Australian College of Care Workers

Information Technology Use Policy

Introduction

This policy deals with the provision of information technology (IT) resources by Australian College of Care Workers Ltd ABN 39 633 248 610 (ACCW) and the associated responsibility of authorised users when accessing these information technology resources. These resources include, but are not limited to, the ACCW network, computer systems and software, access to the Internet, electronic mail, telephony and related services.

Principles

The policy is based on the following principles, which must be followed by all those responsible for the implementation of this policy and to whom this policy applies:

- The information technology resources of ACCW are provided to support the registration, research and administrative activities of the ACCW;
- Authorised users are granted access to valuable ACCW resources, confidential, personal and sensitive data and to external networks on the basis that their use of ACCW ICT resources shall be responsible, ethical and lawful at all times;
- Authorised users are required to observe ACCW policy, and Australian or other local laws which may apply;
- The privacy of personal information relating to persons and other confidential matters acquired for business purposes shall be protected and must not be used or disclosed for any unlawful purpose or any purpose contrary to any policy of ACCW;
- ACCW business information shall be protected from unauthorised and/or accidental disclosure; and
- ACCW ICT resources must not under any circumstances be used to humiliate, intimidate, offend or vilify others on the basis of their race, gender, or any other attribute prescribed under anti-discrimination legislation.

Broad Overview

1. **What Is Provided and Why** – The information technology resources of ACCW are provided to support the registration, research and administrative activities of the ACCW. These resources include the ACCW network, computer systems and software, access to the Internet, electronic mail, telephony and related services.
2. **Access** – This policy prescribes the conditions under which access to ACCW ICT resources is granted.
3. **Responsible Usage** – Staff and other specifically authorised users who are granted access to ACCW ICT resources are required to utilise ACCW ICT resources in a responsible, ethical and lawful manner.

Date Created	Review Date	Authorised by
3.7.2019	3 years	ACCW Board

4. **What is and is Not Acceptable Usage** – This policy, with which all staff and other authorised users must comply, identifies what is acceptable usage including the personal use of ACCW ICT resources.

5. **Breach of Policy** – This policy identifies the possible consequences should a breach of the policy occur.

Scope and Application

This policy applies to all ACCW staff, honorary appointees, contractors and guest/visitors of ACCW plus any authorised users or organisations accessing ACCW ICT resources. This policy applies to all use of ACCW ICT resources, including (but not limited to):

- copying, saving or distributing files;
- data;
- online forms and membership details;
- downloading or accessing files from the Internet or other electronic sources;
- electronic bulletins/notice boards;
- electronic discussion/newsgroups;
- email;
- file sharing, file storage and file transfer;
- instant messaging;
- online discussion groups and 'chat' facilities;
- printing material;
- publishing and browsing on the Internet;
- the use of social networks and social media;
- streaming media;
- subscription to list servers, mailing lists or other like services;
- video conferencing;
- viewing material electronically; and
- weblogs ('blogs') and video blogs ('vblogs')

Operative Date: Effective immediately

Policy Authorisation: Director

Policy Administrator: IT Manager - Information Technology Division

Policy and Consultancy: Human Resources Division

Definitions

ACCW email systems – any email system used for the purpose of ACCW-related electronic communications. ACCW email systems are part of ACCW ICT resources.

ACCW ICT resources – includes, but is not limited to, all networks, systems, software and hardware (including local area networks, wide area networks, wireless networks, intranets, ACCW email

systems, computer systems, software, desktop computers, printers, scanners, personal computers, mobile phones, portable storage devices, hand held devices and other ICT storage devices)

ACCW Officer/Supervisor – ACCW staff member who has the authority (or delegated authority) to recommend a staff appointment.

Authorised User – any person who has been authorised by the relevant ACCW Officer/Supervisor to access any ACCW IT system or IT facility, including but not limited to:

- Staff of ACCW
- Staff of any entity/company in which ACCW has an interest
- Staff of any entity/company /organisation with which ACCW is pursuing a joint venture
- Students
- Consultants
- Visitors
- Honorary appointees
- Collaborative researchers

Email and Messaging - Email means the ACCW-provided electronic mail systems and computer accounts. Additional messaging facilities may include but are not limited to calendar and scheduling programs, chat sessions, IRC, newsgroups and electronic conferences.

