

Wyndham Community and Education Centre Inc

Policy and Procedure

Policy name	Computers, Internet and E-mail Policy and Procedure
Responsible person	CFO and IT & Creative Design Manager
Staff involved	All Staff, Students, Users
Review dates	Approved: 25 November 2024 Review Date: 2025

Policy Context

This policy and procedure sets out the guidelines for acceptable use of the organisation's computer network, including internet and email by employees, students, volunteers and members of Wyndham Community and Education Centre Inc. (Wyndham CEC). The primary purpose for which access is provided is to carry out the duties of employment or training.

The use of Wyndham CEC Information Technology resources carries with it responsibilities. Users must at all times remember that when using Wyndham CEC Information Technology (IT) resources, these resources are to be used primarily for education/ business purposes.

For the purpose of this policy and procedure the term computer includes mobile phone, tablet and laptop devices.

This Policy covers the following broad areas:

- electronic file management and storage, please refer to *Information Security and Asset Governance Policy & Procedure, Records Management and Record Keeping Policy & Procedure, Privacy Policy & Procedure, and Data Breach Response and Information Security Incident Policy & Procedure* for detailed guidelines;
 - acceptable and unacceptable use of computers, internet, email and social networking sites, please refer to *Social Media Policy & Procedure, Cyber bullying Policy & Procedure and Harassment, Discrimination, Victimisation, Bullying Policy & Procedure* for detailed guidelines;
- access to computer files, please refer to *Information Security and Asset Governance Policy & Procedure, Records Management and Record Keeping Policy & Procedure, Privacy Policy & Procedure, and Data Breach Response & Information Security Incident Policy and Procedure* for detailed guidelines;
- email and internet etiquette, *Information Security and Asset Governance Policy & Procedure, Records Management and Record Keeping Policy & Procedure, Privacy Policy & Procedure, and Data Breach Response & Information Security Incident Policy and Procedure, Social Media Policy & Procedure, Cyber bullying Policy & Procedure and Harassment, Discrimination, Victimisation, Bullying Policy & Procedure* for detailed guidelines

This policy and procedure should be applied in conjunction with the *Information Security and Asset Governance Policy & Procedure* and the *Data Breach Response & Information Security Incident Policy and Procedure*.

All employees will receive a copy of this policy and procedure on employment or at induction. It is also available on our website at www.wyndhamcec.org.au and on SharePoint via your allocated logon.

This document was reviewed and accepted by the Board of Governance of the Wyndham Community and Education Centre Inc on 25/11/2024 and supersedes all previous versions.

Version: 2024v1

Document number: 331

Page 1 of 8

G:\Policies\Record management\Computers Internet and E-mail Policy and Procedure 2024v1.docx

Wyndham Community and Education Centre Inc

Policy and Procedure

General Policy Guidelines

Electronic File Management - Authorised Cloud Storage: Wyndham CEC maintains setups as an organisation with Google and Microsoft, as part of these setups Wyndham CEC staff and volunteers have access to organisation wide provisioned cloud storage on both Google Drive and Microsoft One Drive. To maintain client and staff/volunteer privacy, information security and reduce risk of data breach cloud stored electronic files should only be stored on organisation provisioned accounts, files should never be stored on personal accounts and/or unauthorised platforms. Other storage providers may be considered for use after analysis of potential risks, this evaluation should be performed by member/s of senior management in conjunction with the IT & Creative Design manager.

Electronic File Management and Storage: Information held on a computer, Wyndham CEC server or authorised cloud storage, needs to be managed in a similar way to hard copy filing systems. This includes naming documents, storing documents appropriately, data back-ups and archiving information. When saving files in standard user file areas in Windows such as Documents, Downloads, Desktop or Pictures employees with a domain logon have their files automatically stored on one of Wyndham CEC's servers and are backed up according to schedule. It is important to report any accidental deletions or missing documents or folders immediately to IT Support: itsupport@wyndhamcec.org.au failure to do so may result in data being irretrievable from Wyndham CEC's backups. Server backups occur twice a day, at 7am and 12pm.

Users must not store files that contain sensitive information on personal devices. Where necessary, users will be supplied with a computing device that has been setup in accordance with industry security standards. Portable storage should not be used outside the office; where portable storage has been used secure storage of the portable storage device must be maintained. Portable devices are not backed up, users should store files in one of their organisation allocated cloud storage accounts as part of data loss prevention. See *Working from Home Policy and Procedure* and *Information Security and Asset Governance Policy & Procedure* for more information.

Users are responsible for all use of their computer account(s). They should make appropriate use of the system and network-provided protection system features and take precautions against others obtaining access to their computer resources, users should lock their computer before stepping away from their desk. Individual password security is the responsibility of each user. See *Information Security and Asset Governance Policy & Procedure* for more information.

