Information Technology Use Policy

Authorisation	DSCCC Management Committee
Review Date	August 2023
Approved Date	5 September 2023
Next Review Date (Frequency)	August 2026 (3 years) or sooner if required.
Relevant Documents	

AUTHORISATION

This policy was reviewed and adopted by the Dawson Street Child Care Co-operative (DSCCC), at a committee meeting on the Approved Date defined above.

POLICY STATEMENT

Values

We are committed to:

- Providing clear guidelines on the appropriate use of information technology facilities at DSCCC.
- Ensuring use of DSCCC's information technology facilities is primarily for business activities, but the Management Committee acknowledges that from time to time staff may need to access the facilities for limited and appropriate personal use.
- Preventing inappropriate use.
- Providing a safe work place for staff, the employer and others using DSCCC's information technology facilities.
- Maximising the protection needed to safeguard the privacy and confidentiality of matters received, transmitted or stored electronically.
- Ensuring the use of DSCCC's information technology facilities complies with its policies and relevant legislation.

Purpose

The aim of this policy is to:

- Protect confidential and sensitive information.
- Provide users of DSCCC's information technology facilities with a safe working environment.
- Restrict use to authorised persons as determined by the Management Committee.
- Restrict use for DSCCC-related activities only, whilst acknowledging that from time to time staff may need to access the facilities for limited and appropriate personal use.
- Prevent inappropriate use.
- Provide clear guidelines for users of DSCCC's information technology facilities.

SCOPE

This policy applies to staff, the Management Committee, staff, students, volunteers and any other persons who have access to, or use the information technology facilities at DSCCC.

This policy governs access to the Internet via the World Wide Web (www), electronic mail (email) or other electronic means available at DSCCC, including access via computers, mobile phones and tablets. It is intended to encourage responsible action and to reflect a respect for the ability of its adherents to exercise good judgement and to behave in a professional and ethical manner.

This policy is intended to operate within, and be consistent with, the existing constitution and policies.

Use of any of DSCCC's secure online applications, used to record and disseminate children's' learning and development experiences at DSCCC, constitutes acceptance of this policy.

BACKGROUND AND LEGISLATION

The Internet is a wonderful resource for research, communication and for conducting business. In the future, DSCCC seeks to provide its staff, Management Committee and parents/guardians with online information resources and communication tools, to support them in the education of children and operation of the Centre.

Legislation

This may include, but is not limited to:

- *Education and Care Services National Law Act 2010*
- *Education and Care Services National Regulations 2011*
- *Disability Discrimination Act 1992 (Cth)*
- *Equal Opportunity Act 2010 (Vic)*
- *Health Records Act 2001 (Vic)*
- *Australian Human Rights Commission Act 1986 (Cth)*
- *Privacy and Data Protection Act 2014 (Vic)*
- *Racial Discrimination Act 1975 (Cth)*
- *Sex Discrimination Act 1984 (Cth)*
- Censorship legislation: Commonwealth and state laws prohibit publication of hard core pornography (in particular where it involves children, bestiality, violence, cruelty and/or exploitation). A breach of these laws would constitute a criminal offence.
- *Spam Act (2003) (Cth):* Under this Act, users must not send unsolicited commercial electronic messages. Any commercial messages that are sent electronically (including email, instant messaging or telephone accounts) must include information about the individual or organisation who authorised the sending of the message and a functional unsubscribe facility.
- *The Occupational Health & Safety Act 2004 and Occupational Health & Safety Regulations 2007*

- *Trade Marks Act (1995) (Cth):* Users must not copy a trademark or a logo belonging to another party. Trademark infringement will expose the user to liability for damages.
- *Competition and Consumer Act 2010 (Cth):* This Act contains provisions which prohibit passing off and misleading and deceptive conduct. If a user were to copy material from an external site onto DSCCC's site so that the persons accessing the website would believe that DSCCC had been authorised to carry the material, this would constitute passing off or deceptive or misleading conduct.
- *Copyright Act (1968) (Cth):* Text (including song lyrics), computer programs, illustrations (including maps and diagrams), photographs, music recordings, videos, films and television broadcasts are all protected by copyright. The duration of copyright protection is generally 50 years following the death of the author. A user must not copy, send or place materials on the web without permission from the copyright owner. Infringement of another person's copyright could result in personal liability for damages. If users wish to include material from another webpage, for example in DSCCC's web page, they should create a hypertext link pointing to the material rather than copy it. It is suggested practice to seek permission from other webpage owners prior to creating links to their pages.

Examples of conduct which will infringe copyright if undertaken without permission of the copyright owner:

- Converting a CD to an audio format, such as MP3, and using it on a computer
- Downloading software from the Internet using centre Internet access
- Uploading software or commercial photographs, to a centre website and making these available to the public
- Sending copyright material to another person using a DSCCC computer
- Storing copyright material on DSCCC computers.

