[Insert organisation name/logo]

INFORMATION AND COMMUNICATION TECHNOLOGY 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 policy and procedure.*

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

*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. See the NADA Policy Toolkit User Guide for more editing tips.*

*\*Please delete 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 Ctlr and click to select the relevant page number.*

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

CONTENTSINFORMATION AND COMMUNICATION TECHNOLOGY POLICY 1

SECTION 1: INFORMATION AND COMMUNICATION TECHNOLOGY FRAMEWORK 6

1.1 Policy statement 6

1.2 Purpose and scope 6

1.3 Definitions 6

1.4 Principles 7

1.5 Outcomes 7

1.6 Delegations 8

1.7 Policy implementation 9

1.8 Risk management 10

SECTION 2: ICT STRATEGY 11

2.1 ICT Planning 11

2.2 Staff consultation 11

2.3 ICT needs and assessment 12

2.4 ICT planning template 12

SECTION 3: INFORMATION AND RECORD MANAGEMENT 13

3.1 Records 13

3.2 Creation and collection of data or files 13

3.3 File management system 14

3.4 Access and security 14

3.5 Records migration, retention and disposal 15

3.6 Use and distribution of records, data and information 16

3.7 Client information 17

3.8 The Privacy Act 1988 and Australian Privacy Principals 17

SECTION 4: PURCHASING OF ICT EQUIPMENT, SOFTWARE AND SERVICES 19

4.1 ICT tools 19

4.2 ICT purchasing or acquisition principles 19

4.3 ICT purchasing by the [insert IT allocation position] 20

4.4 No approval required 20

4.5 Staff members’ purchase of ICT equipment, software or services 20

4.6 Recording of ICT equipment, software and services 21

SECTION 5: ICT EQUIPMENT DISPOSAL 22

5.1 ICT disposal principles 22

5.2 ICT disposal timeframe 22

5.3 ICT disposal methods 22

5.4 Deletion of data prior to disposal 23

5.5 Recording disposals 24

SECTION 6: IT NETWORK 25

6.1 IT network components 25

6.2 Network security and anti-virus software 26

6.3 Network backup 26

6.4 Setting up user access to the ICT systems 26

6.5 Deleting a user or removing their access to ICT systems 26

6.6 Levels of access 27

6.7 Encryptions 27

6.8 Unauthorised access to or interference of data 27

6.9 Accessing the network from home 27

6.10 Maintenance of ICT equipment 27

SECTION 7: PASSWORDS 28

7.1 [Insert IT allocated position] responsibilities 28

7.2 User responsibilities 28

SECTION 8: COPYRIGHT AND SOFTWARE LICENCES 29

8.1 Software licences 29

8.2 Use of materials from the internet 29

8.3 Further information 30

SECTION 9: STAFF USE OF COMMUNICATION TOOLS 31

9.1 Email use 31

9.2 Social media use 32

9.3 Internet use 35

9.4 Phone use 35

SECTION 10: WEBSITE 37

10.1 Website hosting and security 37

10.2 Access to the website content 37

10.3 Website design or redevelopment 38

SECTION 11: INTERNAL CLIENT DATABASE 39

11.1 Access and maintenance 39

11.2 Updating records 39

11.3 Reporting and verification of data 40

11.4 Database security 40

11.5 Database improvement or redevelopment 40

SECTION 12: ICT STAFF SUPPORT 41

12.1 ICT support 41

12.2 ICT training 41

SECTION 13: INTERNAL REFERENCES 43

13.1 Supporting documents 43

13.2 Related policies 43

SECTION 14: EXTERNAL REFERENCES 44

14.1 Legislation 44

14.2 Resources 44

14.3 Websites 44

14.4 Others 44

# SECTION 1: INFORMATION AND COMMUNICATION TECHNOLOGY 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.

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

|  |  |
| --- | --- |
| **Consent** | Consent means voluntary agreement to some act, practice or purpose. Consent has two elements: knowledge of the matter agreed to and voluntary agreement. |
| **ICT assets or 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 IT allocated position e.g. ICT Officer]** | The staff member responsible for managing ICT, including infrastructure and client and organisational systems. |
| **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. |
| **Public domain** | In relation to confidentiality is “common knowledge,” i.e. information that can be accessed by the general public. |
| **Records** | Records refer to all information created, sent and received in the course of carrying out the organisation’s business. |
| **Social media** | Online tools or websites (e.g. Facebook, Twitter, YouTube, Instagram, etc.) that engage, create and share user-generated content, data and comments. |
| **Social media identification** | Online name, ID, user name or user account name of individuals when using online or social media tools and programs. |
| **Software** | Any form of computer program which provides a service to users, such as Microsoft Office Word (creates text-based reports), Internet Explorer (allows access to the internet), Outlook Express (email program), and so on. |

## 1.4 Principles

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

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, acceptable use of internet and email, software licensing, privacy, confidentiality, discrimination and harassment.
6. Staff, Board members, volunteers 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.

## 1.5 Outcomes

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

* Secure
* Stable
* Efficient
* User-friendly.

## 1.6 Delegations

|  |  |
| --- | --- |
| **Board of Directors** | * Endorse and ensure compliance with the ICT policy. * Contribute to internal ICT strategies and activities. * Be familiar with the organisation’s legislative requirements regarding communication, privacy and the collection, storage and use of personal information. * Approve outstanding ICT expenditure. * Understand the organisation’s ethical standards with regard to communication, social media and the treatment of confidential information relating to the organisation’s clients, staff and stakeholders. |
| **Business services/ management** | * Comply with the ICT policy. * 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 with regard to communication, social media and the treatment of confidential information relating to the organisation’s clients, staff and stakeholders. * Ensure systems are in place across the organisation to communicate appropriately and to protect adequately the privacy of personal information of clients, staff members and stakeholders. * Monitor information and communications technology systems and procedures. * Ensure orientation of new staff members to the organisation’s information and records management systems. * Facilitate alignment of ICT systems with other organisational programs, 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 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. * 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 with regard to communication, social media and the treatment of confidential information relating to the organisation’s clients, staff 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 in order to carry out their work. |
| **[Insert IT allocated position or external contractor]** | * Compliance with ICT policy. * 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. * 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 notification as to whether a number of quotes are required. * 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. * 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. * Make urgent ICT decisions to remedy a disaster, vulnerability or unacceptable risk to the organisation’s security, reputation or business effectiveness. |

## 1.7 Policy implementation

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

All staff, Board members, volunteers and students are responsible for understanding and adhering to this ICT Policy.

Specific monitoring and support activities undertaken include:

* ICT updates that are a standing agenda item in staff meetings
* This policy is to be part of relevant **[insert organisation name]** staff orientation processes.
* This policy should be referenced in relevant **[insert organisation name]** policies, procedures and other supporting documents to ensure that it is familiar to all relevant staff and is actively used.
* This policy will be reviewed in line with the quality improvement program and/or relevant legislative changes.
* Supervision of **[Insert IT allocated position or external contractor]** (if relevant).
* Review of ICT strategy after the organisation strategic plan is reviewed.
* Report on ICT in the organisation Annual Report and other relevant publications.

**🖌Note\***

Quality improvement programs provide opportunities to identify and review your service practices. If your organisation doesn’t have a quality improvement program it is recommended to develop one to ensure better outcomes for your organisation. For more information refer to the Organisational Development Policy of the NADA Policy Toolkit.

\*Please delete note before finalising this policy

This policy is implemented in conjunction with the following policies:

* Communications Policy
* Human Resources Policy
* Service and Program Operations Policy
* Risk Management Policy
* Financial Management Policy
* Program Management Policy.

## 1.8 Risk management

**[Insert organisation name]** develops and implements information and communication technology systems informed by and complying with relevant legislation. This ensures these systems are effective as well as regularly monitored.