Users are reminded that Wyndham CEC retains ownership over all electronic documentation including email messages created by its employees as part of their employment.

Cyber Security

When malicious code is detected, the following steps will be taken to handle the infection:

- the infected systems are isolated
- all previously connected media used in the period leading up to the infection are scanned for signs of infection and isolated if necessary
- antivirus software is used to remove the infection from infected systems and media
- if the infection cannot be reliably removed, systems are restored from a known good backup or rebuilt.

Wyndham Community and Education Centre Inc

Policy and Procedure

Staff are advised to not post work information to unauthorised online services and to report cases where such information is posted.

Acceptable use of Computers, Internet, Email and Social Networking sites:

All employees, volunteers, students, users and members accessing computer facilities at Wyndham CEC or owned by Wyndham CEC, should do so in an ethical and lawful manner that abides by Wyndham CEC's policies, procedures and codes.

As a user you are required to:

- use Wyndham CEC computer facilities primarily for education/ business purposes;
- use moderation when using computers for personal use;
- abide by the conditions of software licence agreements;
- access only those files and data that are relevant to your work, which are publicly available, or to which you have authorised access;
- only use software that has been authorised for organisational usage, this includes mobile phone and tablet apps;
- use the supplied desktop computer when working in the office
- prevent unauthorised use by not disclosing your login and password to others.

Unacceptable use includes, but is not limited to:

- creating and exchanging messages that are offensive, harassing, obscene or threatening;
- plugging unauthorised devices into Wyndham CEC's network;
- using software that has not been authorised for organisational usage;
- accessing unauthorised or illegal websites;
- accessing any material that is fraudulent, discriminatory, threatening, bullying, racist or sexually explicit or otherwise inappropriate or unlawful;
- creating, storing or exchanging information in violation of copyright laws;
- exchanging or advertising work related information via social networking sites such as Facebook without prior approval (see *Social Media Policy & Procedure*);
- online contact with a child or their family (unless authorised);
- wilful damage of computer or computer related equipment and,
- any activity that is contrary to Wyndham CEC's policies, procedures and codes.

Any illegal activities will be reported to police. For more information regarding information sharing, access control, authorisation and authentication please see *Information Security and Asset Governance Policy & Procedure*.

Access to Computer Files: As part of its Risk Management strategy, Wyndham CEC implements a system of different levels of access to information (see *Information Security and Asset Governance Policy & Procedure* and *Records Management and Record Keeping Policy & Procedure*). Only the CEO and senior management team have access to each other's electronic files. Employees issued with a computer log in and password should under no circumstances share these details with anyone, either internal or external to Wyndham CEC. If a password has been compromised, IT Support must be informed immediately to have the password reset. See section 7.5 in the *Information Security and Asset Governance Policy & Procedure* for more details.

Wyndham Community and Education Centre Inc

Policy and Procedure

Email Etiquette:

Wyndham CEC's email facilities are provided fundamentally for work purposes. However, Wyndham CEC will accept limited and reasonable personal use of its email facilities, if it is in all respects otherwise compliant with this policy and is:

- Occasional;
- Trivial in terms of amount of Wyndham CEC resources used; and
- Is not for personal commercial purposes, private commercial gain or for the significant promotion of private beliefs.

Guidelines for Personal Use

Staff are not to use the 'All Staff' email group lists without prior approval from Senior Management.

If approval from Senior Management is granted, emails sent to all staff must include the following statement 'this email has been approved by Wyndham CEC Senior Management'.

Group email addresses should be placed in the BCC section of the email; "*All Staff - 20 Synnot Street*" and "*All Staff - Inc Vol & BoM - O365*" are examples of group email addresses. To maintain external contact's privacy external email addresses should be placed in the BCC section of a group email.

When an email is received from one of the 'All Staff' email groups staff are to use the reply function not the reply all function when replying to the email.

Guidelines for Work/Business Use

To ensure effective communication, emails informing staff of Wyndham CEC's own programs, events, well-being activities, sustainability initiatives or maintenance at head office will be sent to all staff, no matter what venues they work from.

From time to time, staff will also be invited to 'opt-in' to other Wyndham CEC initiatives that have been approved by Senior Management. For example, fund raising initiatives for charity or staff well-being initiatives.

Email messages should be answered in a timely manner (3 working days).

When preparing an email the following should be considered;

Emails:

- must be sent from your Wyndham CEC email address only;
- should not contain any offensive material;
- should not cc other Wyndham CEC staff indiscriminately;
- should not contain words in CAPITAL LETTERS;
- Emoticon use should be minimised; and,
- should be signed off with your name.

