[Insert organisation name/logo]

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY

**Version: [Year/no]**

**Document status: Draft or Final**

**Date issued: [date]**

**Approved by: [insert organisation name] Board of Directors on [date]**

**Date for review: [date]**

**Record of policy development:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version number** | **Date of issue** | **Lead author/ reviewer** | **Consultative panel** | **Significant changes on previous version** |
| [Year/no] | [Date] | [Name/role] | [Name/role/ organisation] | [For example, incorporate changes to new legislation] |
|  |  |  |  |  |

***Note\****

*This policy template has been developed to meet the needs of a diverse range of services and includes items for consideration in your policy.*

*NADA advises organisations to seek advice and review from their own IT provider.*

***Not all content will be relevant to your service.******Organisations are encouraged to edit, add and delete content to ensure relevancy.***

*All material provided by the Network of Alcohol and other Drugs (NADA) is for guidance purposes only. While this document has undergone pro bono legal review, NADA nor the legal reviewer accept legal responsibility for the implementation of this document within services.*

*All notes (like this one) should be considered and deleted before finalising the policy, and the contents list should be updated as changes are made and when content is finalised.*

*\*Please delete this note before finalising this policy.*

***Note\****

*To update the contents list when all content has been finalised, right click on the contents list and select ‘update field’, an option box will appear, select ‘Update entire table’ and ‘Ok’. To use the contents list to skip to relevant text, use* ***Ctrl and click*** *to select the relevant page number.*

*\*Please delete this note before finalising this policy.*

[INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY 1](#_Toc213658574)

[SECTION 1: ICT POLICY FRAMEWORK 3](#_Toc213658575)

[1.1 Policy statement 3](#_Toc213658576)

[1.2 Purpose and scope 3](#_Toc213658577)

[1.3 Definitions 3](#_Toc213658578)

[1.4 Principles 4](#_Toc213658579)

[1.5 Outcomes 5](#_Toc213658580)

[1.6 Delegations 5](#_Toc213658581)

[1.7 Policy implementation 7](#_Toc213658582)

[1.8 Risk management 8](#_Toc213658583)

[1.9 Consequences of breach of policy 8](#_Toc213658584)

[SECTION 2: POLICY IMPLEMENTATION 9](#_Toc213658585)

[2.1 ICT service agreement 9](#_Toc213658586)

[2.2 ICT Physical security 9](#_Toc213658587)

[2.3 Cyber security 10](#_Toc213658588)

[2.4 Data breach 12](#_Toc213658589)

[2.5 Technology access and passwords 12](#_Toc213658590)

[2.6 File, data and record management 12](#_Toc213658591)

[2.7 Copyright and software licenses 14](#_Toc213658592)

[2.8 Email, internet and social media usage 15](#_Toc213658593)

[SECTION 3: REFERENCES 18](#_Toc213658594)

[3.1 Supporting documents 18](#_Toc213658595)

[3.2 Related policies 18](#_Toc213658596)

[3.3 Legislation 18](#_Toc213658597)

# SECTION 1: ICT POLICY FRAMEWORK

## 1.1 Policy statement

**[Insert organisation name]** is committed to ensuring staff members have access to appropriate information and communication technology (ICT) infrastructure, tools, training and support which assists them to undertake their work efficiently and effectively.

## 1.2 Purpose and scope

This policy aims to provide **[insert organisation name]** with guidance in managing the ICT infrastructure and tools provided to staff and clients, and to ensure staff use of these resources is secure and appropriate. The policy also aims to provide **[insert organisation name]** with guidance to manage the risks associated with ICT management systems.

This policy applies to all employees, Board members, volunteers and student placements.

This policy is not intended to guide staff in administration and use of the website or other electronic systems. For clients’ use of communication and online equipment, refer to the Service and Program Operations Policy.

