Policy

IT Fair and Safe Use

Purpose and Scope

Access to and use of information technology (IT) computer systems and networks owned or operated by The Centre imposes certain responsibilities and obligations and is granted subject to this policy. Client/ learner and staff members who are granted access and use of The Centres' IT systems should have the right to use our technology safely and without harm or harassment.

This policy applies to all users who are granted access to The Centre's IT facilities and resources, by The centre.

Policy

1 Usage

1.1 The Centre aims to provide access to IT and electronic communication systems that is free from, harm, harassment, intimidation or retribution. This includes but is not limited to the prevention of:

1.1.1 Bullying: Threatening behaviour towards others using digital technologies including mobile phones, email and social media tools. For example, setting another learner up to be assaulted, video-recording their humiliation, posting the videorecording online and then sending the website address to others.

1.1.2 Pranking: Repeated hang ups, anonymous, mocking or threatening phone calls.

1.1.3 Image sharing: Forwarding or sharing unflattering or private images without permission.

1.1.4 Sexually explicit images: People of any age, who forward or share images of a sexual nature. If this is images of a person under 18, this is a criminal offence (child pornography) that may result in prosecution.

1.1.5 Text and email: Sending insulting or threatening text messages or emails.

1.1.6 Personal online information: Publishing online someone's private, personal or embarrassing information without permission, or spreading rumours online.

1.1.7 Identity theft: Assuming someone's identity online and negatively representing them in a way that damages their reputation and/or relationships.

1.1.8 Hate sites: Creating hate sites or implementing social exclusion campaigns on social networking sites.

1.1.9 Creating or distributing content that denigrates, demeans or vilifies another person or group

1.2 At all times, The Centre's IT facilities and resources are to be used for an approved or designated purpose. Any usage that does not comply with this designated purpose is considered a breach of this policy, and action will be taken relevant to the appropriate Code of Conduct.

2 Violations

2.1 Violations of this policy may result in the immediate suspension of the user's access to The Centres IT infrastructure and network , pending investigation and may lead to their eventual revocation of access rights. Serious violations of the policy will be referred directly to the appropriate authorities. Unauthorised use of The Centre's IT and/or computing facilities can be a criminal offence. The penalties may include suspension or dismissal from The Centre and/or criminal prosecution.

2.2 Examples of violations of this policy (actual or attempted) include, but are not limited to:

2.2.1 attempting to gain unauthorised access or rights on any Centre I.T. systems or networks, including the bypassing of antivirus software or other systems installed on devices to ensure their safe use

2.2.2 accessing, viewing, downloading or using pornographic material of any nature

2.2.3 excessive downloading or viewing of internet sites or files that are not related directly to The Centre's learning, research activities

2.2.4 accessing or using a protected computer/device account assigned to another person or sharing a password to a protected account with another person

2.2.5 deletion, examination, copying, or modification of network traffic, files and/or data belonging to other users without their prior consent

2.2.6 decryption of system or user passwords and files

2.2.7 copying and/ or storage of copyrighted material, without the express written permission of the copyright owner

2.2.8 connecting any computer, virtual machine or another networked device to any of The Centre's networks without proper authorisation from the appropriate network administrator

2.2.9 loading of software on The Centre's computers/devices and/or networks without compliance to all licensing requirements. Proof of licensing must be readily available.

2.2.10 loading of software on The Centre's computers/devices and/or networks without prior consent from appropriate network administrator

2.2.11 use of a Centre email address for personal business/correspondence

2.2.12 Use of a personal email address for professional, business correspondence

2.2.13 using The Centre's IT infrastructure or equipment to engage in or perpetrate any illegal act under state and federal law. This includes cyber bullying as defined in this policy.

Definitions

Learner
Any person engaged in programs or activities conducted by or at The Centre

Client
For the purpose of this policy a client includes any participant in a Centre-related program that is not direct training. This includes The Centre's community based programs and initiatives.

Workplace
Any of the buildings or structures operated by The Centre or any other place a learner is receiving a component of their learning experience, or a client is involved in a Centre program. This includes offsite or rented premises.

Safe Use
The ability to use IT and electronic communication systems without fear, harm, harassment, intimidation or retribution. Safe use includes the prevention of:

- **Bullying**: Threatening behaviour towards others using digital technologies including mobile phones, email and social media tools. For example, setting another learner up to be assaulted, video-recording their humiliation, posting the videorecording online and then sending the website address to others.
- **Pranking:** Repeated hang ups, anonymous, mocking or threatening phone calls.
- **Image sharing:** Forwarding or sharing unflattering or private images without permission.
- **Sexually explicit images:** People of any age, who forward or share images of a sexual nature. If this is images of a person under 18, this is a criminal offence (child pornography) that may result in prosecution.
- **Text and email:** Sending insulting or threatening text messages or emails.
- **Personal online information:** Publishing online someone's private, personal or embarrassing information without permission, or spreading rumours online.
- **Identity theft:** Assuming someone's identity online and negatively representing them in a way that damages their reputation and/or relationships.
- **Hate sites:** Creating hate sites or implementing social exclusion campaigns on social networking sites.
- **Creating or distributing** content that denigrates, demeans or vilifies another person or group

Version Control

Procedure Operative From	03-2007	Date and Current Version	V3.3 10-2022

Policy

Responsible Officer	CEO	Policy Approved By	Leadership

References

Crimes Act 1958 (Vic)	Electronic Transactions (Victoria) Act 2000
Education and Training Reform Act 2006(Vic)	Education and Training Reform Amendment Act 2010
Education Training Reform Act 2006 (VIC)	

Related Policy

Quality Training and Assessment Policy	Complaints and Appeals Policy
Anti-Harassment and Anti-Bullying policy	Welfare Policy
Information Privacy and Data Security Policy	

Related Procedures

Learner Discipline Procedures	

Related Document, Forms or Guidelines

Learner Code of Conduct	