Information Technology Resources (ACCW ICT resources) – covers all IT facilities including all computers, computing laboratories, lecture theatres and video conferencing rooms across ACCW together with use of all associated networks, internet access, email, hardware, dial-in access, data storage, computer accounts, software (both proprietary and those developed by the ACCW), telephony services and voicemail.

Malware – malicious software programs designed to cause damage and other unwanted actions on a computer system, such as (but not limited to) computer viruses, worms, spyware and Trojans.

Personal information means information or an opinion (including information or an opinion forming part of a database) that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Personal Use – all non-work-related use of ACCW ICT resources including Internet usage, social networking and private emails.

Personal Web Page –Personal web pages are those pages produced by authorised users that are not directly related to work responsibilities. They may not include any commercial information, and must not under any circumstances be used for business-related activities.

Phishing – the attempt to obtain confidential, personal or sensitive information such as usernames, passwords, and credit card details (and, indirectly, money) often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

Publish – to make information available for access by others via any method or format, including, but not limited to, on a web page, email, or the use of peer-to-peer programs.

Spam – unsolicited commercial electronic messages sent over the Internet.

User – any person using ACCW ICT resources.

Issues Addressed

1. Access to Information Technology Resources

1.1 Lawful Use

The use of ACCW ICT resources must be lawful at all times. Unlawful use will breach this Policy and will be dealt with as a discipline offence.

Unlawful use of ACCW ICT resources may also lead to criminal or civil legal action being taken against individual authorised users. This could result in serious consequences such as a fine, damages and/or costs being awarded against the individual or even imprisonment.

ACCW will not defend or support any authorised user who uses ACCW ICT resources for an unlawful purpose. For further information on some (but not all) relevant laws, refer to the section of this policy titled Relevant Australian Legislation, Policies and Associated Documentation.

1.2 Business Purposes

ACCW ICT resources are provided to authorised users for business purposes. Other than limited personal use, ACCW ICT resources must be used for business purposes.

Users are allowed reasonable access to electronic communications using ACCW ICT resources to facilitate communication between employees and their representatives, provided that use is not unlawful, offensive or otherwise improper. This may include communications with a union on matters relating to the employer/employee relationship.

Each user must minimise large data downloads or transmissions, in order to ensure that the performance of the ACCW ICT resources for other users is not adversely affected.

1.3 Granting of Access

Access to ACCW ICT resources ACCW ICT resources is authorised by the relevant ACCW Officer/Supervisor and provided by the Information Technology Services Division or other organisational unit responsible for managing the ACCW ICT resources (eg, the Library). Access is normally based on a need to access that ACCW ICT resources and an individual's current status with ACCW as recorded in the ACCW's human resources database or other database managed by the Information Technology Services Division or the Human Resources Division or Student and Community Services Division.

1.4 User Declaration Form

Users may be required to complete a User Declaration form prior to authorisation being granted for access to certain ACCW ICT resources.

1.5 Access on contract expiry or authorised access period

Email and computer access will cease on expiration of contract or end-date as recorded in the Human Resources database. For strictly professional or work-related reasons, staff and other authorised users may request that computer access be extended for a period up to 30 days. Approval must be given by Head of Department or equivalent. Following this approval, an option to forward email to another external email account can be authorised by the Director or equivalent and shall not exceed 6 months.

1.6 Responsibilities

Use of ACCW Computer Accounts

Each authorised user is responsible for:

- The unique computer accounts which the ACCW has authorised for the user's benefit. These accounts are not transferable;
- Selecting and keeping a secure password for each of these accounts, including not sharing passwords and logging off after using a computer; and
- Familiarising themselves with legislative requirements which impact on the use of ACCW ICT resources and acting accordingly. ACCW takes no responsibility for users whose actions breach legislation – for further information refer to the section of this policy titled Relevant Australian Legislation, Policies and Associated Documentation.

1.7 Restrictions to Access

Users are expressly forbidden unauthorised access to accounts, data or files on ACCW ICT resources or any other IT resource. The Administrator of an IT Resource may restrict access to an individual user on the grounds that the user is in breach of this policy.

1.8 Third Party Access

Entities other than Information Technology Services may neither negotiate nor grant third parties access to ACCW communications and network infrastructure. Applications for access should be made in writing to the Office of the Director.