## 1.3 Definitions

|  |  |
| --- | --- |
| **Cloud-based technology** | A term that refers to applications, services or resources made available to users on demand via the Internet from a cloud computing provider. |
| **Cyber security** | Also known as computer security or IT security, this refers to the practice of protecting computer systems, networks, and data from digital attacks, theft, and damage to ensure the confidentiality, integrity, and availability of an organisation’s information. |
| **Electronic record** | Any piece of information or data which is created sent or received by a computer, phone or other electronic device. |
| **ICT consultants** | External consultants engaged to provide technical support via a helpline and remote access, in addition to program management support on database upgrades. |
| **ICT equipment** | Physical items that are used for information technology or communications purposes, including computers, tablets, printers, multi-function copiers, mobile or smart phones, cameras, and data projectors. |
| **ICT hardware or infrastructure** | Interchangeable terms to describe ICT equipment along with cabling, modems, routers, phone lines and other equipment required for the operation of ICT assets. |
| **[insert ICT allocated position e.g. ICT Officer]** | The staff member responsible for managing ICT, including infrastructure and client and organisational systems. |

|  |  |
| --- | --- |
| **ICT services** | Services provided by third parties for information and communication management, for example, access to the internet, web hosting services, phone services, website development, social media consultants and external ICT support. |
| **ICT software** | Any form of computer program which provides a service to users, such as Microsoft Office, Internet browsers (allows access to the internet), Outlook (email program). |
| **ICT systems** | Sets of procedures or ways of doing things. ICT systems include protocols and policies put in place by an organisation or a third party relating to the use of or access to ICT hardware or software. |
| **ICT system user** | A person who is set up with access to the organisation’s ICT systems. System users include all staff members but can also include anyone else who is explicitly authorised to use the organisation’s ICT systems, including students, consultants, Board members or volunteers. |
| **Information and communication technology (ICT)** | An umbrella term describing technology systems and objects that enable users to access, store, transmit, exchange and manipulate information, including computers, networks, telecommunications (telephone lines and wireless signals), software, data storage, and audio-visual systems. |
| **Information management** | Includes the creation, collection, storage, access, use and disposal of information assets. |
| **Knowledge Management** | The process of capturing, developing, sharing, and effectively using organisational knowledge. |
| **Public domain** | In relation to confidentiality is “common knowledge,” i.e. information that can be accessed by the public. |
| **Social media** | Media designed to be disseminated through social interaction, created using accessible publishing techniques. Social media allows for the easy sharing of existing content. Popular social media services include Facebook, Twitter, LinkedIn, blogs, Instagram, YouTube. |

## 1.4 Principles

The following principles guide **[Insert organisation name]**’s ICT policy:

1. Responsibilities for ICT management and administration are clearly defined.
2. An ICT strategy canvasses the current and future ICT needs of the organisation and aligns with the organisation’s strategic plan.
3. ICT purchases are made for a valid reason, in an approved way and in alignment with the ICT Strategy.
4. ICT tools and systems are “fit for purpose” and responsive to changing environments and technologies.
5. All relevant laws are complied with, including laws relating to data protection, notifying of data breaches, acceptable use of internet and email, software licensing, privacy, confidentiality, discrimination and harassment.
6. Staff, Board members, volunteers, contractors and students are entitled to training and other support to assist them in using ICT systems that are relevant to the work of the organisation and regular cyber security training
7. The organisation’s information and knowledge management processes align with current industry best practice, government and legal requirements.

These principles are derived from the [Australian and New Zealand Standards relating to *Corporate Governance of IT*, AS/NZS ISO/IEC 38500:2010.](http://www.professionalsaustralia.org.au/wp-content/uploads/sites/41/2014/11/Standards-Australia-Corporate-Governance-of-IT1.pdf)

## 1.5 Outcomes

The outcome of this policy is that **[insert organisation name**] has ICT systems which are:

