CHS Internet, Email and Computer Use Policy

Policy Number: 1006

Notice: CHS has signed a shared services agreement with ECA that covers provision of IT Systems and Services as well as provision of a responsive and reliable electronic infrastructure in each of the campuses runs by CHS (see *CHS-ECA Shared Services Agreement*). ECA has several policies that govern the services provided by their ICT Department. These are all adopted by CHS, i.e. as part of the Shared Services Agreement, CHS will require all staff and students abide by the ECA policies and procedures.

1. Purpose

1.1 This Internet, Email and Computer Use Policy ('Policy') sets out the standards of behaviour expected of persons using Education Centre Australia ('ECA')'s computer facilities, or when making reference to ECA on external sites.

2. Commencement of Policy

2.1 This Policy will commence from 21 November 2017. It replaces all other policies relating to use of ECA's computers, internet and email facilities (whether written or not).

3. Application of Policy

3.1 This Policy applies to all people who use ECA's computer network by any means ('users'). The Policy also applies to users who contribute to external blogs and sites that identify themselves as associated with ECA.

3.2 This Policy also sets out the type of surveillance that will be carried out in ECA's workplace, relating to the use of ECA's computer network.

3.3 This Policy does not form part of any employee's contract of employment. Nor does it form part of any other user's contract for service.

4. Definitions

4.1 In this Policy:

a) 'Blogging' means the act of using web log or 'blog'. 'Blog' is an abbreviated version of 'weblog' which is a term used to describe websites that maintain an ongoing chronicle of information. A blog is a frequently updated website featuring diary-style commentary, audio-visual material and links to articles on other websites.

b) 'Confidential information' includes but is not limited to trade secrets of ECA; non-public information about the business and affairs of ECA such as: pricing information such as internal cost and pricing rates, production scheduling software, special supply information; marketing or strategy plans; exclusive supply agreements or arrangements; commercial and business plans; commission structures; contractual arrangements with third parties; tender policies and arrangements; financial information and data; sales and training materials; technical data; schematics; proposals and intentions; designs; policies and procedures documents; concepts not reduced to material form; information which is personal information for the purposes of privacy law; and all other information obtained from ECA or obtained in the course of working or providing services to ECA that is by its nature confidential.

c) 'Computer surveillance' means surveillance by means of software or other equipment that monitors or records information input or output, or other use, of ECA's computer

network (including, but not limited to, the sending and receipt of emails and the accessing of websites).

d) 'Computer network' includes all ECA's internet, email and computer facilities which are used by users, inside and outside working hours, in the workplace of ECA (or a related corporation of ECA) or at any other place while performing work for ECA (or a related corporation of ECA). It includes, but is not limited to, desktop computers, laptop computers, Blackberrys, Palm Pilots, PDAs, other handheld electronic devices, smart phones and similar products, and any other means of accessing ECA's email, internet and computer facilities, (including, but not limited to, a personal home computer or personal electronic devices such as iPads, Tablets, Blackberrys, Palm Pilots, PDAs, other personal handheld electronic devices, smart phones and similar products which have access to ECA's IT systems).

e) 'Intellectual property' means all forms of intellectual property rights throughout the world including copyright, patent, design, trade mark, trade name, and all confidential information and including know-how and trade secrets.

f) 'Person' includes any natural person, company, partnership, association, trust, business, or other organisation or entity of any description and a person's legal personal representative(s), successors, assigns or substitutes.

5. Use of Internet, Email and Computers

5.1 Users are entitled to use ECA computer network only for legitimate business purposes.

5.2 However, users are permitted to use ECA's computer network for limited and reasonable personal use. Any such personal use must not impact upon the user's work performance or ECA resources or violate this Policy or any other ECA Policy.

5.3 A user must not use ECA's computer network for personal use if that use interferes with the efficient business operations of ECA or relates to a personal business of the user.

5.4 ECA gives no warranty or assurance about the confidentiality or privacy of any personal information disclosed by any user in the course of using the computer network for the user's personal purposes.

6. Requirements for Use

6.1 Users must comply with the following rules when using ECA's computer network.

a) Users must use their own username/login code and/or password when accessing the computer network.

b) Users in possession of ECA's electronic equipment must at all times handle the equipment in a responsible manner and ensure that the equipment is kept secure.

c) Users should protect their username/login code and password information at all times and not divulge such information to any other person, unless it is necessary to do so for legitimate business reasons.

d) Users should ensure that when not in use or unattended, the Computer System is shut down.

e) A disclaimer is automatically included in all ECA emails, and must not be removed.

f) If a user receives an email which the user suspects contains a virus, the user should not open the email or attachment to the email and should immediately contact the ICT for assistance.

g) If a user receives an email the content of which (including an image, text, materials or software) is in breach of this policy, the user should immediately delete the email and report the matter to ICT. The user must not forward the email to any other person.