When replying to email please consider carefully if the reply or reply all option should be used; generally, reply should be used for email distributed to global groups e.g. all staff, reply all should not be used in this instance.

This document was reviewed and accepted by the Board of Governance of the Wyndham Community and Education Centre Inc on 25/11/2024 and supersedes all previous versions.

Version: 2024v1

Document number: 331

Page 4 of 8

G:\Policies\Record management\Computers Internet and E-mail Policy and Procedure 2024v1.docx

Wyndham Community and Education Centre Inc Policy and Procedure

Group email addresses should be placed in the BCC section of the email; “*All Staff - 20 Synnot Street*” and “*All Staff - Inc Vol & BoM - O365*” are examples of group email addresses. To maintain external contact’s privacy external email addresses should be placed in the BCC section of a group email.

For consistency, personalised signatures are not to be created and used; uniform signatures will be produced automatically by our email provider. No spam email should be intentionally perpetrated. See section 7.8 of the *Information Security and Asset Governance Policy & Procedure* for more information about digital messaging.

Internet Etiquette: Use of the Internet at Wyndham CEC owned sites for private or personal use during working hours should be kept to a minimum. This includes the use of social networking sites such as Facebook. Employees are cautioned about posting messages or information that refer to work, work related matters, volunteers or fellow colleagues on social networking sites that may not be appropriate or which may be deemed offensive. The *Social Media Policy & Procedure* should be read in conjunction with this Policy for further information and guidelines.

Computer Hardware/Systems: All necessary precautions are to be taken to protect the organisation from computer failure, such as virus control measures, regular maintenance and updating of all computer hardware and software as required. No illegal software is to be loaded onto the computers of the organization, all software installations must follow procedure as set out in the *Information Security and Asset Governance Policy & Procedure*. All reasonable security measures are to be taken to ensure the safety of computer and associated equipment. Wyndham CEC will employ IT qualified staff to ensure the safety and security of all electronic files.

Under no circumstance are users to attempt to disassemble, unplug or move computers/computer hardware without direct instruction from a member of IT Support. Portable computer hardware is an exception, proper safety precautions should be maintained when dealing with sources of electrical current, and placement of portable equipment must follow OH&S guidelines; if you are unsure, please contact one of the organisation’s OH&S reps as listed on the “*My OH&S Team*” posters throughout Wyndham CEC sites.

Staff may be provided with a mobile computing device for work from home or offsite usage, to minimise data security risk devices are not to be used on site via a connection to the organisations network, device can be connected to secure open Wi-Fi or tethered to an organisation allocated mobile phone or mobile internet device.

Server rooms, communications rooms, security containers and secure rooms are not to be left in unsecured states. Server rooms should be checked daily at each location by IT support staff if present on site or by admin staff in the absence of IT support staff. These areas should always remain locked unless there is an IT support staff member present to observe any interactions within these spaces.

Access to systems

A method of emergency access to systems must be documented and tested at least once when initially implemented and each time fundamental information technology infrastructure changes occur.

Wyndham Community and Education Centre Inc

Policy and Procedure

Procedures

Reporting of computer and computer related equipment issues

Computer and computer related equipment issues at 4 Synnot St are to be reported to Senior Secondary Programs Administration, once reported basic troubleshooting will be performed. If basic troubleshooting does not achieve a positive result the issue is to be reported to IT Support at itsupport@wyndhamcec.org.au.

Computer and computer related equipment issues at 20 Synnot St, 106 Duncans Rd, Steam Packet House, Corio Central Shopping Centre should be reported to IT Support at itsupport@wyndhamcec.org.au

When reporting IT issues to IT support please give as much detail as possible:

- Computer name/number; this will be a Dymo label applied by IT support at the time of setup
- What were you doing when the issue occurred
- If software related; what software were you using
- Any basic steps you have taken to resolve the issue, e.g., rebooting the computer/device

IT Support staff will make a determination on the severity of a reported issue, and support will be allocated based on this information.

Software updates and new software installs

Due to strict government guidelines and the potential time requirements involved to upgrade or install new software all requests for new or updated software must be requested via your manager for tabling at the next senior management meeting.

Users may not attempt to modify Wyndham CEC's IT Facilities including its computer system and network facilities or attempt to crash systems. They must not tamper with any software protection, hardware configuration or restrictions placed on computer applications or files unless instructed to do so by a member of IT Support.

Guidelines for Teachers, Trainers and students in the use of computers and the internet in the classroom:

Computers and the internet provide opportunities to enhance the student learning experience by providing access to global information and resources to assist with student learning outcomes.