1.9 Domain Name Registration

All domain names for ACCW projects/activities must be registered through the Office of the Director. This requirement must be observed in all instances. Users should note it is ACCW that owns and controls the site not the person who registers the name.

1.10 Software License Restrictions

Use of proprietary software is subject to terms of licence agreements between ACCW and the software owner or licensor and may be restricted in its use.

2. Personal Use of Information Technology Resources

2.1 Extent of Personal Use

A user who is authorised to use the ACCW ICT resources may also use the ACCW ICT resources for limited, incidental personal purposes. Personal use of the ACCW ICT resources is permitted provided such use is lawful, does not negatively impact upon the user's work performance, hinder the work of other users, or damage the reputation, image or operations of ACCW. Such use must not cause noticeable additional cost to ACCW.

2.2 Commercial Use

ACCW ICT resources must not be used for private commercial purposes except where the paid work is conducted in accordance with ACCW Practice and Paid Outside Work Policy, or the work is for the purposes of a corporate entity in which ACCW holds an interest.

2.3 Reasonable Use Determination

Whether or not use was reasonable in the circumstances will be a matter to be determined by the Director.

2.4 ACCW Liability

ACCW accepts no responsibility for:

- Loss or damage or consequential loss or damage, arising from personal use of the ACCW ICT resources.
- Loss of data or interference with personal files arising from the ACCW's efforts to maintain the ACCW ICT resources.

3. Internet, Email and Messaging

3.1 Access to the Internet

3.1.1 Work Purposes

Authorised users are permitted to access the Internet for work related purposes, subject to compliance with this policy.

3.1.2 Personal Usage

Access is also permitted for personal purposes provided such use is lawful, not excessive in terms of time and cost to ACCW and does not otherwise breach this policy.

Examples of permitted personal use are:

- Online banking
- Travel bookings
- Browsing.

3.1.3 Reasonable Use Determination

Whether or not use was reasonable in the circumstances will be a matter to be determined by the user's Manager, having regard to the following criteria:

- the use occurred during normal working hours (but excluding lunch or other official breaks);
- the use adversely affects (or could reasonably be expected to adversely affect) the performance of the employee's duties;
- the use is not insignificant.

ACCW may seek reimbursement from a user for all or part of any costs where the user caused ACCW to incur costs due to excessive use of the ACCW ICT resources for purposes not related to his/her employment in breach of this policy.

Subject to limited personal use, the use of social networks and social media, on-line conferences, discussion groups and other similar services or tools using ACCW ICT resources must be relevant and used only for ACCW purposes or professional development activities. Users must conduct themselves professionally and appropriately when using such tools.

3.2 Email and Messaging

3.2.1 User Responsibilities

When using the email or messaging system users must always :

- Respect the privacy and personal rights of others;
- Take all reasonable steps to ensure copyright is not infringed – refer section 3.3.3;
- Take all reasonable care not to:
  - plagiarize another person's work; or
  - defame another person;
- Take reasonable care to ensure that the email is sent to the intended recipient and that any documents or other attachments to be sent to the intended recipient are the documents and attachments intended to be attached to the email;
- Not forward or otherwise copy a personal email (except with permission of the author) or an email which contains personal information or an opinion about a person whose identity is apparent (except with permission of that person);
- Not send forged messages, or obtain or use someone else's e- mail address or password without proper authorisation;
- Not send mass distribution bulk messages and/or advertising without approval of the user's Supervisor;
- Not send spam (refer Relevant Australian Legislation). The user must ensure that the recipient(s) of the intended email have consented to receive such email(s);

- Not harass, intimidate or threaten another person/s – refer also to section 3.2.2;
- Not send sexually explicit material, even if it is believed that the receiver will not object. Remember, the intended receiver may not be the only person to access the communication – refer to section 3.3.2; and
- Adhere to the practices as set out in sections 3.2.2, 3.2.3 and 3.2.4 below.