Other risk management actions include:

* All staff, volunteers, students and Board Members are made aware of this policy during the orientation process.
* Staff are provided with ongoing support and training to assist them to use ICT systems safely.
* 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 and update.
* The need for improvements can be identified by any Board, management, staff member or client through feedback or quality monitoring systems.
* ICT is a standing agenda item forstaff meetings to discuss any relevant issues.
* 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.

# SECTION 2: ICT STRATEGY

This section ensures that **[insert organisation name]** develops and implements a consistent ICT strategy to effectively manage internal information and communication technology systems, in order to enhance the organisation’s operation and achieve its strategic goals.

This section provides guidance on the plans, mechanisms and tools that **[insert organisation name]** adopts in order to prioritise and provide organisational strategies for resolving ICT needs and inform ICT decision making.

This section ensures that the organisation:

* establishes within the organisation an ICT culture and a strategy that integrates ICT with the organisation’s mission and functions
* ensures that ICT complements and enhances the organisation’s service to its clients
* provides a structure for the continuing development of digital proficiency
* enhances the role of ICT in fulfilling the organisation’s mission and improving its function
* builds awareness of the cultural and operational importance of the digital revolution.

## 2.1 ICT Planning

The aim of ICT planning is to align the organisation’s ICT use, acquisition and management with the **[insert organisation name]**’s mission, vision and strategic plan. The organisation consults and engages all staff levels within the organisation including students, volunteers and Board members.

**[Insert organisation name]** reviews ICT plans and processes as part of organisation’s Policy Review Schedule, within **[insert number of years]** years unless circumstances require an earlier review and update.

ICT planning processes are managed by **[insert IT allocated position]** and guided by the CEO/Manager.

## 2.2 Staff consultation

**[Insert organisation name]** implements diverse consultation methods to seek feedback from employees, Board members, students and volunteers. This may include:

* Workshops
* Surveys
* Staff meetings
* **[Insert other consultation method].**

The purpose of the organisation’s ICT consultation is to:

* Build awareness and understanding of current ICT issues or activities
* Obtain general information of ICT guiding documents
* Validate, qualify and prioritise ICT needs
* Discuss possible approaches and solutions.

The organisation’s ICT Consultation Survey Template guides and informs the organisation’s ICT consultation processes.

## 2.3 ICT needs and assessment

**[Insert organisation name],** as part of the consultation processes with employees, implements an ICT Needs and Prioritisation Tool Template. ICT needs are then validated, qualified and priorities are established on the basis of criticality and urgency to assist in the development of the ICT Plan.

## 2.4 ICT planning template

Informed by the organisation ICT consultation processes and tools, the ICT Plan Template assists in developing the organisation’s ICT Plan in order to:

* develop awareness of the range of technological solutions that are available to the organisation
* develop an ICT acquisition strategy that ensures the optimum quality of ICT hardware and software is made available to staff
* establish protocols for monitoring the quality and use of ICT hardware and software
* improve staff training in ICT proficiency
* enhance the monitoring of staff ICT proficiency
* enhance staff record-keeping and client management systems
* provide stock control processes that include maintaining up-to-date registers of ICT hardware and software
* realise the potential for co-operation, communication and referral between all organisations providing services to our clients
* ensure management board supervision of the organisation’s ICT proficiency.

The current **[insert organisation name]** ICT Plan is located in **[insert electronic file name and folder location]**.

# SECTION 3: INFORMATION AND RECORD MANAGEMENT

**[Insert organisation name]** recognises that information is a valuable organisational asset requiring effective management and that all its related activities should be delivered accordingly.

The purpose of this section is to provide guidance to **[insert organisation name]** on the manner in which electronic information is created, collected, exchanged, retained, disposed of, used and disclosed by the organisation.This includes the use of email to record information.

The section conforms to the current legislation and aligns with the Privacy and Confidentiality Section of the **[insert organisation name]** Communications Policy in relation to the management of personal information that it collects about its staff, Board, students, volunteers and stakeholders, as well as client information.

For Client File Management refer to the Service and Program Operations Policy and Client Clinical Management Policy for specific information on case notes.

This section applies to all staff, volunteers, students and Board members.

This section also ensures that:

* File management systems are systematic, compliant with legislation and quality standards, informative and protects the interests of the organisation
* Internal organisational files are effectively established, reviewed, maintained and retained
* Employees, students, volunteers and Board members’ information is secure, accessible, relevant and used primarily for the purpose it is being collected.

## 3.1 Records

The organisation maintains and creates paper and electronic records that are authentic, reliable, legible, have integrity, and are usable.

The organisation aims to ensure information it collects, uses or discloses is accurate and complete at the time it is collected. In the event that clients wish to correct errors in their information, these corrections will be made in all circumstances where it is reasonable to do so.

Managing information and records to meet **[insert organisation name]**’s operational and legal requirements includes:

* Managing records throughout their life cycle
* Documenting activities and decisions
* Filing, securing and storing information
* Documenting, protecting and preserving information critical to the organisation’s business systems.

## 3.2 Creation and collection of data or files

**[Insert organisation name]** only creates and collects records to meet the organisation’s operational and legal requirements. Information that provides evidence of decisions, strategies, activities, and outcomes related to **[insert organisation name]**’s operations are to be created and collected. This includes internally and externally generated records, whether they are created through email, word processing software, databases, spreadsheets, scans, or by other means.

Electronic record-keeping is the preferred format for maintaining records in order to increase their accessibility and minimise unnecessary use of paper. Some paper records may be scanned and saved in electronic format only, or with the original also maintained and filed. Original paper documents containing signatures are to be maintained in physical filing systems.

Final versions of key corporate records, such as Board meeting minutes, annual reports, and staff disciplinary matters, are to be filed in an unalterable **[insert file format, for example PDF]** format and maintained for the length of time specified in the relevant legislation and with the necessary security set out in the Communications Policy and Human Resources Policy.

## 3.3 File management system

The file management system on **[insert organisation name]**’s ICT network follows a business classification scheme that shows the organisation’s functions, activities and transactions in a hierarchical relationship.

A map to using the organisation’s electronic drives and files is provided to all staff members at commencement of their employment or placement within the organisation and is guided by the Electronic Records Map template.

Work-related information should never be saved directly to ICT equipment (hardware); all electronic records relating to the organisation’s operations are maintained on the **[insert name and file location on the internal shared network].**

All staff are provided with an individual drive for personal use, with access restricted to the specific staff member. Records relating to **[insert organisation name]** operations are not to be maintained in individual drives.

**🖌Note\***

Organisations are advised to delete/amend/adapt the above statement, based on their internal ICT arrangements and equipment. In some cases, staff members have access to the same files and senior staff members are provided with individual and privates drives, according to the type of information they are managing.

Organisations using cloud storage need to consider if the collection, transfer, processing, storage and security / protection of personal data aligns with the Australian Privacy Principles. For more information refer to the Commonwealth of Australia (Digital Transformation Agency), Secure Cloud Strategy, 2017.

\*Please delete this note before finalising this policy.

## 3.4 Access and security

Records are kept secure, with staff members having access through their computer log-in account and password.

Board members have access to governance, finance and compliance records through **[insert organisation name]** Board meetings and specific requests through the CEO/Manager.

Student placements and volunteers are provided with limited electronic record access through computer log-in.

In order to maintain electronic record security, staff are required to set up an automatic locking screensaver that comes on when users are away from their desk for a set time period. Levels of access to **[insert organisation name]**’s electronic records vary, according to position and responsibility of the staff member, as outlined below:

|  |  |
| --- | --- |
| **Drive** | **Access by** |
| **[Insert drive name: for example general shared, human resources, clients, quality improvement]** | **[insert access person: for example all staff, CEO/Manager, finance officer]** |
| **Example**  **Human resources** | **Example**  **CEO/Manager and related supervisors** |
|  |  |

Stakeholders, visitors, consultants, clients and other non-staff members are not provided with access to any **[insert organisation name]** electronic records unless it is necessary for their work. The CEO/Manager makes determination on such access as required, ensuring optimum privacy and security levels are maintained.