7. Prohibited Conduct

7.1 Users must not send (or cause to be sent), upload, download, use, retrieve, or access any email or material on ECA's computer network that:

a) is obscene, offensive or inappropriate. This includes text, images, sound or any other material, sent either in an email or in an attachment to an email, or through a link to a site (URL). For example, material of a sexual nature, indecent or pornographic material;

b) causes (or could cause) insult, offence, intimidation or humiliation;

c) may be defamatory or could adversely impact the image or reputation of ECA. A defamatory message or material is a message or material that is insulting or lowers the reputation of a person or group of people;

d) is illegal, unlawful or inappropriate;

e) affects the performance of, or causes damage to ECA's computer system in any way;

f) gives the impression of or is representing, giving opinions or making statements on behalf of ECA without the express authority of ECA. Further, users must not transmit or send ECA's documents or emails (in any format) to any external parties or organisations unless expressly authorised to do so.

7.2 Users must not use ECA's computer network:

a) to violate copyright or other intellectual property rights. Computer software that is protected by copyright is not to be copied from, or into, or by using ECA's computing facilities, except as permitted by law or by contract with the owner of the copyright;

b) in a manner contrary to ECA's Privacy Policy;

c) to create any legal or contractual obligations on behalf of ECA unless expressly authorised by ECA;

d) to disclose any confidential information of ECA or any customer, client or supplier of ECA's unless expressly authorised by ECA;

e) to install software or run unknown or unapproved programs on ECA's computer network. Under no circumstances should users modify the software or hardware environments on ECA's computer network;

f) to gain unauthorised access (hacking) into any other computer within ECA or outside ECA, or attempt to deprive other users of access to or use of any ECA's computer network;

g) to send or cause to be sent chain or SPAM emails in any format;

h) to use ECA's computer facilities for personal gain. For example, running a personal business.

7.3 Users must not use another user's computer network facilities (including passwords and usernames/login codes) for any reason without the express permission of the user or ECA.

8. Details on Blocking Email or Internet Access

8.1 ECA reserves the right to prevent (or cause to be prevented) the delivery of an email sent to or from a user, or access to an internet website by a user, if the content of the email or the internet website is considered:

a) obscene, offensive or inappropriate. This includes text, images, sound or any other material, sent either in an e-mail message or in an attachment to a message, or through a link to an internet website (URL). For example, material of a sexual nature, indecent or pornographic material;

b) causes or may cause insult, offence, intimidation or humiliation;

c) defamatory or may incur liability or adversely impacts on the image or reputation of ECA. A defamatory message or material is a message or material that is insulting or lowers the reputation of a person or a group of people;

d) illegal, unlawful or inappropriate;

e) to have the potential to affect the performance of, or cause damage to or overload ECA's computer network, or internal or external communications in any way;

f) to give the impression of or is representing, giving opinions or making statements on behalf of ECA without the express authority of ECA.

8.2 In the case that an email is prevented from being delivered to or from a user, the user will receive a prevented delivery notice. The notice will inform the user that the delivery of the email has been prevented. The notice will not be given if delivery is prevented in the belief that:

a) the email was considered to be SPAM, or contain potentially malicious software; or

b) the content of the email (or any attachment) would or might have resulted in an unauthorised interference with, damage to or operation of any program run or data stored on any of ECA's equipment; or

c) the email (or any attachment) would be regarded by a reasonable person as being, in all the circumstances, menacing, harassing or offensive.

8.3 ECA is not required to give a prevented delivery notice for any email messages sent by a user if ECA is not aware (and could not reasonably be expected to be aware) of the identity of the user who sent the e-mail or is not aware that the e-mail was sent by the user.

9. Type of surveillance in ECA's workplace

9.1 On a continuous and ongoing basis during the period of this Policy, ECA will carry out computer surveillance of any user at such times of ECA's choosing and without further notice to any user.

9.2 Computer surveillance occurs in relation to:

a) storage volumes;

b) internet sites — every web site visited is recorded including the time of access, volume downloaded and the duration of access;

c) download volumes;

d) suspected malicious code or viruses;

e) emails — the content of all emails received, sent and stored on the computer network (this also includes emails deleted from the Inbox); and

f) computer hard drives — ECA may access any hard drive on the computer network.

9.3 ECA retains logs, backups and archives of computing activities, which it may audit. Such records are the property of ECA, are subject to State and Federal laws and may be used as evidence in legal proceedings, or in workplace investigations into suspected misconduct.