3.2.2 Standards Required When Using Email

Appropriate standards of civility should be used when using e-mail and other messaging services to communicate with other staff members, students or any other message recipients. When using the email or messaging system users must not send:

- Angry or Antagonistic Messages – these can be perceived as bullying or threatening and may give rise to formal complaints under grievance procedures or discrimination/sexual harassment procedures; or
- Offensive, Intimidating or Humiliating Emails – ACCW ICT resources must not be used to humiliate, intimidate or offend another person/s based on their race, gender, or any other attribute prescribed under anti-discrimination legislation. Commonwealth and State laws and the ACCW Equal Opportunity policy prohibit sexual harassment and discrimination, vilification or victimisation on certain grounds such as race, gender, sexual preference, disability, or status as a parent or carer.

3.2.3 Forwarding of Emails – Privacy and Ownership of Copyright

ACCW owns copyright in all e-mail correspondence created by members of its staff in relation to their employment duties, excepting correspondence created by academic staff in respect to their research or being conducted in accordance with ACCW's Paid Outside Work Policy.

Copyright in work-related email will not be infringed by forwarding a message to another staff member or interested party (such as a consultant providing services to ACCW) on a need-to-know basis. However, care must be taken if an email contains personal information. Under *the Privacy Act 1988* (Cth), "*Personal Information means information or an opinion, whether true or not, about a person whose identity is apparent*". This kind of information must not be used or disclosed (including being forwarded to a third party via email or through other means) unless the use or disclosure is for the purpose for which the information was collected and is otherwise lawful. Copyright will be infringed if you send, without permission of the copyright owner, an audio or video file, music charts/lyrics, commercial photographs, journal article or report to another person using email.

3.2.4 Commercial Usage Prohibited

The private commercial use of e-mail and messaging is not allowed. Messaging and e-mail must not be used for private commercial purposes except where the paid work is conducted in accordance with the ACCW **Practice and Paid Outside Work Policy**, or the work is for the purposes of a corporate entity in which ACCW holds an interest.

3.2.5 Forwarding of emails after contract expiry or end-date

Email and computer access will cease on expiration of contract or end-date as recorded in the Human Resources database. An option to forward email to another external email account for professional or work- related reasons must be authorised by the Director or equivalent and shall not exceed 6 months.

4. Security of Information Technology Resources and Data

4.1 Records Management

Authorised Users are required at all time to take reasonable steps to ensure that important ACCW data is stored appropriately on ACCW servers for preservation and backup and observe appropriate ACCW record management protocols such as the Electronic Mail Recordkeeping Protocol.

4.2 Authorised User's Responsibilities

Authorised Users always have a responsibility to:

- Act lawfully;
- Keep all ACCW ICT resources secure and to observe the ACCW IT Security Policy;
- Not compromise or attempt to compromise the security of any IT Resource belonging to ACCW or other organisations or individuals, nor exploit or attempt to exploit any security deficiency.
- Take reasonable steps to ensure physical protection including damage from improper use, food and drink spillage, electrical power management, anti-static measures, protection from theft, and sound magnetic media practices;
- Ensure their computers are not left unattended without first logging-out and/or securing the entrance to the work area – particularly if the computer system to which they are connected contains sensitive or valuable information; and
- Adhere to the practices as set out in sections 4.2, 4.3 and 4.4 below.

4.3 Confidential Information

Authorised Users have a duty to keep confidential:

- All ACCW data unless the information has been approved for external publication; and
- Information provided in confidence to the ACCW by other entities.

Each staff member is under a duty not to disclose ACCW business information unless authorized to do so. Breach of confidentiality through accidental or negligent disclosure may expose a User to disciplinary action.

4.4 Personal Information

Personal information about an individual, including personal information that is also Health Information, must not be used or disclosed (including being sent by email or through some other

means to a third party) unless the use or disclosure is for a purpose for which the information was collected and the use is otherwise lawful.

4.5 ACCW Liability

The ACCW accepts no responsibility for:

- Loss or damage or consequential loss or damage, arising from the use of the ACCW ICT resources.
- Loss of data or interference with files arising from the ACCW's efforts to maintain the ACCW ICT resources.

5. Prohibited use of Information Technology Resources and Possible Consequences

5.1 ACCW Name and Logo

The ACCW Name or logo may only be used with prior approval from the Director. All use must be in accordance with the ACCW Visual Identity Manual or with the prior approval of the Director.

5.2 Unauthorised Access

Authorised users are expressly forbidden from unauthorised access or attempting to gain unauthorised access to ACCW ICT resources belonging to other organisations.