* Secure
* Stable
* Efficient
* User-friendly

## 1.6 Delegations

|  |  |
| --- | --- |
| **Board of Directors** | * Endorse ICT policy * Ensure compliance with the ICT policy and procedure * Contribute to internal ICT strategies and activities. * Be familiar with the organisation’s legislative requirements regarding communication, privacy and the collection, data security and breaches, cyber security requirements, storage and use of personal information. * Approve larger ICT expenditure. * Understand the organisation’s ethical standards regarding communication, social media and the treatment of confidential information relating to the organisation’s clients, staff and stakeholders. * Comply with systems in place across the organisation to communicate appropriately and to protect the privacy of personal information of clients, staff members, contractors, volunteers, students and stakeholders. |
| **Business services/ management** | * Comply with the ICT policy and procedure. * Contribute to internal ICT strategies and activities. * Be familiar with the organisation’s legislative requirements regarding communication, use of technology, privacy and the collection, storage and use of personal information. * Understand the organisation’s ethical standards regarding communication, social media and the treatment of confidential information relating to the organisation’s clients, staff and stakeholders. * Ensure and comply with systems in place across the organisation to communicate appropriately and to protect the privacy of personal information of clients, staff members, contractors, volunteers, students and stakeholders. * Monitor ICT systems and procedures, including cyber security * Ensure orientation of new staff members to the organisation’s information and records management systems. * Facilitate alignment of ICT systems with other organisational projects and activities. * Authorise staff members to make a request from the **[insert IT allocated position/contractor]** for updating/purchase of new equipment in line with ICT strategy and plan. * Authorise access of new staff members or other people to the organisation’s ICT systems. * Authorise the redirecting of emails from staff who no longer work with the organisation. * Responsible for reviewing ICT contract and budgets.   **CEO/Manager**   * Ensure risk assessments are undertaken. * Monitor ICT budget in conjunction with **[insert allocated staff member]** and approve the expenditure of ICT equipment/services. * Ensure and comply with systems in place across the organisation to communicate appropriately and to protect the privacy of personal information of clients, staff members, contractors, volunteers, students and stakeholders. * Ensure cyber security processes regarding access of ICT systems. * Refer decisions to the Board where expenditure is beyond general CEO/Manager delegation or requires major departure from ICT strategy. |
| **Program services/clinical** | * Compliance with ICT policy and procedure. * Contribute to internal ICT strategies and activities. * Be familiar with the organisation’s legislative requirements regarding communication, use of technology, privacy and the collection, cyber security, storage and use of personal information. * Understand the organisation’s ethical standards regarding communication, social media and the treatment of confidential information relating to the organisation’s clients, staff and stakeholders. * Ensure and comply with systems in place across the organisation to communicate appropriately and to protect the privacy of personal information of clients, staff members, contractors, volunteers, students and stakeholders. * Act in accordance with organisational systems in place to protect privacy and personal information. * Responsible for determining whether they need new/updated ICT equipment/services to carry out their work. |
| **[Insert IT allocated position or external contractor]** | * Compliance with ICT policy and procedure. * Contribute to internal ICT strategies and activities. * Implement the organisation’s legislative requirements regarding communication, use of technology, privacy and the collection, storage and use of personal information. * Implement and comply with the organisation’s ethical standards regarding communication, social media and the treatment of confidential information relating to the organisation’s clients, staff and stakeholders. * Maintain equipment and keep systems up to date. * Seek approval for ICT expenditure from CEO/Manager. * Ensure that requests from staff for new/updated ICT equipment include **x** number of quotes required to ensure the best price is sought. * Select suppliers and equipment and recommend to CEO/Manager. * Seek approval from the CEO/Manager for providing or removing access to ICT systems. * Provide staff and other authorised people with access to ICT systems. * In conjunction with **[insert allocated position, for example administration officer],** introduce new staff to ICT systems and provide support/training for ongoing use. * Manage, communicate and implement the organisation’s cyber security incident process, incident register and incident response plan * Provide ongoing maintenance to equipment used by the organisation’s clients. * Recommend upgrades or service improvements in line with ICT strategy and/or based on changing environment. * Perform risk assessments, identify unacceptable risks to ICT, and consult with CEO/Manager on risk management strategy. |

## 1.7 Policy implementation

This policy is developed in consultation with **[insert organisation name]** staff and approved by the Board.

All staff, Board members, volunteers, contractors and students are responsible for understanding and adhering to this ICT Policy and to complete any mandatory training required such as cyber security awareness and software training.

Specific activities undertaken include:

* ICT updates are a standing agenda item in staff meetings
* This policy (and related procedure) is to be part of all **[insert organisation name]** staff orientation processes.
* Cyber security training for relevant staff to ensure risk prevention and monitoring
  + Mandatory induction training in recognising and reporting scams
  + Phishing simulation tests conducted annually
  + Regular updated training
* Review annual record retention and disposal
* Supervision of **[Insert IT allocated position or external contractor]** (if relevant).
* Review of ICT strategy/audit after the organisation’s strategic plan is reviewed.
* Report on ICT in the organisation’s Annual Report and other relevant publications.