DEFINITIONS

Chain mail: Email sent to a number of people asking the recipient to send copies of the email with the same request to a number of recipients

Cloud storage: Online space that you can use to remotely store & share data.

Defamatory: Injure or harm another's reputation without good reason or justification, slander or libel.

DHHS: Department of Health and Human Services

Information technology facilities: This includes all computers, networks, Internet access, email, hardware, data storage, computer accounts and software. Use of personal information technology facilities, such as personal mobile phones, is also covered by this policy.

Social Media: Online applications such as social networking sites, wikis, blogs, microblogs, video and audio sharing sites and message boards that allow people to easily publish, share and discuss content.

Spam: Unsolicited commercial electronic messaging.

Vicariously: Delegated, acting or carried out on behalf of another. (The employee could be seen to be acting on behalf of the employer).

Viruses: A program or programming code that replicates by being copied to another program, computer or document. Viruses can be sent in attachments to an email or file, or be present on a disk or CD. Some viruses are benign or playful in intent and some can be quite harmful, erasing data or causing your hard disk to require reformatting.

PROCEDURES

The Management Committee is responsible for:

- Authorising members of the Management Committee, staff and students to have access to the computer.
- Authorising members of the Management Committee, director and administration officer to have access to DSCCC's Cloud storage account and providing passwords.
- Changing DSCCC's Cloud storage password each time the Committee has a change in members.
- Keeping the information in Cloud storage up to date and relevant to the current goings on with the committee and Centre.
- Governing desirable behaviours in the use of IT for DSCCC.
- Reviewing Centre policies, practices, measures and procedures to ensure data and information are kept secure and that DSCCC meets the evolving challenges posed by threats to information systems and networks.
- Adhering to the Centre's *Privacy and Confidentiality Policy* in regard to all emails and information accessed on DSCCC's computer.
- Ensuring no unauthorised access to DSCCC's IT facilities.
- Providing the Director/Administration Officer with a secure email address for confidential and staffing correspondence that is not accessible to other staff.
- Providing the Director/Administration Officer separate log-in to provide a secure location in which to store electronic material relating to staff.
- Providing Authorisation Capacity to the Director/Treasurer to DSCCC's on-line bank account.
- Providing view only/data input access to the Administration Officer and authorised personnel to DSCCC's on-line bank accounts.
- Authorising the use of contemporary and secure online applications for the purpose of recording and disseminating children's' learning and development experiences at DSCCC.

The Director is responsible for:

- Ensuring the email account provided by DHHS through Vicnet is checked on a regular basis and forwarding relevant emails to appropriate members of the Management Committee and staff.
- Identifying the need for additional password protected email accounts for staff and Management Committee members (refer to *Background Information*).
- Identifying training needs of existing staff and new staff for inclusion in professional development.

- Adhering to DSCCC's *Privacy Policy* in regard to all emails and information accessed on the Centre's computer.
- Removing outdated emails from the computer within 30 days and saving copies of relevant emails securely on DSCCC's main computer. For example correspondence with DHS, KPV, CCMS.
- Responding to emails within three days, where possible, but using discretion to prioritise responses.
- Authorising the use of contemporary and secure online applications for the purpose of recording and disseminating children's' learning and development experiences at DSCCC.
- Maintaining the security of ICT facilities belonging to DSCCC and keeping allocated passwords secure, including not sharing passwords and logging off after using a computer

The Administration Officer is responsible for:

- Removing outdated emails from the computer within 30 days and saving copies of relevant emails securely on DSCCC's main computer. For example correspondence with DHS, KPV, CCMS.
- Backing up the office computers to a portable hard drive, purchased solely for this purpose, on a monthly basis.
- Ensuring current virus protection software is installed on each of DSCCC's computers.

Each authorised user is responsible for:

- Complying with relevant legislation and centre policies.
- Ensuring electronic files containing information about children and families are kept secure at all times.
- Keeping the secure password allocated to them by the Management Committee, including not sharing passwords and logging off after using a computer. Users must not compromise or attempt to compromise the security of any IT facility belonging to the Centre, nor exploit or attempt to exploit any security deficiency.
- Using the IT facilities in an ethical and lawful way, in accordance with Australian laws (refer to legislation listed in this document).
- Only accessing accounts, data or files on DSCCC's computers which they have authorisation to access.
- Co-operating with other users of the IT facilities to ensure fair and equitable access to the facilities.
- Programs on DSCCC's computers are approved by the Management Committee and loaded onto the computer by the Director or Administration Officer.
- Not attempting to access or transmit at any time, via email or any other medium, material (language and images), which a reasonable person could consider indecent, offensive, obscene, profane, sexually explicit or objectionable.
- Not harassing, slandering, intimidating, embarrassing, defaming, vilifying, seeking to offend or make threats against another person, group of people or organisation via electronic mail or other medium.