5.3 Infringement of Copyright

Authorised users are expressly forbidden to engage in any of the conduct described in the Schedule as infringing conduct. Wilful or negligent infringement of copyright (for example on personal pages or in breach of the statutory licence (CAL) may attract

- Personal liability for damages
- denial of access to computer facilities
- disciplinary action.

5.4 Databases, online journals, ebooks

Use of electronic resources provided by ACCW is governed by individual licence agreements. Users are required to comply with use restrictions set out on the specific site or stated in the licence agreement, and must not systematically download, distribute or retain substantial portions of information.

Any use of electronic resources must comply with the contractual terms of use of the electronic resource from which the material was sourced. Each electronic resource has its own set of contractual terms. To check whether your proposed usage falls within the relevant contractual terms, send an email to the Director. Your email should include a description of the way in which you propose to use the material and the names of the electronic resources (and journals) from which the material was sourced.

5.5 Peer to Peer File Sharing

Installation or use of peer to peer file sharing software such as Kazaa, BitTorrent, etc is not permitted on the ACCW network. Exceptions for legitimate use must be approved by the Director or delegate, and only where no alternative technology is appropriate.

5.6 Pornography

Authorised users are not permitted to utilize the ACCW ICT resources to access pornographic material or to create, store or distribute pornographic material of any type.

5.7 Gambling and crypto-currencies

Authorised users are not permitted to utilize the ACCW ICT resources to gamble or to mine crypto currencies.

5.8 Illegal Use and Material

ACCW ICT resources must not be used in any manner that is contrary to law or likely to breach the law. Any suspected offender may be referred to the police or other relevant authority and their employment may be suspended or terminated.

Certain inappropriate, unauthorised and non-work-related use of the ACCW ICT resources may constitute a criminal offence under the *Crimes Act 1958* (Vic). Examples include computer hacking, unauthorised and malicious release of data or documents and the distribution of malware.

Illegal or unlawful use includes (but is not limited to):

- use of certain types of pornography under the *Crimes Act 1958* (Vic), such as child pornography
- offences under the *Classification (Publications, Films and Computer Games) (Enforcement) Act 1995* (Vic)
- defamatory material
- material that could constitute racial or religious vilification, or unlawful discriminatory material
- stalking
- blackmail and threats under the *Crimes Act 1958* (Vic)
- use that breaches copyright laws, fraudulent activity, computer crimes and other computer offences under the *Cybercrime Act 2001* (Cth) or the *Crimes Act 1958* (Vic)
- breaches under any other relevant legislation

5.9 Offensive or Inappropriate Material

The use of ACCW ICT resources must be appropriate to a workplace environment and aligned to the values of ACCW. This includes (but is not limited to) the content of all electronic communications, whether sent internally within ACCW or externally from ACCW to third parties.

ACCW ICT resources must not be used for material that is pornographic, harassing, hateful, racist, sexist, abusive, obscene, discriminatory, offensive or threatening.

All users of ACCW ICT resources must familiarise themselves with relevant ACCW policies that address anti-discrimination, equal opportunity, bullying and harassment.

Users of ACCW ICT resources that receive unsolicited, offensive and/or inappropriate material via ACCW ICT resources should delete it immediately and report the matter to their manager. Where the sender of the material is known to the user, the user should notify the sender to refrain from sending such material again (if it is appropriate to do so).

Offensive or inappropriate material should not be forwarded internally or externally, or saved onto ACCW ICT resources, except where the material is required for the purposes of investigating a breach of the ACCW policies and/or a police investigation.

5.10 Malware

Electronic and web communications are potential delivery systems for malware. ACCW will use anti-virus and threat protection software to scan all data, programs and files downloaded electronically or attached to email messages before being launched, opened, accessed or sent.

Users are to treat all email and web communications with caution, particularly those communications with attachments and users should not open any attachments or click on any links embedded in an email unless the user is confident in the identity of the sender and has checked to confirm that the sender's email address on the email transmission matches the sender's usual email address.

Malware has the potential to seriously damage or otherwise adversely affect ACCW ICT resources and may cause ACCW to be in breach of its statutory obligations to maintain the privacy of personal information.

5.11 Social Engineering

In the context of information security, social engineering is the use of deception to manipulate individuals into disclosing confidential or personal information to an unauthorised recipient who may use such information for malicious or fraudulent purposes.