## 1.8 Risk management

ThisICT policy is informed by and complies with, relevant legislation. *The* [*Privacy Act 1988*](https://www.legislation.gov.au/Series/C2004A03712) (Cth), and the [*Health Records Information Privacy Act 2002*](https://legislation.nsw.gov.au/view/html/inforce/current/act-2002-071) (NSW) (‘Privacy Laws’), govern the way [**insert organisation name]** manages personal and health Information.

Other risk management actions include:

* All staff, volunteers, students, volunteers, contractors and Board members are made aware of this policy during the orientation process.
* Staff are provided with ongoing training and support to assist them to use ICT systems safely.
* [Insert organisation name] invests in protection against, and proactively manages, cyber risk in its client and financial management activities. Refer to the supporting documents of this policy.
* As part of the organisation’s policy review schedule, this policy will be reviewed within **[insert number of years]** years unless circumstances require an earlier review.
* The need for improvements can be identified by any Board, staff member or client through feedback.
* ICT is a standing agenda item forstaff meetings.
* ICT systems and plans are appropriately monitored and controlled by the allocated staff member/contractor.

For further information on ICT risk management and mitigation procedures, refer to the Risk management policy.

## 1.9 Consequences of breach of policy

While all efforts will be made to help individuals to meet the requirements of this policy, any breach will lead to standard disciplinary procedures.

# SECTION 2: POLICY IMPLEMENTATION

## 2.1 ICT service agreement

All ICT service agreements must be reviewed by the **[insert organisation name]**’s CEO before entering into an agreement. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by the CEO.

Where an IT service agreement renewal is required, if the agreement has substantially changed from the previous agreement, **[insert organisation name]**’s CEO and relevant staff are to review before finalising the renewal. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by the **[insert organisation name]**’s CEO.

Refer to the organisation’s ICT procedure document for information relating to IT support.

## 2.2 ICT Physical security

For all servers, mainframes and other network assets, the area must be secured by closing and locking (where possible) all cabinets, while maintaining adequate ventilation. Access to the cabinets should be monitored and tracked.

It will be the responsibility of the **[Insert IT allocated position]** or ICT provider to ensure that this requirement is always followed. Any employee becoming aware of a breach to this security requirement is obliged to notify the **[Insert IT allocated position]** immediately.

All security and safety of all portable technology, such as laptop, notepads, iPad and mobile phones, will be the responsibility of the employee who has been issued with the device and they should complete an employee IT equipment agreement form (see supporting documents).  
  
Any loss, or damage to a laptop, company mobile or other equipment is to be reported to the **[Insert IT allocated position]** and an incident report or written notification will be required. In the event of loss or damage, the **[Insert IT allocated position]** will assess the security measures undertaken to determine if the employee will be required to reimburse the business for the loss or damage.

**2.2.1 IT Hardware Failure**

Where there is failure of any of the business’s hardware, this must be referred to the ICT manager or ICT provider immediately.

The ICT manager or ICT provider will advise management of any equipment that is unable to be repaired (either due to age, vendor support or damage). The ICT manager or ICT provider is not authorised to issue, or procure, new equipment without a purchase order from the organisation.

## 2.3 Cyber security

**[Insert organisation name]**, **[Insert IT allocated position]** or **ICT provider** are responsible for ensuring:

1. All accounts are secured with passwords and multi-factor authentication
2. All devices are protected with automatic updates
3. Mandatory cyber security training is regularly undertaken by all staff on:
   1. How to identify scam messages
   2. Being aware of email attacks via compromised email accounts/impersonation
   3. Vigilance about malicious software (ransomware)
   4. The importance of using Multi-factor authentication
4. All devices have anti-virus software installed and is always kept up to date.
5. Cyber security incidents follow the *Cyber security incident response plan* and are recorded in the *Cyber security incident management register*
6. All information used within the business adheres to the privacy laws and the business’s confidentiality requirements (refer to the organisation’s *Privacy policy)*
7. Data back-ups are conducted daily and stored in a cloud environment, with no limitation on storage duration.

**2.3.1 Cyber security incident management process (*Example*)**

* **Preparation**

**[insert organisation name]** has an ICT policy in place and the below supporting documents which is read and complied with by all new staff.

* + *Cyber security checklist*
  + *Cyber security incident response plan*
  + *Cyber security incident register*
* **Identification**

**[insert organisation name]**’s ICT manager or ICT provider detects and classifies potential security incidents based on their severity levels.