- Not using personal devices to record images of children *(National Law 167)*
- Not making copies of, or transmit, commercial software illegally in breach of copyright.
- Not participating in spamming or sending mass unsolicited email.
- Not transmitting confidential information inappropriately.
- Not attempting to access or transmit at any time, via email or any other medium material that is illegal.
- Removing outdated emails from the computer after 30 days.
- Not undertaking game playing on DSCCC IT facilities.
- Being aware of the need for security of information systems and networks and what they can do to enhance security. This includes acting in a timely and cooperative manner to prevent, detect and respond to security incidents and report any concerns to the Management Committee.
- Using DSCCC's email and messaging facilities for Centre-related activities, provided such use is lawful. Messaging facilities may include chat sessions (for example with Management Committee members or other professionals), and electronic conferences (where applicable). The Management Committee reserves the right to withdraw this permission in the event that such use places the IT facilities at risk or poses a security or other threat. Users must respect the privacy and personal rights of others.
- Not using DSCCC's IT facilities to access pornographic material or to create, store or distribute pornographic material. It will not be a defence to claim that the recipient was a consenting adult.
- Not using DSCCC's IT facilities to run a personal business on the Centre's IT facilities.
- Not publishing their DSCCC email address on a private business card.
- Adhering to DSCCC's *Privacy and Confidentiality Policy* in regard to all emails and information accessed on DSCCC's computer.
- Unless authorised by the Director, not posting information about DSCCC to a social networking site or uploading photos taken at DSCCC or on excursion onto a social networking website.

Email spam management

Unsolicited and unwanted emails are known as spam. They can have a number of aims, some of which are harmless (but often annoying) sales and marketing pitches and others which are malicious and may cause damage to your computer/data, or enable people to steal your financial records and access your bank accounts. Some spam emails contain viruses. All users are advised never to open files or start programs that have been sent as attachment via email from an unknown/untrustworthy source. Suggested practice is to scan the attachment with anti-virus software before you open it and check for unusual filenames.

Information stored on computer/s

- Records containing personal, sensitive, health information or photographs of children will be stored securely so that the privacy and confidentiality of all information is maintained. For example, password protected or transferred to remote storage device, including but not limited to, CD-rom, DVD, hard drive or memory stick, and kept in a

secure location or a secured cloud storage program such as but not limited to 'box' or 'dropbox' that is also password protected.

- Users of the computers are not to view or interfere with other users' files or directories or knowingly obtain unauthorised access to information or damage, delete, insert or otherwise alter data without permission.

Accessing Social Media

- Guidelines around accessing or engaging with social media using a DSCCC computer is contained in the *Staff Conduct Policy*.

Breaches of this policy

- Users who fail to adhere to the procedures set out in this policy may be liable to personal criminal or civil legal action. This could result in serious consequences such as a fine, damages and/or costs being awarded against the individual or even imprisonment. The centre will not defend or support any user who uses the IT facilities for an unlawful purpose.
- Parents/guardians or other users failing to adhere to this policy may be expelled from the centre in line with DSCCC's constitution.
- Staff failing to adhere to this policy may be liable to counselling or disciplinary action.
- Volunteers and/or students failing to adhere to the policy may have access to DSCCC's computers denied or have their placement terminated.

The centre accepts no responsibility for loss or damage or consequential loss or damage, arising from the use of DSCCC's IT facilities.

Procedures

Refer to *Attachment 1* for the following procedures:

- Email usage
- Digital storage of personal and health information
- Data back up
- Password management

RELATED DOCUMENTS

- OECD (2002) *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (Appendix 1)

  DSCCC policies

  - Behaviour Guidance and Interactions with Children Policy
  - Privacy and Confidentiality Policy
  - Occupational Health and Safety Policy
  - Staff Conduct Policy

DISCLAIMER

Although the Internet and email are valuable resources it is often open to hazardous programs including but not limited to a virus, adaware, spyware and foreign intrusion by outside sources (hackers).

For this reason the centre cannot guarantee the privacy and confidentiality of matters transmitted or stored electronically.

EVALUATION

In order to assess whether this policy has achieved its purposes the Management Committee will:

- Monitor complaints received in relation to the use of DSCCC's computer and online resources.
- Take into account reports from staff, the Management Committee, parents/guardians and any other persons, in relation to the policy.