Phishing is a common form of social engineering. A typical example of phishing is sending an email that contains a link to a website that appears legitimate but includes or embeds malware that may expose the ACCW ICT resources (and the data and information stored on the ACCW ICT resources) to misuse, unauthorised use or disclosure.

Users are expected to be vigilant against social engineering and are required to report to their immediate manager any attempted social engineering attack.

5.12 Attribution

A user may be inadvertently be in breach of this policy due to false attribution. It is possible for a communication (such as an email) to be modified to reflect a false message, sender or recipient. In those examples, an individual may be unaware that he/she is communicating with an impostor or receiving false or misleading information.

Users are expected to verify the identity of a recipient or a sender of an electronic communication (such as an email) if the user suspects or is aware that the recipient or sender is or could be falsified. If a user believes that an email or other form of communication has been modified, altered or falsified, then the user should inform his/her immediate manager.

In accordance with the requirements of this policy, all users are responsible for the use of ACCW ICT resources that have been made available to them for work-related purposes and for all use of ACCW ICT resources that have been performed under their user identification (login and password information).

All users are always required to supervise and physically control all ACCW ICT resources , including mobile phones, tablets and notebook computers issued by or on behalf of ACCW to a user.

Users are expected to maintain the security and confidentiality of all credentials used to access and to use ACCW ICT resources, including login and password combinations. Users must not either undertake, assist or allow to be undertaken any unauthorised access to or use of the ACCW ICT resources (including through the use by a third party of the user's login credentials)

5.13 Possible Consequences

- **For ACCW Staff**

Staff found to have breached this policy will be subject to disciplinary action in accordance with the disciplinary procedures contained in the ACCW Enterprise Agreement or the relevant Terms and Benefits Policy and the ACCW Workplace Policies and Procedures as amended from time to time. Criminal offences will be reported to the police.

- **Authorised Users Other Than ACCW Staff**

Authorised Users (other than ACCW staff) found to have breached this policy may be subject to appropriate action as determined by the ACCW. Such action may include but is not limited to; sanctions and/or removal of access to ACCW ICT resources. Criminal offences will be reported to the police.

6. Privacy and Surveillance

6.1 Security and Privacy

The accounts, files and stored data including, but not limited to, e-mail messages belonging to users at ACCW are normally held private and secure from intervention by other users, including the staff of the Information Technology Services Division.

There are situations in which duly authorised Information Technology Services staff may be required to intervene in user accounts, temporarily suspend account access or disconnect computers from the network in the course of maintaining the ACCW ICT resources such as repairing, upgrading or restoring file servers or personal computer systems.

Users should be aware that Information Technology Services staff may from time to time become aware of the contents of user directories and hard disk drives in the normal course of their work, and they are bound to keep this information confidential.

Notwithstanding the foregoing, all users should be aware of and understand that electronic communication is not a secure means of communication. ACCW will use its best endeavours to maintain the security of the ACCW ICT resources but cannot guarantee this security (especially in relation to communications with external parties). Each user should consider the confidentiality, the privacy and the sensitivity of the material he/she intends to send when choosing the appropriate means of communication.

ACCW will handle any personal information collected through the use of ACCW ICT resources in accordance with its statutory obligations under the *Privacy Act 1988* (Cth), any application health records legislation and ACCW's privacy policy.

6.2 Access to and Monitoring

ACCW does not generally monitor e-mail, files or data stored on ACCW ICT resources or traversing the ACCW network. However, ACCW reserves the right to access and monitor any computer or other electronic device connected to the ACCW ICT network. This includes equipment owned by ACCW and personal computing equipment (e.g. laptops) that are connected to the network.

Access to and monitoring of equipment is permitted for operational, maintenance, compliance, auditing, legal, security or investigative purposes, including but not limited to, suspected breaches by the user of his/her duties as a staff member, unlawful activities or breaches of legislation and ACCW policies. Access to and monitoring includes, but is not limited to e-mail, web sites, server logs and electronic files.

If there is a reasonable belief that the ACCW ICT resources (or any of them) are being used contrary to the requirements of this policy by a user, the immediate manager of the suspected user is empowered under this policy to secure the relevant ACCW ICT resources while the suspected breach is investigated. The manager may also request that the user's access to and use of the ACCW ICT resources be suspended pending the outcome of the investigation.