The ICT manager or ICT provider will initiate the *cyber security incident response plan* if required and will liaise with the relevant management personnel for isolation, remediation and ongoing protection.

* **Containment**

The ICT manager or ICT provider and the Management team at **[insert organisation name]** will implement short-term and long-term containment strategies to limit the spread and effect of the incident, such as isolating affected systems and networks and blocking malicious traffic and access attempts. Additional strategies include applying security patches and updates and collecting and preserving evidence for further analysis.

* **Eradication**

The ICT manager or ICT provider and the management teamwill identify the incident's root cause and remove it from the environment. This may involve removing malware and compromised files, closing vulnerabilities and security gaps, resetting passwords, revoking compromised credentials, and rebuilding affected systems from clean backups.

* **Recovery**

Once eradication is completed, the ICT manager or ICT provider will restore systems and operations to their normal state, e.g. restoring data and configurations from backups, testing and validating the integrity of restored systems, monitoring for any signs of re-infection or residual issues, and communicating the resolution to stakeholders.

* **Lessons learned**

**[Insert organisation name]** will ensure continuous improvement of the cyber security incident response process and will conduct a post-incident review and analysis, identifying strengths and weaknesses in the response process, updating incident response plans and procedures based on insights from the current incident, and providing additional training and resources to all staff.

Any employee breaching **[insert organisation name]**’s IT and cyber security policy will undergo a performance management or disciplinary process.

Refer to the supporting documents for more detailed information on **[insert organisation name]**’s handling of cyber security.

*The Australian Signals Directorate (ASD) is responsible for monitoring and responding to cyberthreats targeting Australian interests. Cyber security incidents, depending on level of severity, may be reported to ASD to ensure timely assistance is provided, if required. This may be in the form of investigations or remediation advice.*

***Note\****

*It is recommended that organisations register with the* [*ACSC Partnership Program*](https://www.cyber.gov.au/resources-business-and-government/partner-hub) *to ensure your organisation’s cyber security related information is always up to date*

## 2.4 Data breach

In accordance with the *Privacy Act 1988* (Cth), in the case of unauthorised access or disclosure of personal information (which could be as a result of a cyber security incident or other incident), **[insert organisation name]** which is recorded in the *Data breach incident report form template*.

The organisation assesses such data breaches where notifying individuals, or the regulator (Office of the Australian Information Commissioner), is required. Refer to **[Insert organisation name]**’s Privacy policy where this is covered in more detail and includes the *Notifiable Data Breach response plan template* as a supporting document.

Disclosure of **[insert organisation name]**’s records that does not comply with this policy and relevant legislation may lead to the instigation of disciplinary procedures with the employee or Board member who disclosed the records.

## 2.5 Technology access and passwords

The **[Insert IT allocated position]**, with support from the ICT Manager or ICT provider allocates initial passwords to each new user for access to the network, email, and/or other relevant database or software.

Employees are responsible for the security and complexity of their own password. Refer to the supporting document *Creating strong passwords* for more information.

To facilitate self-service password resets, each employee will be required to register a mobile phone, a (non-**[insert organisation name]**) email address and have access to an Authenticator application to ensure Multi-Factor Authentication

## 2.6 File, data and record management

**[insert organisation name]** recognises that information is a valuable organisational asset requiring effective management. This policy provides guidance on the way in which electronic information is created, collected, exchanged, retained, disposed of, used and disclosed. This includes the use of email to record information.

The policy complies with the requirements of the [*Privacy Act 1988* (Cth)](https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act), the [*Privacy and Personal Information Protection Act 1998* (NSW)](https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-1998-133) and the [*Health Records Information Privacy Act 2002*](https://legislation.nsw.gov.au/view/html/inforce/current/act-2002-071) (NSW) in relation to the management of personal information that the organisation collects and holds about its staff, Board, member organisations and stakeholders.

**2.6.1 Creation and collection of records**

For the purposes of this policy, a ‘record’ refers to all information collected, created, sent and received while carrying out business.

**[insert organisation name]** maintains both electronic records and hard copy records.

**2.6.2 Electronic records**

* Responsibilities for ICT management and administration are clearly defined and mapped in the organisation structure
* All electronic records relating to operations are maintained in **[insert organisation]** file system
* Access to these files will be provided to approved personnel, as required and relevant to their role. Any other requests for access to the files will be referred by the ICT manager or ICT provider to the **[Insert IT allocated position]** for approval.
  + 1. **Hard copy records**

Paper and other hard copy records are maintained by **[insert organisation name]** in relation togeneral administration, finance, organisational compliance, performance reporting, members, WHS, human resources, governance and internal and external program and project materials, research and reference material.