Use of Wyndham CEC computers and internet resources are intended for learning and research. Responsible use of these resources by students, with guidance from teaching staff, will provide a secure and safe learning environment.

Students using Wyndham CEC computers and the internet have the responsibility to report inappropriate behaviour to their teachers or trainers. Students must abide by this policy and its guidelines.

All usage of computer rooms will be monitored; computer rooms located at 4 Synnot St are additionally monitored by security cameras.

Teachers/Trainers will ensure that:

This document was reviewed and accepted by the Board of Governance of the Wyndham Community and Education Centre Inc on 25/11/2024 and supersedes all previous versions.

Version: 2024v1

Document number: 331

Page 6 of 8

G:\Policies\Record management\Computers Internet and E-mail Policy and Procedure 2024v1.docx

Wyndham Community and Education Centre Inc Policy and Procedure

- students do not save files to the Hard Disk Drive. They should save to their allocated cloud storage, or a USB;
- any problems with computers are to be reported as per the **Reporting of computer and computer related equipment issues** above;
- any student found accessing any material that is fraudulent, discriminatory, threatening, bullying, racist, sexually explicit or otherwise inappropriate or unlawful are to be reported to senior management;
- anyone found performing malicious activities are to be reported to senior management;
- anyone found wilfully damaging computer or computer related equipment, are to be reported to senior management;
- all students are aware of this policy at enrolment and induction;
- all students in youth programs including Senior Secondary Education Programs sign the Computer, E-Mail and Internet Usage Contract form at enrolment

Students will ensure that:

- if issued with an individual computer login and password, they will under no circumstances share these details with anyone, either internal or external to Wyndham CEC;
- they report any computer problems to the teacher or trainer present;
- no settings for virus protection, spam or filtering that have been applied are disabled or bypassed;
- computer and the internet usage is related to learning;
- no chain letters or email hoaxes will be forwarded knowingly;
- no viruses will be forwarded knowingly;
- no inappropriate or unlawful material is sent or published, including offensive, abusive, racist, sexually explicit or discriminatory comments;
- no threatening, bullying or harassing behaviour occurs;
- no defamatory information about a person or the organisation occurs;
- they report any internet site accessed that is considered inappropriate;
- ensure privacy and confidentiality are maintained;
- they don't plagiarise information or fail to acknowledge sources used in their work.

Students will be aware that:

- they are held responsible for their actions while using computers and internet at Wyndham CEC;
- the misuse of internet and computer equipment may result in disciplinary action which includes, but is not limited to, the withdrawal of access;
- they could be held accountable and responsible for wilful damage to computer equipment and any associated costs;
- their emails are archived and their web browsing is logged;
- personal or sensitive information in emails or on websites, could be used as records in investigations, court proceedings or for other legal reasons;
- computer rooms located at 4 Synnot St are monitored by security cameras;
- student computers reset on restart, as such all work saved locally to a computer will be deleted on restart;
- any illegal activity will be reported and may constitute criminal activity.

Wyndham Community and Education Centre Inc

Policy and Procedure

Related Documents

Legislation: Occupational Health & Safety Act 2004 (Vic); Crimes Act 1958 (Vic); Charter of Human Rights and Responsibilities Act 2006; Education and Training Reform Act 2006 (Vic); Equal Opportunity Act 2010 (Vic); Privacy Act 1988 (Cth); Privacy and Data Protection Act 2014 (Vic), Worker Screening Act 2020 (Vic), Children, Youth and Families Act 2005 (Vic), Child Wellbeing and Safety Act 2005 (Vic), Fair Work Act 2009 (Cth).

Policies: Information Security and Asset Governance Policy & Procedure, Data Breach Response & Information Security Incident Policy and Procedure, Working from Home Policy and Procedure, Risk Management Policy & Procedure; Records Management and Record Keeping Policy & Procedure; Privacy Policy & Procedure (Staff/Volunteers) (Students/Clients); Social Media Policy & Procedure; Cyber bullying Policy & Procedure; Harassment, Discrimination, Victimization, Bullying Policy & Procedure, Complaints and Appeals Policy and Procedure, Grievance Policy & Procedure, Disciplinary Action and Termination of Employment Policy & Procedure, Child Safety and Wellbeing Policy & Procedure (including Statement of Commitment), Mandatory Reporting Policy & Procedure, Staff Recruitment, Induction and Exiting Employment Policy & Procedure.

Other: Risk Management Plan; IT & Creative Design Job Description; Desktop Support Job Description; IT Support Job Description; Code of Ethics; Codes of Conduct; General Information for Participants; Computer, E-Mail and Internet Usage Contract.