Computers, Internet and E-mail Policy and Procedure

Policy number	P-59		
Version number	1.0		
Drafted by	Veronica Kioria		
Responsible person CEO	Veronica Kioria	Signature	Date: 22/05/2019
Approved by the Board:			
On behalf of the Board	David Ling President	Signature	Date: 22/05/19
Scheduled review date	December 2021		

Basic Beliefs/Purpose

Diamond Valley Learning Centre (DVLC) has established guidelines for the use of its computer network, including internet and email, and other media and devices for work-related activities, learning or research. This policy should be read in conjunction with the Social Media Policy.

Scope

This policy applies to all DVLC staff, students, volunteers, Board members, DVLC members and hirers (referred to as users). It applies to DVLC computer facilities used during and outside of business working hours, and accessed from inside the workplace or remotely.

Policy Guidelines

DVLC provides computer and internet resources to support the effectiveness of its business and administrative activities, and as part of training services. DVLC has established processes for maintaining the integrity and security of its computer facilities, to protect against computer failure, loss of records, loss of privacy, and unauthorised updates to computer hardware and software.

DVLC expects all users to behave in a responsible, ethical and lawful manner, and to observe workplace health and safety when accessing computers. All potential hazards and faulty equipment must be reported to management or IT support.

All users are required to:

- use DVLC computer facilities primarily for education or DVLC business purposes;
- comply with software licensing agreements;

- only access electronic files and data relevant to work that are publically available or where authorised permission has been granted;
- avoid unauthorised access by not disclosing logins or passwords; and
- refrain from downloading software or shareware that has not been authorised by management.

DVLC regards the following activities as unacceptable computer use:

- creating or exchanging messages that are offensive, harassing, obscene or threatening;
- accessing unauthorised or illegal websites;
- accessing material that is fraudulent, discriminatory, threatening, bullying, racist, sexually explicit, or is inappropriate or unlawful ;
- creating, storing or exchanging information in violation of copyright laws;
- exchanging or advertising work-related information on social networking sites without approval;
- intentionally breaching confidentiality;
- theft of identity through the unauthorised use of another person's credentials, or by impersonating or falsely representing another person;
- disabling or bypassing virus protection, spam or filtering measures;
- unauthorised online contact with a child or their family; and
- wilful damage of computer or computer related equipment.

All users will be held responsible for their actions when using DVLC computer facilities, and all unacceptable use will be reported to management. Illegal activities will be reported to the police. Disciplinary measures may apply, including the termination of employment or enrolment.

Procedure Guidelines

1. Guidelines for email usage by DVLC staff:
    a. treat email correspondence with the same care and diligence as you apply to hard copy documentation;
    b. use a professional tone at all times ;
    c. use generally accepted email etiquette;
    d. manage your email account by actioning emails in a reasonable timeframe (3 working days), clearing unwanted emails, and organising your inbox;
    e. only send work emails from your DVLC email account;
    f. do not include confidential information in the subject line;
    g. limit personal use of the DVLC email system and never use it for private commercial purposes;
    h. use an out of office message when on leave;
    i. use the approved DVLC email signature which includes your name, role and standard DVLC contact information;
    j. do not share your login or password with anyone; and
    k. do not use your DVLC email account if you no longer work at DVLC.

2. Guidelines for internet usage by DVLC staff:
    a. internet usage may be monitored from time to time;
    b. management approval is required before any DVLC information is made available for public access;
    c. do not use DVLC computer facilities to access inappropriate websites or subject matter that are not in keeping with DVLC's equity principles, code of ethics and legal responsibilities such as child safety standards;
    d. permission must be requested before accessing prohibited websites for legitimate research purposes;
    e. minimise personal use of the internet and social media sites during work times;
    f. carefully consider any posts to social media that reference your work at DVLC; and
    g. report any misuse or breach of this policy.

3. Guidelines for DVLC teaching staff and students in the use of computers and internet in the classroom. Teachers must:
    a. ensure that their students are aware of, and do not engage in, unacceptable computer use, and how DVLC will deal with breaches of behaviour (such as losing access to DVLC computer facilities);
    b. report unacceptable and malicious behaviour, and wilful computer damage immediately;
    c. ensure that students comply at all times with workplace health and safety;
    d. encourage students to report potential hazards or computer equipment issues;
    e. report hazards and equipment issues to IT Support;
    f. encourage students to use computer equipment with care and consideration;
    g. raise student awareness of legal requirements in relation to copyright, privacy, discrimination, child safety, spam, sharing music and other content etc.
    h. remind students that DVLC computers are to be used for education and research purposes only and not for malicious purposes;
    i. ensure that students are aware of where to save their work e.g. to USB;
    j. ensure that students understand security processes such as not divulging their email and computer login or password; and
    k. raise student awareness of safe online behaviour, email and internet etiquette, plagiarism, software or copyright infringements, the need to acknowledge source in their work, etc.

4. Reporting computer related issues.
    a. unacceptable computer usage must be reported immediately to management so that it can be investigated and disciplinary measures taken.
    b. computer-related or equipment issues, including software update requirements, must be reported to IT Support by lodging a ticket at www.razornet.com.au

Definitions

Computer facilities means electronic equipment and computer software accessed by users, and includes, but is not limited to:

- computers, including PC's, laptops/notebooks, tablets and handheld devices;
- printers;
- scanners;
- digital cameras or any other digital imaging equipment;
- all software and programs provided to facilitate work or training needs;
- network operating systems (e.g. Windows);
- all network infrastructure including data cabling and transmission equipment;
- all forms of e-mail;
- internet access; and
- mobile phones connected to the internet and/or email.

Email refers to messages distributed by electronic means from one computer user to one or more recipients via the DVLC network.

Email etiquette includes:

- using a clear subject line;
- being clear and concise (consider using dot points and subheadings)
- proofreading, editing, spellchecking and reading for meaning and tone before sending the email;
- carefully considering who should be a recipient of the email – don't use reply all or CC indiscriminately;
- not forwarding on email chains with FYI and without adding context;
- sending a holding email if you cannot respond in a reasonable timeframe; and
- do not spam.

Internet means a global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardised communication protocols.

Social Media refers to internet-based applications that allow the creation and exchange of user-generated content, or participation in social networking.

Related Policies

P-8 Student Welfare and Duty of Care Policy and Procedure
P-11 Occupational Health &Safety Policy and Procedure
P-13 Code of Ethics Policy
P-26 Access, Anti-Discrimination, Equity, Diversity and Empowerment Policy
P-43 Privacy Policy
P-51 Bullying and Harassment Policy and Procedure
P-60 Social Media Policy and Procedure

Related Documents

D-028 Student Handbook
D-044 Human Resources Policy and Procedure Manual

Legislation

Charter of Human Rights and Responsibilities Act 2006 (Vic)
Children, Youth and Families Act 2005 (Vic)
Disability Act 2006 (Vic)
Education and Training Reform Act 2006 (Vic)
Fair Work Act 2009
Health Records Act 2001 (Vic)
Human Rights and Equal Opportunity Commission Act 1986
Occupational Health and Safety Act 2004 (Vic)
Privacy Act 1988
Privacy and Data Protection Act 2014 (Vic)

Mapping Information

VRQA Guidelines for Non-school Senior Secondary Education Providers: Minimum Standards for Registration to Provide an Accredited Senior Secondary Course, Standard 3
AQTF Standard 2.1, 2.3, 2.5, 3.2