For further details on information managed by specific staff members, please refer to the List of Information Custodians. For information on deleting or removing staff access see Section 6.5.

## 3.5 Records migration, retention and disposal

The retention and disposal of electronic records is to comply with relevant legislation, including:

* Privacy Act 1988 (Cth)
* A New Tax System (Goods and Services Tax) Act 1999 (Cth)
* Electronic Transactions Act 2000 (NSW)
* Fair Work Act 2009 (Cth)
* **[Insert other relevant legislation for example your organisational entity, Associations Incorporations Act 2009 (NSW)].**

Certain corporate records must be retained for a period of time as identified in relevant legislation and/or as determined by the organisation – refer to the **[insert organisation name]** Record Retention and Disposal Schedule.

The rise in predominance of electronic communication has elevated email systems to a comparable level as hard copy filing systems. The Email Retention Guide[[1]](#footnote-1) assists **[insert organisation name]** staffdetermine what information sent or received by email should be retained, for how long, the broad categories of electronic messages processed by **[insert organisation name]** and sets out the factors to be considered in setting practice guidelines to be adopted in each case.

In the event that electronic records are required to be retained over a period of time where data/information access and storage technology becomes obsolete, e.g. CD’s and CD drives are phased out in favour of USB’s and USB drives, **[insert organisation name]** has developed a strategy to migrate the records to a suitable medium that renders records readily accessible using current technology. Refer to the ICT Plan for further details.

***🖌Note\****

*Records Migration is a process whereby the integrity and accessibility of data, long term, is secured. Data retained in a format that is no longer accessible with today’s technology could be viewed as ‘lost’ forever. Examples include:*

*- floppy disc drives as a standard feature on computers were phased out in favour of CD drives; hence historical data stored on floppy discs is no longer readily accessible*

*- software platforms for recording client data, e.g. your client database system, are changed in favour of an alternative client database package, with minimal meshing and transference of data*

*General guidance on records migration can be found at the NSW State Archives and Records website.*

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

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
* **[Insert other activity].**

The disposal of corporate records is managed by **[insert allocated position]**.

The disposal of program, services and project records is managed by **[insert allocated position]**.

Documents containing confidential or sensitive information are to be shredded using the organisation shredder located in **[insert shredder location].**

Bulk amounts of documents containing confidential or sensitive information are shredded by **[insert external contractor, if applicable].** Bulk documents for shredding are placed in **[insert secure document disposal equipment e.g. wheelie bin, bag, etc.]** located in the **[insert equipment location].**

Once the secure document disposal equipment is full, the contractor is contacted for secure disposal of the contents.

**🖌Note\***

If your organisation manages a large amount of confidential and sensitive information, make sure the organisation is implementing the most secure system to manage the disposal and destruction of that information.

This may include utilising onsite shredders, secure bins, external contractors or others tools to protect the privacy of the organisation, clients, staff members, volunteers and Board members.

\*Please delete note before finalising this policy

## 3.6 Use and distribution of records, data and information

Records created and collected by **[insert organisation name]** are used only to meet organisational goals and for the purpose they have been created and collected, complying with all legal requirements.

Relevant corporate records are distributed externally only for the purposes of demonstrating funding and legislative compliance, and demonstrating transparent organisational processes to clients, stakeholders and the broader community.

Program, services and project information is distributed externally as part of project management/ event management processes. For further information refer to the Program Management Policy.

In relation to information that the organisation may collect relating to individuals, please refer to the Privacy and Confidentiality Section of the **[insert organisation name]** Communications Policy.

Disclosure of collated or created records that does not comply with this policy and the Communications Policy and other relevant legislation may lead to the instigation of disciplinary procedures with the relevant employee, student, volunteer or Board member.

Re-usable information is made widely available across the organisation to avoid redundancy and duplication of effort, and is organised and described in a way that makes the information visible and easily re-used.

Information is shared within and outside the organisation, in line with the mechanisms outlined in the Communications Policy.

## 3.7 Client information

**[Insert organisation name**] collects and provides information to and about clients through a range of communication mechanisms and acts in accordance with the Communications Policy and the Client Clinical Management Policy.

Client data is collected using the internal client database as outlined in this policy.

## 3.8 The Privacy Act 1988 and Australian Privacy Principals

This policy complies with the Privacy Act 1988, including the 13 Australian Privacy Principles (APPs), and outlines the management of personal information by **[insert organisation name],** including how the organisation collects, holds, uses and discloses personal information, including notification of data breaches, and also how individuals can access and seek correction of that information.

For the purpose of this policy **[insert organisation name]** abides by the Privacy Act 1988, taking into account the following amendments:

* Federal Circuit Court of Australia (Consequential Amendments) Act 2013
* Privacy Amendment (Enhancing Privacy Protection) Act 2012, and
* Privacy Amendment (Notifiable Data Breaches) Act 2017

Under the Privacy Amendment (Notifiable Data Breaches) Act 2017, an eligible data breach happens if:

1. there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity; and
2. the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates.

An entity must give a notification if:

1. it has reasonable grounds to believe that an eligible data breach has happened; or
2. it is directed to do so by the Commissioner.

In the event of a data breach at **[insert organisation name]**, the CEO/Manager, in consultation with the Board will take the following steps:

1. Notify the agency responsible for the data collection
2. Immediately commence an investigation into how the breach occurred
3. Notify the individuals whose personal data was breached with an explanation of steps being taken to ameliorate the situation
4. Depending on the severity and/or nature of the data breach, determine the need for implementation of **[insert organisation name]**’s Crisis Communications Plan, Media Releases to reassure the wider public, etc. - see section 4.5 of the Communications Policy for more information
5. Determine best course of corrective action, implement it and monitor to ensure that the event does not recur

**🖌Note\***

In 2014, the Australian Privacy Principles (APPs) replaced the National Privacy Principles (NPPs) that previously applied to organisations in the regulation of handling of personal information.

There are thirteen Australian Privacy Principles (APPs) and they are divided into five parts:

Part 1 - Consideration of personal information privacy

APP 1 - open and transparent management of personal information

APP 2 - anonymity and pseudonymity

Part 2 - Collection of personal information

APP 3 - collection of solicited personal information

APP 4 - dealing with unsolicited personal information

APP 5 - notification of the collection of personal information

Part 3 - Dealing with personal information

APP 6 - use or disclosure of personal information

APP 7- direct marketing

APP 8 - cross-border disclosure of personal information

APP 9 - adoption, use or disclosure of government-related identifiers

Part 4 - Integrity of personal information

APP 10 - quality of personal information

APP 11 - security of personal information

Part 5 - Access to, and correction of, personal information

APP 12 - access to personal information

APP 13 - correction of personal information.

For more information about the new 13 Australian Privacy Principles (APPs,) refer to the OAIC website.

To find more information about your organisation’s responsibility under the new Privacy Act 1988 refer to the OAIC website.

\*Please delete note before finalising this policy.

For further information on how **[insert organisation name]** manages privacy, refer to the Privacy and Confidentiality Section of the Communications Policy.

# SECTION 4: PURCHASING OF ICT EQUIPMENT, SOFTWARE AND SERVICES

**[Insert organisation name]** encourages the appropriate and timely acquisition of ICT equipment to support the organisation’s operations, including research, programs, services and activities.

This section provides guidance to **[insert organisation name]** in purchasing ICT equipment, software and ICT services to suit the organisation’s needs.

The organisation ensures that all ICT equipment, software and services are used and disposed of in an ethical and responsible manner and recognises the need to be consistent, cautious and thorough in the way that these tools support the organisation’s operations.