10. What Will the Computer Surveillance Records Be Used For?

10.1 ECA may use and disclose the computer surveillance records where that use or disclosure is:

a) for a purpose related to the employment of any employee or related to ECA's business activities; or

b) use or disclosure to a law enforcement agency in connection with an offence; or

c) use or disclosure in connection with legal proceedings; or

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

10.2 For example, use or disclosure of computer surveillance records can occur in circumstances of assault, suspected assault, theft or suspected theft of ECA's property (or that of a related corporation of ECA) or damage to ECA's equipment or facilities (or that of a related corporation of ECA).

11. Blogging Facility

11.1 The website of ECA includes a blogging facility that only authorised users may use.

11.2 Authorised users are only permitted to contribute to blogs on ECA's website in order to share information and knowledge, obtain constructive feedback, interact directly with clients, collaborate over projects and solve problems, promote our organisation, and raise ECA's profile.

12. Standards in Relation to Blogs and Sites Operated by ECA

12.1 Users must not engage in prohibited conduct. Further:

a) Only users who are authorised by the Chief Operating Officer are permitted to publish a blog on any sites operated by ECA, and the content of any such blog must first be approved by the Chief Operating Officer before publishing.

b) The user **must** list their name and job title and add the following disclaimer: '*The opinions expressed here are the personal opinions of the writer. Content published here does not necessarily represent the views and opinions of* ECA.'

c) Public communications concerning ECA must not violate any provisions of any applicable ECA Policy, procedure or contract.

d) A user may participate in ECA-related public communications during normal work time. However, if doing so interferes with any of the user's normal work responsibilities, ECA reserves the right to withdraw the user's access to the communication facilities.

e) A user must not communicate any material that violates the privacy or publicity rights of another party.

f) A user must not cite or refer to clients, business partners, suppliers, other users etc without their prior approval.

g) A user may respectfully disagree with ECA's actions, policies, or management, but must not make personal attacks on any person. This includes competitors of ECA.

h) Users will be personally legally responsible for any content they publish and need to be aware of applicable laws.

12.2 If the user subsequently discovers a mistake in their blog, they are required to immediately inform the Chief Operating Officer and then take steps authorised by the Chief Operating Officer to correct the mistake. All alterations should indicate the date on which the alteration was made.

13. Standards In Relation To Blogs and Sites Not Operated by ECA

13.1 ECA acknowledges that users have the right to contribute content to public communications on websites not operated by ECA, such as social networking sites like LinkedIn, Facebook or YouTube. However, inappropriate use of such communications has the potential to cause damage to ECA, employees, clients and suppliers. For that reason, the following provisions apply to all users:

a) As it may be possible for any user of an external site to conduct a search that will identify any comments about ECA, users must **not** publish any material which identifies themselves as being associated with ECA, except in the case of appropriate postings on LinkedIn.

b) Users must not publish any material that may expose ECA to any possible legal liability. Examples include, but are not limited to, defamation or discrimination proceedings.

c) If it comes to ECA's attention that a user has made inappropriate and/or unauthorised comments about ECA or an ECA employee, or ECA contractor, ECA may choose to take disciplinary action against a user as outlined in this Policy.

14. Warning

14.1 Apart from the potentially damaging effects a blog or post may have on ECA, inappropriate blogs or posts on internal or external sites can also have adverse consequences for a user in terms of future career prospects, as the material remains widely and permanently accessible to other site users.

15. Use of Personal Computers and Electronic Devices

15.1 This Policy applies to the use of personal computers, personal electronic devices such as iPads, Tablets, Blackberrys, Palm Pilots, PDAs and other personal handheld electronic devices, smart phones and similar products which have access to ECA's IT systems, to the extent that such use may damage ECA's business interests and employment relationships, whether this occurs during working hours or not.

16. Enforcement

16.1 Users must comply with the requirements of this Policy. Any breach of this Policy may result in disciplinary action which may include termination of employment (or, for persons other than employees, the termination or non-renewal of contractual arrangements).

16.2 Other disciplinary action that may be taken includes, but is not limited to, issuing a warning, suspension or disconnection of access to all or part of ECA's computer network whether permanently or on a temporary basis.

Variations

16.3 *ECA reserves the right to vary, replace or terminate this Policy from time to time.*

Associated Documents

Workplace Surveillance Policy. Docx

Policy Version and Revision Information

Policy Authorised by: Cesar Muradas

Original issue: 17/09/2015

Title: Group Manager, Technology and Innovation

Policy Maintained by: Cesar Muradas

Current version: 6.0

Title: Group Manager, Technology and Innovation

Review date: 04/12/2019

Acknowledgement

I acknowledge:

- *receiving the Policy;*
- *that I will comply with the Policy; and*
- *that there may be disciplinary consequences if I fail to comply, which may result in the termination of my employment.*

Employee Name: _____

Signed: _____

Date: _____