The ACCW may keep a record of any monitoring or investigations.

6.3 Prior Approval Required

Prior written approval must be obtained from the Director or his/her delegate, before a user's e-mail, files or data may be accessed by authorised staff. Any information obtained under this approval will be treated as confidential, and only disclosed to relevant 3rd parties. Access to the information will be strictly on a need-to-know basis.

6.4 ACCW Property

All electronic communications created, sent or received using ACCW ICT resources are the property of ACCW.

Electronic communications may also be subject to discovery in civil litigation and criminal investigations.

7. Email Disclaimer

All emails sent externally from ACCW will automatically have a disclaimer attached to them.

All users must recognise and acknowledge that the inclusion of a disclaimer on any email or other electronic communication using ACCW ICT resources may not necessarily prevent ACCW or the sender of the email from being held liable for the email or other electronic communication (including the contents therein).

8. Complaints

If an ACCW employee has a complaint or a report of inappropriate use of the ACCW ICT resources, he/she should file such complaint or report with the immediate manager of the person the subject of the complaint.

If the complaint relates to the employee's immediate manager, the complaint should be directed to the manager above.

Complaints arising from the use of ACCW ICT resources or complaints arising from the application of this policy may be investigated in accordance with ACCW guidelines for managing complaints, misconduct and unsatisfactory performance for employees.

Schedule

Relevant Australian Legislation, Policies and Associated Documentation

Copyright *Copyright Act* (1968) (Commonwealth)

Copyright protects intellectual property rights in literary (including computer programs), dramatic, musical and artistic works (includes photographs/charts/maps) and in films/videos, recordings/tapes and TV and radio broadcasts. Use of any part of a copyright work without permission of the copyright owner will infringe copyright unless the use was for your personal research or study/criticism and review and in accordance with the fair dealing provisions of the Copyright Act OR for the educational purposes of the ACCW and in accordance with the statutory licence in the Copyright Act (1968) (Commonwealth).

Trademarks and Logos *Trade Marks Act* (1955) (Commonwealth)

A user must not copy a trademark or logo belonging to another party. Trademark infringement may expose the user to liability for damages.

Misleading and Deceptive Conduct *Trade Practices Act* (1974) (Commonwealth)

The Trade Practices Act contains provisions which prohibit passing off and misleading and deceptive conduct. For example, if a user were to copy material from an external site onto an ACCW website (including features such as logos and trademarks) so that persons accessing the website would believe that ACCW had been authorised to carry the material, this would constitute passing off or deceptive or misleading conduct.

Spam *Spam Act* (2003) (Commonwealth)

This legislation sets up a scheme for regulating commercial e-mail and other types of commercial electronic messages. Under the Act, users must not send unsolicited commercial electronic messages, i.e. messages that are sent without the recipient's consent. Any commercial messages that are sent electronically (including email, instant messaging or

Telephone accounts) must include information about the individual or organisation which authorised the sending of the message and provide for a functional unsubscribe facility.

Discrimination and HarassmentAnti-Discrimination Legislation

State and Commonwealth legislation prohibits discrimination based on age, impairment/imputed impairment, industrial activity, lawful sexual activity, marital status, physical features, political belief or activity, pregnancy, race, religious belief or activity, sex, parental status or status as a carer. It is also prohibited to victimise a person who has made a complaint of discrimination under these Acts.

Defamation

A user must not publish a statement about another person (or entity) which could harm that other person’s (or entity's) reputation. There is no need for the person to have been named specifically if he/she can reasonably be identified. Photographs and cartoons can also be defamatory if they hold someone up to ridicule or contempt. In a defamation case, truth is not always a defence.

Date Created	Review Date	Authorised by
3.7.2019	3 years	ACCW Board

Illegal material 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 and will also result in disciplinary action under the ACCW's disciplinary procedures.

Incitement to commit a crime

Users must not publish material which is an incitement to commit or instruction in crime eg, material on how to prepare explosive devices, or how to steal.

Associated Policies and Legislation (including Guidelines & Procedures)

- *Copyright Act* (1968) (Commonwealth)
- *Disability Discrimination Act* (Cwlth) 1992
- *Equal Opportunity Act* (Vic) 1995