INTERNET, EMAIL, AND COMPUTER USAGE POLICY

Policy Category	Operational Policy		
Document Owner	Executive Management Committee		
Implementation Officer	Cesar Muradas – Director of Technology		
Review Date	July 2023		
Relevant to	ECA staff, contractors, agents, business partners, and students		
Related Documents	ECA Code of Conduct ECA Communications Policy Workplace Surveillance Policy Use of Personal Electronic Devices for Work-Related Purposes ECA Privacy Policy Workplace Surveillance Act (NSW) Invasion of Privacy Act 1971 (Qld) The Surveillance Devices Act 1999 (Vic) The Telecommunications (Interception and Access) Act 1979 (Cth) Copyright Act 1968 (Cth)		
Version	**Change description**	**Approved by/date**	**Effective date**
1.0	New Policy	ECA Executive Management Committee (EMC)	26 November 2019
1.1	Reviewed and updated	ECA Executive Management Committee (EMC) on 21 July 2021	21 July 2021

1. Overview

The Internet, Email, and Computer Usage Policy has been established to ensure that a transparent environment exists within the Education Centre of Australia Pty Ltd, its subsidiaries, and associated providers ('ECA'), regarding the computer, Internet, and email usage in the workplace.

2. Purpose

This Internet, Email, and Computer Usage Policy ('Policy') set out the standards of behaviour expected of persons using ECA's computer facilities or when referencing ECA on external sites. This Policy complies with the legislative and regulatory Australian jurisdictions that ECA, its subsidiaries, and associated providers operate.

3. Scope

This Policy applies to all ECA staff, contractors, agents, business partners, and students who use ECA's computer network by any means ('users'). The Policy also applies to those who contribute to external blogs and sites that identify themselves as associated with ECA and sets out the type of surveillance carried out by ECA in the workplace, relating to the use of ECA's computer network.

4. Definitions

Definitions	
Blogging	Means the act of using a weblog or 'blog.' A blog is a frequently updated website featuring diary-style commentary, audio-visual material, and links to articles on other websites.

Definitions	
Confidential Information	Includes but is not limited to trade secrets of ECA; non-public information about the organisation and affairs of ECA such as pricing information; 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; personal information as identified in the ECA Privacy Policy; 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.
Computer Surveillance	Is surveillance using software or other equipment that monitors or records the information input or output, or other use, of a computer (including, but not limited to, sending, receiving emails, and accessing Internet websites).
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 subsidiary or associated provider 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, smartphones 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, smartphones, and similar products which have access to ECA's IT systems).
Intellectual property	Means all forms of intellectual property rights throughout the world, including copyright, patent, design, trademark, trade name, and all confidential information, including know-how and trade secrets.
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. The Policy

5.1 Use of Internet, Email, and Computers

i. Users are entitled to use the ECA computer network only for legitimate ECA business purposes.
ii. 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.
iii. 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 the personal business of the user.
iv. ECA gives no warranty or assurance about the confidentiality or privacy of any personal information disclosed by any user using the computer network for the user's personal purposes.

5.2 Requirement for use

i. Users must comply with the following rules when using ECA's computer network.
ii. Users must use their own username/login code and/or password when accessing the computer network.
iii. Users in possession of ECA's electronic equipment must at all times responsibly handle the equipment and ensure that the equipment is kept secure.
iv. 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.
v. Users should ensure that when not in use or unattended, the Computer System is shut down.
vi. A disclaimer is automatically included in all ECA emails and must not be removed.
vii. 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.
viii. 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.

5.3 Prohibited Conduct

5.3.1 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.

5.3.2 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.

5.3.3 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.

5.4 Detailed on blocking email or Internet access

5.4.1 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 email 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.

5.4.2 If 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.

5.4.3 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 email or is not aware that the user sent the email.

5.5 Type of surveillance in ECA's workplace

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.

Computer surveillance occurs in relation to:

a. storage volumes;

b. internet sites — every website 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.

ECA retains logs, backups, and archives of computing activities, which it may audit from time to time. 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.

5.6 What will the computer surveillance records be used for?

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 property damage.

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 an ECA related subsidiary or associated provider) or damage to ECA's equipment or facilities (or that of an ECA related subsidiary or associated provider).

6. Blogging Facility

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

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

6.1.3 The ECA Director of Marketing is responsible for monitoring and maintaining appropriate records to ensure legislative and regulatory requirements are met.

6.2 Standards in relation to blogs and sites operated by ECA

6.2.1 Users must not engage in prohibited conduct. Further:

a. The ECA Director of Marketing authorises those users permitted to publish a blog on any sites operated by ECA and will approve the content of any such blog before publishing.
b. The user must list their name and job title and add the following disclaimer: 'The opinions expressed here are the writer's personal opinions. Content published here does not necessarily represent the views and opinions of ECA.'
c. Public communications concerning ECA must not violate any applicable ECA Policy, procedure, or contract provisions.
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 must be aware of the applicable legislation.

6.2.2 If the user subsequently discovers a mistake in their blog, they are required to immediately inform the Director of Marketing and then take steps approved by the Director of Marketing to correct the mistake. All alterations should indicate the date on which the alteration was made.

6.3 Standards in relation to blogs and sites not operated by ECA

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 an ECA contractor, ECA may choose to take disciplinary action against a user as outlined in this Policy.

6.4 Warning

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 regarding future career prospects, as the material remains widely and permanently accessible to other site users.

7. Use of personal computers and electronic devices

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, smartphones, 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.

8. Enforcement

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

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 temporarily.