* + 1. **Retention and disposal**

The retention and disposal of records is managed by the **[Insert IT allocated position]**.

**[insert organisation name]**’sprocesses and procedures complies with the retention/disposal/de-identification requirements as per the Privacy Act 1988 (Cth), Australian Privacy Principles, the Privacy and Personal Information Protection Act 1998 (NSW), Information Privacy Principles, Health Records Information Privacy Act 2002 (NSW) and Health Privacy Principles with regard to records containing personal or health information.

A list of applicable retention periods for corporate, administrative and governance records, as determined by relevant legislation is in the *Record retention and disposal schedule* (supporting documents).

Secure disposal of electronic records may include the following activities:

* Wiping content from electronic medium
* Physical destruction of electronic medium
* Physical removal and destruction by registered contractors

Hard copy records are disposed of through the secure document destruction bin.

**2.6.5 Use and distribution of records, data and information**

Records created and collected by **[insert organisation name]** are used as needed to meet **[insert organisation name]**’s operational and legal requirements.

Relevant corporate records are distributed externally when necessary for the purposes of demonstrating funding and legislative compliance and demonstrating transparent organisational processes to **[insert organisation name]**’s clients.

Any use or disclosure of records, data and information relating to individual people is governed by applicable privacy laws and **[insert organisation name]**’s Privacy Policy.

**[insert organisation name]**’s [Privacy Policy](https://nadaau.sharepoint.com/:f:/s/Policies/EtSLVyxuj_VKhKwmyFuNtO4BmxD8eXqrh6us2Pqq63uCzA?e=GsFzef) contains further information about **[insert organisation name]**’s handling of personal information.

## 2.7 Copyright and software licenses

The *Copyright Act 1968* (Cth) protects the rights of creators of material including software, as well as documents, files or pictures on the internet. In addition, software and application developers routinely issue licenses or terms and conditions that users are required to comply with.

**[insert organisation name]** staff members are required to conform to the requirements of the *Copyright Act 1968* (Cth) and licenses for software use.

**2.7.1 Software licenses**

Copying **[insert organisation name]** software in a manner not consistent with the vendor’s license is strictly forbidden. If users are not sure what is and is not permitted under a particular license, they should speak to the ICT manager or ICT provider, or the vendor.

When **[insert organisation name]** disposes of equipment which contains software (other than the operating system) that is licensed to the organisation, the **[Insert IT allocated position]**  is to ensure that the software is removed by the external ICT consultant and that details of the software licence are retained for future staff use.

All computer software copyrights and terms of all software licences will be followed by all employees of the business.

**2.7.2 Software installation**

All software must be appropriately registered with the supplier where required. **[insert organisation name]** is the registered owner of all software.

All software installation is to be carried out by **[insert organisation name]**’s ICT Manager or ICT Provider. A software upgrade shall not be installed on a computer that does not already have a copy of the original version of the software loaded on it.

**2.7.3 Software usage**

All employees must receive training for all new software. Employees are prohibited from bringing software from other sources and loading it onto the **[insert organisation name]**’s devices.

Software cannot be taken home and uploaded to a non **[insert organisation name]** device.

Where an employee is required to use software at home, a **[insert organisation name]** device must be used.

Unauthorised software is prohibited from being used in the business. This includes the use of software owned by an employee and used within the business.

**2.7.4 Use of materials from the internet**

**[Insert organisation name]**’s staff should not use any material from the internet without prior permission. The primary rule is to assume all images are protected by copyright unless stated otherwise.

* Ask the owner of the material - you may need to negotiate a licensing agreement, which specifies how, where, and for how long you can use the image, including any fees.
* Purchase images - Websites like Shutterstock, Adobe Stock, Pexels, and Unsplash offer high-quality images under various licensing agreements (e.g., royalty-free, rights-managed).
* Always read the specific license terms to ensure your intended use (especially commercial use) is permitted.
* Utilise Creative Commons (CC) Licenses - these may require **[Insert organisation name]** tocredit the original creator, cannot be used for any revenue-generating activities, image must remain unchanged etc.