This section ensures that:

* **[Insert organisation name]** provides quality, reliable and up-to-date equipment and software to its employees in order to provide quality services.
* The organisation complies with both legislative requirements and ethical obligations in the purchase and use of equipment, licences and other ICT supportive services.
* All staff, Board members, students and volunteers understand their responsibilities in relation to purchasing ICT equipment.

## 4.1 ICT tools

As defined in Section 1.3 of this policy, **[insert organisation name]** identifies different types of ICT tools; this includes:

* **ICT equipment:** electronic hardware items that include computers, tablets, printers, multi-function copiers, mobile/smart phones, cameras, and data projectors.
* **ICT software:** electronic software items that include programs, operative systems, data management systems and antivirus software programs.
* **ICT services:** include internet services, web hosting, phone services, website development, and IT support.

## 4.2 ICT purchasing or acquisition principles

The general principle underpinning this policy is that ICT purchases are made for a valid reason, in an approved way, and in alignment with the ICT Strategy.

**[Insert organisation name]** is committed to purchasing the most cost-effective ICT goods and services primarily with regard to price, but also relating to quality, reliability, service, delivery and efficiency. This may mean, for example, that a slightly higher priced item or service might be chosen if it is from a supplier that has proven to be reliable in the past.

**[Insert organisation name]** has a commitment to consider environmental and ethical manufacturing issues wherever possible.

## 4.3 ICT purchasing by the [insert IT allocation position]

Where the **[insert IT allocated position]** determines that new ICT equipment, software or services are required as part of the maintenance of current ICT infrastructure, or to further the implementation of the organisation’s ICT Strategy, the following procedures are utilised:

* The **[insert IT allocated position]** sources the item, keeping in mind the organisation’s purchasing principles.
* There is no need to source three quotes UNLESS funding for the item is coming from a funding agreement which specifies that quotes must be sourced for purchasing of assets.
* The **[insert IT allocated position]** collects relevant information about the item and the quote/s, and presents these to the CEO/Manager for approval.
* Once approval is given, the **[insert IT allocated position]** can place the order.
* The **[insert IT allocated position]** can arrange to pay using the assigned organisation’s credit card, or will request the supplier that it be payable on invoice.
* Once the invoice has been received, the **[insert IT allocated position]** completes the organisation’s Supplier Claim Form, attaches the Tax Invoice, receipt, and or contract, then forwards the paperwork to the **[insert allocated staff member, for example financial or administration officer].**
* When the item is delivered or the service commences, it is the responsibility of the **[insert IT allocated position]** to ensure that it matches the order or the contract and that it is in perfect working order as per the product and technical specifications. Any disputes should be referred to the CEO/Manager. **[Insert IT allocated position]** is responsible for entering the item into the asset register.

## 4.4 No approval required

The **[insert IT allocated position]** is not required to seek approval from the CEO/Manager in relation to the following:

* Renewal of domain names
* Renewal or upgrades of anti-virus software and other security software
* Renewal of a service contract which is substantially the same as the original one, in terms of price and service provision
* Purchasing low-value **[insert maximum $ amount, for example <$100]** accessories
* Purchasing equipment, software or services to meet an urgent, critical business need; for example, equipment designed to troubleshoot serious IT problems.

For all these situations, the **[insert IT allocated position]** must provide receipts/invoices, the Supplier Claim Form, and all other relevant documentation to the **[insert allocated staff member, for example financial or administration officer]** for processing.

In relation to expenditure over the maximum amount of **[insert amount, for example $100]** to fix urgent problems, once the immediate problem is resolved, the **[insert IT allocated position]** should provide an explanation of why usual purchasing procedures could not be followed and seek retrospective approval from the CEO/Manager.

## 4.5 Staff members’ purchase of ICT equipment, software or services

The following procedure is to be followed by staff members, other than the **[insert IT allocated position]** when they wish to purchase ICT equipment, software or services required for their project or other work:

* Staff identify what item they need, and why they need it, given the requirements of their project responsibility, the budget for their project, as well as their alignment with the organisation’s ICT Strategy.
* The staff member checks the relevant funding agreement (if appropriate) to determine whether they need to seek quotes before purchasing any items with the project funds.
* Staff members seek approval for the purchase from their manager/direct supervisor, outlining the reasons for their request; if possible, they forward this request by email.
* Manager/direct supervisor discusses the request with the staff member, then makes a decision based on the needs of the project and of the staff member, the budget, and ICT Strategy.
* The manager should notify the staff member of their decision, if possible by email.
* If approved, the staff member should forward the **[insert IT allocated position]** their request, their manager’s approval, and advice as to whether quotes are required under the funding agreement.
* The **[insert IT allocated position]** or the staff member should source appropriate item/s, keeping in mind the organisation’s purchasing principles, and then decide what item should be purchased.
* The **[insert IT allocated position]** should then follow the procedure set out in Section 4.3 of this policy, to get approval from the CEO/Manager and submit paperwork to the **[insert allocated staff member, for example financial or administration officer]**.

In urgent situations, a staff member can purchase an ICT item without involving the **[insert IT allocated position]** if they have approval from their manager/direct supervisor. After this purchase is made, they must supply the **[insert IT allocated position]** with a copy of all documentation, including the Tax Invoice, so the details can be entered into the ICT Equipment Database / records. The staff member is then responsible for providing the Supplier Claim Form and other relevant documents to the **[insert allocated staff member, for example financial or administration officer]**.

## 4.6 Recording of ICT equipment, software and services

**[Insert IT allocated position]** records all new equipment, software and ICT services in an Excel spreadsheet/database titled ICT Equipment Database**.**

Information recorded in this spreadsheet includes information on purchase date, price, serial or other identification number, supplier/service provider details, physical location (e.g. which desk or staff member has it). For software, the information includes the number and expiry dates of licences and for ICT services, and the start and end dates of the contract.

The **[insert IT allocated position]** will update the spreadsheet/database whenever changes occur to items; for example, change in location or users, lost, damaged or equipment that has been disposed of.

The **[insert IT allocated position]** will also keep soft- and hard-copy certificates of software licences in **[insert electronic name and folder location].**

The **[insert IT allocated position]** will provide a copy of the spreadsheet/database to the **[insert allocated position for example Finance Officer]** towards the end of the financial year for reconciliation against depreciation records. A copy will also be provided to the administration team / allocated position to ensure administrative processes are up-to-date.

# SECTION 5: ICT EQUIPMENT DISPOSAL

**[Insert organisation name]** is committed to providing appropriate disposal methods to ensure all equipment is safely disposed of and organisational information is adequately protected.

This section provides guidance to **[insert organisation name]** staff members in disposing ICT equipment.

This section ensures that:

* **[Insert organisation name]** ICT equipment is disposed of safely and appropriately.
* The organisation complies with ethical and environmental requirements in the disposal of   
  ICT equipment.
* All staff, Board members, students and volunteers understand their responsibilities in relation to disposing of ICT equipment.

## 5.1 ICT disposal principles

**[Insert organisation name]** will ensure that ICT equipment is disposed in a manner which is:

* Transparent
* Cost-effective
* Environmentally sound
* Does not compromise the privacy or security of the organisation
* **[insert other principle].**

## 5.2 ICT disposal timeframe

ICT equipment will be retired or disposed of when it fails, is ineffective, is beginning to cost more to maintain than the cost of purchasing a replacement item, or is nearing the end of its effective lifecycle.

**🖌Note\***

Organisations may wish to document estimations of the effective lifecycle of equipment based on the ATO and on their own experience. This can be documented in the ICT Equipment Database and/or the Asset Register.

\*Please delete note before finalising this policy.

## 5.3 ICT disposal methods

ICT items can be disposed of in a range of ways, including sale, trade-in, donation to employees or other organisations, or throwing away these redundant items.

A decision pertaining to how to dispose of equipment should be made on a case-by-case basis, through discussions between the **[insert IT allocated position]** and the CEO/Manager, and taking into account the principles set out above, particularly the need for transparency.

