presence of a virus, the file or attachment is held in quarantine and the user is prevented from accessing it.
- Any incidents regarding the detection of cyber-attacks in Internet files or Digital Communication attachments must be reported immediately to IT Support.

THE INTERNET

5.10 General

ECC provides Internet access for employees for the sole purpose of allowing employees to use the Internet as a research tool, to post communications about ECC, to enhance learning and teaching, and to provide services to our clients.

5.11 Internet Access

- Internet facilities will normally be provided only to workstations attached to the ECC network and connected to ECC Internet Service Provider.
- Wireless Internet and its infrastructure is provided by the University. Access to wireless for both staff and students is managed by the University IT Support – see ECU E-Lab staff for assistance..

5.12 Personal Use

- Access to the Internet for appropriate personal use of staff is permitted during working hours.
- Personal use of the Internet is permitted as long as each of the following applies:
  - All the other rules in this Policy are followed when using the Internet
  - Personal use does not interfere with your working day or ECC organisational needs.

5.13 Restrictions on Access to Certain Websites

- Use of the Internet via ECC's IT systems, to access pornographic, illegal, offensive or obscene materials, will in most circumstances be regarded as gross misconduct under the relevant ECC policies.
- "Offensive materials" include any material that may offend or embarrass any person who might see or be confronted with that material.
- Internet-enabled activities, such as gambling, gaming, conducting a business or conducting illegal activities.
- The uploading or downloading of commercial software, games, music videos or other intellectual property in violation of its copyright. Besides the legal issues, such downloads often create system instability with the standard image, adding unneeded repair costs to IT and associated support groups.
- ECC use special monitoring and control software for network connections to prevent access to the majority of undesirable sites. However, those precautions cannot always prevent access to all such sites due to the ever-changing nature of their design. If you accidentally access unsuitable material, you must disconnect from that site immediately and inform your ECC Line Manager. No action will be taken for genuine accidental access of this material, and steps will be taken to ensure such sites are added to the ECC blacklists as soon as possible.
- If you use a stand-alone connection, then you must be aware of your responsibilities not to access such sites and must acquire additional web site control software for your computer if appropriate.

SOCIAL NETWORKING SITES

5.14 General

When entering personal information on to social networking sites, you need to ensure that you do not include any information or photographs which could bring the organisation into disrepute. For example:

- You must not post discriminatory or libellous remarks about the organisation or work colleagues.
- You must not post inappropriate information and photographs of your activities either inside or outside work.

- You are not entitled to access social networking sites for personal use during working hours, if you do so you will dealt with under the relevant ECC policies.
- You must comply with relevant ECC and Navitas policies.

6. Administrative procedures

6.1. This policy will be available on the ECC website at: www.edithcowancollege.edu.au/policies

6.2. This policy will be communicated to staff at induction.

6.3. Any changes to this policy or related procedures will be communication to staff via email.