IT Fair Use

Purpose and Scope

Access to 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.

This policy applies to all users who are granted access to The Centre's IT and computing facilities and resources. Access is granted solely to employees of The Centre, registered learners, and others designated by The Centre Management as being in the interest of The Centre. The Centre reserves the right to limit, restrict, or extend computing privileges and access to its resources.

Policy

1 Usage

1.1 At all times, The Centre's IT and computer faculties must be used in the interest of their designated purposes. Any usage that does not comply with these designated purposes is considered a breach of this policy, and action/s 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 computer account and network access pending investigation of circumstances and may lead to their eventual revocation. Serious violations of the policy will be referred directly to the appropriate outside authorities. Unauthorised use of The Centre's IT and/or computing facilities can be a criminal offence. The penalties may be include suspension or dismissal from The Centre and/or criminal prosecution.

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

2.2.1 attempting to break into or gain unauthorised access or rights on any computer system or network

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

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

2.2.4 accessing or using a protected computer 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, without the express written permission of the copyright owner

2.2.8 connecting any computer, virtual machine or other 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 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 and/or networks without prior consent from appropriate network administrator

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

2.2.12 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 programs.
Staff	For the purpose of this policy staff refers to permanent, full-time or part-time employees, casual staff, volunteers, trainers and tutors. Contractors are also covered by this policy.
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.
Cyber Bullying	Cyberbullying is bullying using digital technologies including mobile phones, email and social media tools. Cyberbullying includes: • **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 an/dor relationships. • **Hate sites:** Creating hate sites or implementing social exclusion campaigns on social networking sites. • when a learner, or learners, uses technology to run a multi-step campaign to bully another learner. For example, setting another learner up to be assaulted, video-recording their humiliation, posting the video-recording online and then sending the website address to others.

Version Control

Policy Operative From	03/2007	**Date and Current Version**	V3.10 9/2019
Responsible Officer	Quality and Compliance	**Policy Approved By**	Board of Governance

References

Crimes Act 1958 (Vic)

Electronic Transactions (Victoria) Act 2000

NSSSP Standards

Related Policy

HR Policy

Learner/Client Complaints and Appeals Policy

Anti harassment and anti bullying policy

Education Training Reform Act 2006 (VIC)

Education Training Reform Regulations 2007

Education and Training Reform Amendment Act 2010

Related Procedure

Staff Discipline Procedure

Welfare Procedure

Related Document, Forms or Guidelines

Staff Code of Conduct

Learner Code of Conduct