Given the short life of most personal-use ICT items, **[insert organisation name]** generally will not consider a sale or trade-in on such items unless the anticipated profit to the organisation will clearly be greater than the cost in the **[insert IT allocated position]**’s time spent arranging the sale or trade-in.

### 5.3.1 Donations to other organisations

**[Insert organisation name**] may wish to offer such items for donation to other non-profit organisations; for example, in the **[insert local area name]** area or a **[insert partner organisation name]**.

In offering an ICT item, organisations will be advised of the following warnings:

* **[Insert organisation name]** makes no guarantees or warranties as to the condition of the item
* **[Insert organisation name]** is under no obligation to repair or maintain the item in the future
* **[Insert other warning statement].**

### 5.3.2 Donations to staff

If sale, trade-in or donation of an ICT item to other organisations are not considered feasible, **[insert organisation name]** may want to consider offering the item to staff members. Usually the staff member who most recently used the item will be offered first option to purchase the item.

In offering an ICT item, staff members will be advised of the following warnings:

* **[Insert organisation name]** makes no guarantees or warranties as to the condition of the item
* **[Insert organisation name]** is under no obligation to repair or maintain the item in the future
* **[Insert other warning statement].**

If the current staff user does not want the item, the **[insert IT allocated position]** will send an email to the rest of the team and ask if anyone else would like the item. If more than one person is interested, the **[insert IT allocated position]** will ask those interested to give reasons why they want or need the item, then discuss with the CEO/Manager who should receive the item. Considerations include:

* Whether the staff member/s have in the past received other ICT items
* Which staff member has a greater personal need for the equipment; for example, is currently a student or has no other ICT equipment at home.

### 5.3.3 Recycling and environmentally responsible disposal

Where items are not able to be passed on to staff or other organisations, the **[insert IT allocated position]** should make reasonable attempts to dispose of the item in a manner that does not contribute to landfill. Some e-waste recycling/disposal companies offer free disposal if organisations drop-off their superseded items.

**🖌Note\***

For further information on recycling in your area visit the Planet Ark, Recycling near you website or visit your local council website to find recycling options.

\*Please delete note before finalising this policy.

If, after reasonable efforts have been made, the **[insert IT allocated position]** is unable to locate a recycling or environmentally responsible disposal option at nil or low cost, the **[insert IT allocated position]** will dispose of through the usual garbage disposal methods.

## 5.4 Deletion of data prior to disposal

Before disposing of items (whether by providing to staff members for personal use, to another organisation or to e-waste services) the **[insert IT allocated position]** will securely deleteall data and software so as to protect **[Insert organisation name]**’s privacy, comply with copyright law, and minimise the risk of data harvesting.

## 5.5 Recording disposals

The **[insert IT allocated position]** will record all ICT records disposals in the ICT Record Retention and Disposal Schedule. All ICT equipment and tools disposals are recorded in the ICT Equipment Database.

Details to be recorded include: the date, disposal method, where/who the item goes to, who authorised the disposal, and any income derived from that disposal.

# SECTION 6: IT NETWORK

**🖌Note\***

The following section provides general guidance to organisations in accessing and maintaining IT networks. Organisations are encouraged to amend/delete the section if is not relevant to the organisation’s facilities and/or equipment.

\*Please delete note before finalising this policy

**[Insert organisation name]** understands that a quality internal communication network is a crucial component to ensure communications and business are carried out inside the organisation to allow staff members to achieve organisational goals and outcomes.

The purpose of this section is to provide guidance to **[insert organisation name]** staff members into how the organisation accesses, manages and updates the internal network.

The following processes ensure that staff members, Board of Directors, students and volunteers are provided with a reliable and stable IT network. This section ensures that:

* Staff members are able to work in a shared network environment
* Organisation files are current, secure and up-to-date
* Back-up systems and procedures are in place to protect internal documentation
* Private and confidential information is appropriately managed according to current legislation
* The network is used in a manner that is consistent with the organisation’s values, legal requirements, related policies, and code of conduct.

**🖌Note\***

Organisations are encouraged to consider the use of cloud as part of their overall ICT Strategy. For guidance, refer to the Commonwealth of Australia (Digital Transformation Agency), Secure Cloud Strategy, 2017.

\*Please delete this note before finalising this policy.

This section does not provide guidance on network/server or other equipment types and providers.

## 6.1 IT network components

**[Insert organisation name]** has a computer network consisting of:

* **[insert number]** desktop computers
* **[insert number]** printer(s)
* **[insert number]** firewall(s)
* **[insert number]** server(s)
* **[insert number]** back-up hard drive(s)
* Multifunction copier (printer, scanner and fax machine)
* **[insert number]** router(s).

**🖌Note\***

Organisations are encouraged to draw an internal network diagram and attach the document to this policy.

\*Please delete note before finalising this policy

## 6.2 Network security and anti-virus software

* The **[insert IT allocated position]** is responsible for ensuring that the computer network is secure from external attacks. Firewalls and anti-virus software are installed for this purpose.
* The **[insert IT allocated position]** is responsible for installing anti-virus software on the server(s) and every desktop computer. The software is set to auto-update virus definitions.
* The **[insert IT allocated position]** is responsible for evaluating the performance of the anti-virus software at relevant intervals and renewing or switching to a new anti-virus software / licence, as required; all software information is available on the ICT Equipment Database.

## 6.3 Network backup

The **[insert IT allocated position]** is responsible for ensuring that file server(s) are backed-up regularly. The procedure for this back-up is as follows:

* Server(s) are backed-up [**insert number of back-ups a month, for example 4]** times per month on **[insert back up days, for example Monday and Fridays]** into **[insert back-up drive name].**
* Once every 6 months the **[insert IT allocated position]** will conduct a test of each of the back-up hard drives to check that they are correctly backing-up all data.
* **[insert other backup procedure action]**
* **[insert other backup procedure action].**

## 6.4 Setting up user access to the ICT systems

When a new staff member (or other approved user) commences with **[Insert organisation name]**, their supervisor will inform the **[insert IT allocated position]** and ask them to create a new log-in on the organisation’s network.

The **[insert IT allocated position]** will undertake the following tasks:

* Ensure the new user has access to a networked desktop computer and a desktop phone
* Create a new network user account with the appropriate access levels (see Section 6.7 following)
* Ensure the new user has printer access
* Create a new email account
* Allocate a log-in for other internal systems
* Assist the new user to set up their email access through **[insert email system name e.g. Outlook Express]** and to change passwords
* Explain to the new user the network and filing map, how to use the phone, smart phone (if applicable) and set up voicemail facilities
* Provide a copy of this policy and explain where to find information or seek assistance about particular issues
* Support new users to use other internal ICT equipment and systems.

## 6.5 Deleting a user or removing their access to ICT systems

When a staff member/or other user is no longer employed/contracted by **[insert organisation name],** or when directed by the CEO/Manager to disable a current user’s account, the **[insert IT allocated position]** is to undertake the following tasks:

* Disable the user’s access/delete their log-in details in relation to the computer network and other internal systems
* Consult with the CEO/Manager as to whether emails to the former user should be forwarded to another staff member or whether the account should be deleted
* Remove the user’s name from the internal address book.

## 6.6 Levels of access

**[Insert organisation name]**’s server(s) consists of **[insert number]** of drive(s) with certain access restrictions. This is set out in Section 3.4 of this policy. The **[insert IT allocated position]** is to ensure that individual staff members or other users are provided with the appropriate levels of access.

## 6.7 Encryptions

Staff members are not generally permitted to encrypt hard drives or folders, because if an encryption password is lost, the data is impossible to recover. If **[insert organisation name]** staff are required to encrypt data in order to transmit to external clients, the original data or files should first be stored, unencrypted, on the internal network.