Date Reviewed	Details of Changes (if any)	Date of Next Review
August 2023	Minor changes only and addition of Procedures as Appendices	August 2026
April 2017	Minor changes only	April 2020
April 2014	Update to legislation and other minor changes	April 2017
August 2010	Addition of reasonable personal use of facilities by staff. Updated terminology and reference to 2009 Regulations	August 2013
Aug 2007	DSCCC policy based on KPV policy 2006.	Aug 2010

ATTACHMENT 1. PROCEDURES FOR USE OF ICT AT THE SERVICE

Email usage

- Content of emails and email addresses must always be checked before sending.
- When sending emails to multiple recipients, care should be taken to avoid the inappropriate disclosure of email addresses to a whole group of recipients; blind copying (BCC) should be used where appropriate.
- Always include a subject description in the subject line.
- Create an email signature that identifies employee name, title, service name, service phone number and address.
- Always include a disclaimer which is common to all users, on emails to limit liability.
- Be cautious about opening files or launching programs that have been received as an attachment via email from the email itself. Instead, save an attachment to disk and scan with anti-virus software before opening, and keep an eye out for unusual filenames.
- Never open emails if unsure of the sender.
- Check email accounts on a regular basis and forward relevant emails to the approved provider or appropriate committee members/staff.
- Remove correspondence that is no longer required from the computer quarterly.
- Respond to emails as soon as is practicable.
- Never send unauthorised marketing content or solicitation emails
- Be suspicious of clickbait titles.

Digital storage of personal and health information

- Digital records containing personal, sensitive and/or health information, or photographs of children must be password protected and stored securely so that privacy and confidentiality is maintained. This information must not be removed from the service without authorisation, as security of the information could be at risk *(refer to Privacy and Confidentiality Policy).*
- Digital records containing personal, sensitive and/or health information, or photographs of children may need to be removed from the service from time-to-time for various reasons, including for:
    - excursions and service events *(refer to Excursions and Service Events Policy)*
    - offsite storage, where there is not enough space at the service premises to store the records.

  In such circumstances, services must ensure that the information is transported, handled and stored securely so that privacy and confidentiality is maintained at all times.
- ICT users are not to view or interfere with other users' files or directories, knowingly obtain unauthorised access to information or damage, delete, insert or otherwise alter data without permission.
- Ensure all material stored on an endpoint data storage device is also stored on a backup drive, and that both device and drive are kept in a secure location.

Backing up data

Data backup is the process of creating accessible data copies for use in the event of breach or loss.

- Develop a written backup plan that identifies:
    - What's being backed up
    - Where it's being backed up
    - How often backups will occur
    - Who's in charge of performing backups
    - Who's in charge of monitoring the success of these backups

- How will backup drives be stored securely

Services can choose to either between onsite or remote backup:

- Onsite Backup
  - copy data to a second hard drive, either manually or at specified intervals.
- Remote Backup- cloud based backup server
  - install the software on every computer containing data that needs to be backed up,
  - set up a backup schedule, and
  - identify the files and folders to be copied.

Password management

The effective management of passwords is the first line of defence in the electronic security of an organisation. Every ICT facility should have a password strategy in place as part of the overall security strategy. The technical considerations and principals outlined below are intended to be used as a guide for developing a password procedure.

Technical considerations include:

- a strong password should:
  - Be at least 8 characters in length
  - Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z)
  - Have at least one numerical character (e.g. 0-9)
  - Have at least one special character (e.g. ~!@#$%^&*()_-+=)
- always verify a user's identity before resetting a password
- change passwords when an employer leaves the service
- password rotation; changed every 90 days or less
- do not use automatic logon functionality
- use of account lockouts for incorrect passwords, with a limit of 5 or fewer bad attempts.

Users should always follow these principles:

- do not share passwords with anyone. If there is an issue that requires you to do so, remember to change the password immediately after the issue has been resolved.
- never use the same password for work accounts as the one you have for personal use (banking, etc.).
- do not write down passwords or include them in an email.
- do not store passwords electronically unless they are encrypted.
- never use the "remember password" feature on any systems; this option should be disabled
- Do not use the same password for multiple administrator accounts.

Working from home

When an approved provider, nominated supervisor, early childhood teachers, educators or staff members are working from home they must:

- complete the authorised user agreement form
- conduct a workstation assessment; taking reasonable care in choosing a suitable work space, including ergonomics, lighting, thermal comfort, safety, and privacy
- ensure security and confidentiality of work space, keeping private, sensitive, heath information, planning, educational programs and children's records confidential and secure at all times
- keep allocated passwords secure, including not sharing passwords and logging off after using a computer
- adhere to the *Privacy and Confidently Policy*
- report breaches to privacy or loss of private, sensitive, and heath information to nominated superiors as soon as practically possible.