Unauthorised or out of license use of material can lead to expensive legal proceedings against the organisation. Any employee breaching **[insert organisation name]**’s policy on using external material will undergo a performance management or disciplinary process.

Any website that you draw the material from for research purposes should be referenced in the same way that a journal article or book would be referenced.

## 2.8 Email, internet and social media usage

This policy covers usage of **[insert organisation name]**’s email and internet systems by theirstaff and covers use of social media by staff in the following circumstances:

* If the social media site is established or used as a **[insert organisation name]** social media site
* If the social media is accessed using **[insert organisation name]** ICT systems or equipment
* If the staff member identifies themselves as a staff member of **[insert organisation name]** on the site, and/or
* If the content of the social media is specifically about **[insert organisation name]**.

Refer to the separate Social media policy for more details.

**2.8.1 Email passwords**

**[insert organisation name]**’sstaff and other users are required to keep their email passwords secure; refer to section 2.2: ICT security.

**2.8.2 Use of social media**

**[insert organisation name]** recognises the use of social media for open dialogue and the exchange of ideas, which is beneficial for the organisation and / or individual in their work or research capacity.

In using social media, staff members are asked to be considerate, to be transparent and to understand that even when posting in a personal capacity, they may be viewed as a representative of **[insert organisation name]**, and therefore their actions can impact upon **[insert organisation name]**’s reputation. Refer to the **[insert organisation name]** human resources policy, social media policy and code of conduct.

**2.8.3 Prohibited use**

The **[insert organisation name]** email, internet system, and social media sites shall not to be used for the creation, distribution or deliberate downloading of any disruptive or offensive messages, including discriminatory comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.

**2.8.4 Personal use**

Using a reasonable amount of **[insert organisation name]** resources for personal emails and accessing the internet including social media sites is acceptable as long as it:

* Does not interfere with the staff members’ work
* Is not in conflict with the business needs of the organisation
* Is not “prohibited use” under this policy, and
* Does not breach other **[insert organisation name]** policies including the **[insert organisation name]** Code of Conduct.

For clarity, the **[insert organisation name]** email addresses should not be used for retail mailing lists, placing personal orders, or registering for events in a personal capacity, as this increases the risk of hackers and phishing on **[insert organisation name]**’saccounts.

**2.8.5 Monitoring**

**[insert organisation name]**’s staff shall have no expectation of privacy in information they store, send or receive on the company’s email system, and any sites they browse on the internet. Although **[insert organisation name]** is not obliged to monitor email messages or internet usage, executive staff can direct an external ICT provider to monitor the email and internet usage of individual users without notice to the user where there is a concern relating to breaches of policy or the Code of Conduct.

**2.8.6 Enforcement**

Any staff member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

# SECTION 3: REFERENCES

## 3.1 Supporting documents

* Record retention and disposal schedule
* ICT equipment register
* Employee IT equipment agreement form
* ICT new user form
* ICT revoke user form
* Creating strong passwords
* Data breach incident report form
* Cyber security checklist
* Cyber security incident register
* Cyber security incident response plan

## 3.2 Related policies

* Privacy policy
* Communications policy
* Human Resources policy
* Service and program operations policy
* Social media policy

## 3.3 Legislation

* [*Privacy Act 1988*](https://www.legislation.gov.au/C2004A03712/2014-03-12/text)
* [*Privacy Amendment (Notifiable Data Breaches) Act 2018*](https://classic.austlii.edu.au/au/legis/cth/num_act/padba2017346/sch1.html)
* [*Copyright Act 1968 (Cth)*](https://www.legislation.gov.au/C1968A00063/2019-01-01/text)
* [*Fair Work Act 2009 (Cth)*](https://www.legislation.gov.au/Details/C2017C00323)
* [*Electronic Transactions Act 2000 (NSW)*](https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-2000-008)
* [*Associations Incorporations Act 2009 (NSW)*](https://legislation.nsw.gov.au/view/html/inforce/current/act-2009-007)

**3.4 Other references**

* [Notifiable data breaches | OAIC](https://www.oaic.gov.au/privacy/notifiable-data-breaches)
* [Australian Signals Directorate](https://www.cyber.gov.au/) resources
* [Standards and Performance Pathways NGO Services online (Knowledge Management)](https://spp.ngoservicesonline.com.au/)