In the event that staff are required to encrypt data for internal use only, for example: **[insert organisation name]’s** internal policies and procedures in Word format (that form part of the quality management system) may be password protected to eliminate unauthorised changes to the documents, the passwords will be recorded by the CEO/Manager in the **[insert organisation name]** Encryption Password Register template.

If staff members are concerned about the security of specific data, they should consult the **[insert IT allocated position]** as to the best way to improve its security.

## 6.8 Unauthorised access to or interference of data

Unauthorised access or deliberately modifying or damaging **[insert organisation name]** data is a violation of Australian legislation and the organisational Code of Conduct, and may result in criminal charges or civil legal proceedings.

## 6.9 Accessing the network from home

**[Insert organisation name]** staff may access the network from home by connecting to the **[insert type of server to access, for example VPN]** server once authorised to do so. Log-in details are provided by the **[IT allocated position]**.

Staff working offsite should be aware that they have a responsibility to comply with **[insert organisation name]** policies. This means they cannot jeopardise the information security, privacy and confidentiality of the network. Wherever possible, they do not access the network on computer equipment systems that are readily accessible by, or shared with, the general public. Where staff access the network from home, they must ensure passwords for access are secure from other regular or occasional users of that computer, including friends and family.

## 6.10 Maintenance of ICT equipment

Staff are required to take reasonable precautions to protect IT equipment from damage, loss or theft.

If staff members want to change or modify equipment that is provided to them by the organisation for work purposes, they must seek approval from their manager and the **[insert IT allocated position]**.

# SECTION 7: PASSWORDS

**[Insert organisation name]** is committed to providing IT equipment, services and platforms that are secure and provide appropriate expectations regarding the safe use of passwords when working on organisational ICT equipment and tools.

The purpose of this section is to provide guidance to **[insert organisation name]** staff members on the creation and use of safe passwords in order to increase the organisational IT network security and reduce the risk of external intrusion.

The following processes ensure that staff members, Board members, students and volunteers are aware of their responsibilities and the steps to create strong and secure passwords.

This section ensures that:

* Internal network and related document security and privacy is not compromised
* Staff members’ privacy is protected
* Staff members are aware of their password responsibilities.

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorised access and/or exploitation of **[insert organisation name]**’s resources. All system users are responsible for taking the steps outlined below to select and secure their passwords.

## 7.1 [Insert IT allocated position] responsibilities

The **[insert IT allocated position]** is responsible for changing all system-level passwords, on at least a quarterly basis. This could include Windows Administrator, application administration accounts, etc.

The **[insert IT allocated position]** allocates initial passwords to each new user for access to the network, email, and/or other relevant systems. The **[insert IT allocated position]** must then advise new users to change their passwords, and refer them to this policy for advice on choosing passwords.

The **[insert IT allocated position]** cannot reset or access users’ accounts, or change their passwords, unless expressly authorised by the user or by the CEO/Manager. The CEO/Manager may authorise access where there has been a breach in the Code of Conduct and the CEO/Manager requires information to appropriately manage the incident.

## 7.2 User responsibilities

Once computer users have been set up with access to the email and network/computer systems, individual users are prompted to change their passwords at least every **[insert timeframe, for example six months]**.

Users are responsible for the security and complexity of their own password; staff should refer to the Creating Strong and Safe Password Information Sheet or online, go to the Australian Communications Consumer Action Network website.

# SECTION 8: COPYRIGHT AND SOFTWARE LICENcES

**[Insert organisation name]** is committed to comply with copyright legislation, licences and user responsibilities in regard to equipment, software and services purchased by or provided to the organisation in order to fulfil its goals and strategies.

The purpose of this section is to provide guidance to **[insert organisation name]** staff members on their responsibilities in using copyright material and licences appropriately, as part of their role within the organisation.

This section ensures that:

* Employees comply with current legislation and acknowledge copyright work, material and services
* Employees are supported to provide consistent and quality online experiences
* Organisational research, programs, services and activities are consistent with the organisation’s values, legal requirements, related policies, and code of conduct.

This section does not provide guidance on research. For further information, refer to the Organisational Development Policy.

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 licences 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 licences for software use.

## 8.1 Software licences

When at work, or when **[insert organisation name]** computing or networking resources are being used, copying of software in a manner not consistent with the vendor’s licence is strictly forbidden. If users are not sure what is and what is not permitted under a particular licence, they should speak to the **[insert IT allocated position]** or the vendor.

When the organisation disposes of equipment which contains software (other than the operating system) that is licensed to **[insert organisation name]**, the **[insert IT allocated position]** is to remove that software. Refer to section 5, ICT Equipment Disposal for more information.

## 8.2 Use of materials from the internet

Reproduction of materials available over the internet must be done only with the written permission of the author or owner of the document.

Permission is sometimes granted on the website with a statement that declares you may download a document for personal or non-commercial use. In the absence of such a statement, users should email a request for permission to use it. The right to use the material may be limited by the terms of the permission granted, and/or by any conditions that the copyright owner imposes.

**🖌Note\***

In some websites, material is distributed by its creators under “Creative Commons” licences, which usually means internet users can use the item, so long as users follow simple conditions which are clearly explained in their websites.

\*Please delete note before finalising this policy

Unless permission from the copyright owner(s) is obtained, making copies of material or saving material to a hard drive is unlawful, unless it is for a specific list of purposes and it is a “fair dealing”.

**🖌Note\***

There is no general exception for using copyright material simply because you think it is fair or because you are not making a profit. The Copyright Act allows you to use copyright material without permission if your use is a “fair dealing” for one of the following purposes:

* research or study;
* criticism or review;
* parody or satire;
* reporting news; or
* professional advice by a lawyer, patent attorney or trademarks attorney.

In this context, a “dealing” with copyright material means using the material in any of the ways reserved to the copyright owner. Whether a person’s use of copyright material is “fair” depends on the circumstances of the case. In one case, the Federal Court stated that whether a dealing is fair or not “is to be judged by the criterion of a fair minded and honest person”.

For further information about “fair dealing” refer go online to the Australian Copyright Council’s website.

\*Please delete note before finalising this policy.

If **[insert organisation name]** staff are in doubt as to whether they can download and/or copy material from the internet, they should consult their direct supervisor or senior staff members.

Websites and online resources should be referenced as per 5.1.1 Copyright Notice in the Communications Policy. Also refer to section 5.1.2 Use of Copyright Material in the Communications Policy

## 8.3 Further information

If staff members are unsure about copyright issues, information is available from the Australian Copyright Council website.

# SECTION 9: STAFF USE OF COMMUNICATION TOOLS

**[Insert organisation name]** understands that communications tools such as phone, email, internet and social media applications have become essential component parts in the way communications and business are carried out to relate with communities, clients, staff members and other organisations.

The purpose of this section is to provide guidance to **[insert organisation name]** staff members on using these tools as practical instruments to engage with the sector and its stakeholders, improve services participation, enhance transparency and fully realise the organisation’s goals and strategic outcomes.

The following processes ensure that use of communication tools are of a consistent high quality, are collaborative, appropriate, transparent and that users are accountable whether using the tools as part of their work or in their personal life. These communication tools also:

* Are recognised as an integral part of the organisation’s communication
* Enable collaboration and engagement with the sector and stakeholders
* Support responsible and accountable practices.

This section ensures that staff members:

* Use communication systems and equipment provided by the organisation for work purposes only, unless authorised otherwise
* Are supported to provide consistent, quality online experiences.
* Use communication tools in a manner that is consistent with the organisation’s values, legal requirements, related policies, and codes of conduct.

This section does not provide guidance on:

* Social media policy implementation or training
* Official **[insert organisation name]** social media platforms use – refer to Communications Policy
* Client’s use of social media platforms – refer to the Service and Program Operations Policy.

## 9.1 Email use

Employees, volunteers and students may use email access provided by the organisation for any work-related purposes of **[insert organisation name].**

**[Insert organisation name]** allows staff members to send and receive personal emails, provided that if emails are sent with **[insert organisation name]**’s address, a disclaimer is attached stating that the views of the sender may not represent those of the organisation. The organisation’s staff members use the following statement when sending private emails:

[Disclaimer – This email (and any file transmitted with it) is intended for the addressee only and may contain confidential information. If you have received this email in error, please delete it and notify the originator of the message. Any views expressed in this message are those of the individual sender except where the sender (with authority) states them to be the views of **[insert organisation name]**].

Emails related to the core business of **[insert organisation name]** will be stored in **[insert location]** with back-up copies stored on the **[insert server name]** server.

Employees can generally expect that the subject and recipients of emails may be monitored intermittently.

**[Insert organisation name]** reserves the right to read and take action on employee emails if there is reasonable evidence that an employee is breaching this policy.

Email can be subject to production in litigation or other investigations.

### 9.1.1 Passwords

Email users will not compromise the privacy of their password by sharing it with others or exposing it to public view. Staff members and other authorised users are required to keep their email passwords secure and follow internal password procedures as per Section 7 of this policy.

### 9.1.2 Email signature

The Corporate Image section of the Communications Policy sets out the recommended font and text for staff members’ email address block, signature and other inclusions.

### 9.1.3 Prohibited use of email

The use of **[insert organisation name]** email in the following contexts is strictly prohibited:

* Reading or sending messages from another user's account, without **[insert organisation name]** authorisation
* Altering or copying a message or attachment belonging to another user without the permission of the creator of the message/attachment
* Subscribing to list servers and distribution lists unless they are directly related to your work or permitted by your supervisor
* Exchanging information in violation of copyright laws
* Exchanging proprietary information, trade secrets, or any other confidential or sensitive information about the company (unless in the authorised course of their duties)
* Creating or exchanging messages that are offensive, harassing, obscene or threatening
* Promoting websites containing objectionable or criminal material
* Conducting a business or conducting illegal activities
* Creating or exchanging advertisements, solicitations, chain letters and other unsolicited or bulk email.

## 9.2 Social media use

**[Insert organisation name]** recognises the use of social media for open dialogue and the exchange of ideas where it is beneficial for individuals in either 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 the organisation’s reputation.

### 9.2.1 Social media background

For the purpose of this policy, the term social media is defined by a number of online tools or websites that engage, create and share user-generated content, data and comments that might impact on the organisation or the people who use the organisation’s services.

Social media encompasses all tools and programs that allow and promote any user to publish, discuss and share media content. This could include:

* Micro-blogging sites (examples: Twitter, Yammer)
* Social and professional networking sites (examples: Facebook, LinkedIn)
* Video and photo-sharing websites (examples: YouTube, Pinterest)
* Weblogs, or ‘blogs’ – online diaries for pictures and updates (examples: Tumblr, Blogger)
* Wikis – libraries of collaborative documents that anyone can edit (example: Wikipedia)
* Forums and discussion boards (examples: Google Groups, Whirlpool).

### 9.2.2 Official use

Official use is when a staff member, Board member, student or volunteer is using official and related social media platforms identified as a representative of **[insert organisation name]** with permission from the **[insert allocated position name]** or alternatively the CEO/Manager.

Information provided in these messages/posts must:

* Comply with the organisation’s code of conduct
* Follow organisational social media content restrictions.

For official use of **[insert organisation name]** social media platforms, refer to the Communications Policy.

### 9.2.3 Personal use

Personal use is when a staff member, Board member, student or volunteer is using social media platforms identified as themselves and not officially as a representative of **[insert organisation name]** although identifying themselves as affiliated with the organisation in their activity content. This could include photos, profile, current job, etc.

**🖌Note\***

Organisations are encouraged to amend/delete the following paragraph according to the organisation’s internal policies and procedures in regard to the use of social media by staff members.

\*Please delete note before finalising this policy

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

* Does not interfere with the staff member’s work
* Is not in conflict with the business needs of the organisation
* Is not prohibited use under this policy, and
* Does not breach other organisational policies, including the Code of Conduct.

Non-work-related email shall be saved in a separate folder from work-related email.

Documents downloaded for personal use should be saved in the staff member’s personal folder (if applicable).

Storing **[insert organisation name]** information on a personal ICT item must only be carried out when absolutely necessary and when no other option is available. All internal information stored on a personal ICT item will remain the property of the organisation and must adhere to relevant policies and procedures.

### 9.2.4 Inappropriate use

Inappropriate and prohibited use of social media platforms includes, (but is not limited to):

* The creation, distribution or deliberate downloading of any disruptive or offensive messages
* Using discriminatory, defamatory, abusive or otherwise objectionable language against people or organisations
* Stalking, bullying, trolling or marginalising any individual or group
* Uploading information of a confidential nature in regard to the organisation’s business.

It is the direct responsibility of staff members, Board members, students or volunteers to comply with the above guidelines and to advise the **[insert allocated position name],** or alternatively, the CEO/Manager of any unauthorised activity.

Inappropriate and/or incorrect use of social media platforms is considered serious misconduct, as it affects the perception of the organisation’s values, credibility and professionalism with its clients, stakeholders and the broader community.

Engaging in any type of misconduct will be managed as per the Human Resources Policy and consequences may include disciplinary actions or dismissal.

Following any inappropriate or prohibited use of social media platforms the **[insert allocated position name],** or alternatively, the CEO/Manager, will consider:

* Risk assessment and corrective measures
* Corrective measures action plan and responsibilities
* Media release(s)
* **[insert other].**

### 9.2.5 Authorised access

**[Insert allocated position name],** or alternatively, the CEO/Manager, are the only authorised staff members to manage social media platforms and passwords, unless they have authorised and delegated other staff members to access social media tools.

The organisation reserves the right to grant, limit or withdraw at its discretion, access to some or all of its social media platforms, either temporarily or permanently.

### 9.2.6 Systems and security

All **[Insert organisation name]** computer systems and facilities, including social media tools used by the organisation follow due process in terms of user responsibilities, copyright, access, hacking, monitoring and security breaches.

The nature of social media platforms depends on self-regulated communication channels where all individuals are able to provide feedback, complaints and either positive or negative comments.

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

## 9.3 Internet use

Employees, volunteers and students may use internet access provided by the organisation for any work-related purposes.

**[Insert organisation name]** allows staff members to access the web for personal purposes, provided that personal use is moderate in time, does not incur significant cost to the company and does not interfere with the duties of the employee, volunteer, student or colleagues.

**[Insert organisation name]** monitors logs of internet usage which may reveal information, such as which servers (including websites) have been accessed by the employee, and email addresses used.

The internet is used in a manner consistent with the Code of Conduct and as part of the normal execution of an employee’s or volunteer’s job responsibilities or student’s learning needs.

Internet users will not compromise the privacy of their password by sharing it with others or exposing it to public view. Passwords will be changed on a regular basis.

### 9.3.1 Prohibited use of internet

Staff members are strictly prohibited from using **[insert organisation name]’s** internet facilities to undertake the following activities:

* Visiting web sites containing objectionable or criminal material
* Gambling, gaming, conducting a business or conducting illegal activities
* Installation of software without **[insert organisation name]** authorisation
* Creating or exchanging messages that are offensive, harassing, obscene or threatening
* Creating, storing or exchanging information in violation of copyright laws (including the uploading or downloading of commercial software, games, music or movies)
* Exchanging proprietary information, trade secrets, or any other confidential or sensitive information about the company (unless in the authorised course of their duties).

## 9.4 Phone use

Employees, volunteers and students may use phones provided by the organisation for any work-related purposes.

**🖌Note\***

Organisations are encouraged to amend/delete the following paragraph according to the organisations views and policy direction.

\*Please delete note before finalising this policy

**[Insert organisation name]** allows staff members to use the phone for personal purposes, provided that personal use is moderate in time, does not incur significant cost to the company and does not interfere with the duties of the employee, volunteer, student or colleagues.

Employees, students and volunteers will endeavour to make all telephone calls as brief as possible.

### 9.4.1 Incoming calls and voicemail

Employees, students and volunteers will answer the phone courteously with an agreed greeting message and respond appropriately to callers’ requests.

**🖌Note\***

Organisations are strongly encouraged to consider the preparation of a standard greeting message (for voicemail or actual instances of physically receiving an incoming call), particularly for new staff, students and volunteers; training to be delivered during orientation. Further information on voicemail greetings can be sourced here.

\*Please delete note before finalising this policy

When preparing a voicemail message for **[Insert organisation name]** office phones and smart phones, the following tips should be used as a guide:

* Do not begin with “Your call is important to us…” This phrase is overused and can be a “turn off” to callers.
* Let the customer know whose voicemail they have reached.
* Apologise that you cannot take their call right now.
* Invite your caller to leave a detailed message.
* Let your caller now when they can expect a return call.
* List any additional options that are available to your caller. Does the **[Insert organisation name]** website provide meaningful information? What is the web address? Are there additional numbers for them to call in case of an emergency?
* Keep the voice message short. An optimal recording is about 25 seconds.

### 9.4.2 Outgoing Calls

**[Insert organisation name]** employees, students and volunteers are able to make local telephone calls. The CEO/Manager may authorise international telephone calls if required by the role.

* + 1. **Mobile Telephones**

Employees, volunteers and students are responsible and accountable for the use, safekeeping and security of **[insert organisation name]** mobile phones issued on a loan basis to employees, volunteers and students, and which remain the property of the organisation.

Employees must abide by all Commonwealth and State laws when using a mobile phone.

# SECTION 10: WEBSITE

**🖌Note\***

The following section provides general guidance to organisations in regard to website management. Organisations are encouraged to amend/delete the section if it is not relevant to the organisation activities.

\*Please delete note before finalising this policy.

**[Insert organisation name]** has a website which provides information to the general public about the organisation, and its services. **[Insert organisation name]** is committed to promoting the organisation in an accessible, transparent and user-friendly manner.

The purpose of this section is to provide broad guidance to **[insert organisation name]** staff members on the organisation’s website management and the process for contributing content to the website.

This section ensures that:

* Online communication tools support the organisation’s goals and outcomes
* Staff members contribute appropriately to the organisation’s website
* The organisation’s website is reliable, secure and up-to-date.

## 10.1 Website hosting and security

The **[insert IT allocated position]** is responsible for renewing the **[insert organisation name]** website domain name through an online registration process, the details of which are contained in the ICT Equipment Database.

The website is hosted on **[insert fileserver name and location]**. The details about the security and back-up of this server are provided in Section 6 of this policy.

**🖌Note\***

The following paragraph provides general guidance for organisations with internal website modification systems, where staff members can manage the website content according to their roles and projects. Organisations are encouraged to amend/delete the following statement if it is not relevant to the organisation’s activities.

\*Please delete note before finalising this policy.

## 10.2 Access to the website content

The **[insert IT allocated position]** provides staff members with log-ins and initial passwords, allowing them to access the **[insert website content management system name].**

The **[insert IT allocated position]** is responsible for maintaining the security of the log-ins and passwords within the organisation, including ensuring that passwords are regularly changed, at least every **[insert timeframe, for example six months]**.

**🖌Note\***

If staff members are required to update content on the organisation’s website, it is recommended that they are provided more guidance and training to enable them to undertake that task efficiently.

\*Please delete note before finalising this policy.

## 10.3 Website design or redevelopment

Where the organisation identifies that major changes to the website are required which cannot be undertaken by the **[insert IT allocated position]**, the **[insert IT allocated position]** is required to prepare a comprehensive project brief in consultation with other staff members to be approved by the CEO/Manager.

The project brief will set out the budget, responsibilities for project management of the website development, including supervision of the contractors, etc. For further information about project brief or tools refer to the Program Management Policy.

# SECTION 11: INTERNAL CLIENT DATABASE

**🖌Note\***

The following section provides general guidance to organisations in regard to internal client database management. Organisations are encouraged to amend/delete the section if it is not relevant to the organisation’s activities.

\*Please delete note before finalising this policy

**[Insert organisation name]** has an internal client database containing details about all its clients. Basic information about clients is extracted by allocated staff members to inform treatment activities and co-ordinate appropriate support.

**[Insert organisation name]** is committed to maintaining up-to-date client information safely and securely by complying with current legislation and developing appropriate systems to support quality client outcomes.

The purpose of this section is to provide guidance to **[insert organisation name]** staff members on using the internal client database processes as a practical instrument to manage client information, treatment and outcomes. These processes also:

* Are recognised as an integral part of the organisation’s client support
* Enable holistic service provision, collaboration and engagement with the sector to achieve client outcomes
* Support accountable practices and reliable data.

This section ensures that staff members:

* Use responsible and accountable processes to support clients
* Maintain accurate client records
* Use client information in a manner that is consistent with the organisation’s values, legal requirements, related policies, and code of conduct.

The **[insert IT allocated position]** is responsible for maintaining the database and ensures staff members are supported to use the system appropriately.

For information on **[Insert Organisation Name]**’s policy regarding the importance and value of collecting client-related data, including client outcomes data, refer to the Organisational Development Policy.

## 11.1 Access and maintenance

The **[insert IT allocated position]** provides staff members with a log-in and initial password which allows them to use and update the database. Access levels are managed by **[insert IT allocated position]** according to staff roles and positions.

## 11.2 Updating records

All staff members with client responsibilities are required to update information about clients, for example:

* creating new records
* updating contact details
* inserting client program information
* adding client assessment outcomes
* adding changes to the client’s file notes.

## 11.3 Reporting and verification of data

The **[insert IT allocated position]** will:

* Support staff members to generate reports as required
* Be able to generate reports for staff members with the main purpose of complying with funding reporting requirements and/or internal reporting activities
* Not create, delete or edit records without the written authority of the staff member who created or edited a record
* Monitor the quality of the data collected, and work with staff members to improve data input.

**🖌Note\***

For organisations using the NADAbase COMS or N/MDS reporting system, NADA can provide assistance in developing reports. If your organisation uses an alternate client database system, assistance may be available through the host company.

\*Please delete note before finalising this policy.

## 11.4 Database security

In recognition of the sensitivity and confidentiality of the information contained in the Internal Client Database, **[insert organisation name]** has in place a high level of database security and several back-up measures.

The Internal Client Database is stored on the server **[insert server name]** which is located in **[insert server location]**. The **[insert IT allocated position]** conducts **[insert number, for example 2]** back-ups every **[insert days, for example every day]** onto a removable onsite hard drive called **[insert hard drive name]** located in **[insert hard drive location].**

The **[insert IT allocated position]** regularly monitors the security of the database; for example, checking access logs and investigating unusually large transfers of data. The **[insert IT allocated position]** will advise the CEO/Manager, should they identify any suspicious activity that they deem requires further investigation.

## 11.5 Database improvement or redevelopment

The **[insert IT allocated position]** will ensure the data sets used by the Internal Client Database are updated in line with the funding and reporting requirements.

The **[insert IT allocated position]** will keep track of any new requirements, suggestions or recommendations from staff members.

Where **[insert organisation name]** identifies that major changes are required to the database which cannot be undertaken by the **[insert IT allocated position]**, the **[insert IT allocated position]** is required to prepare a comprehensive project brief in consultation with other staff members, to be approved by the CEO/Manager. The development brief will set out the budget, and responsibilities for project management of the website development, including supervision of the contractors, etc. For further information about project brief or tools, refer to the Program Management Policy.

# SECTION 12: ICT STAFF SUPPORT

**[Insert organisation name]** understands that the use of communications tools requires extra staff training and support to be beneficial for the organisation’s goals and strategic outcomes.

The purpose of this section is to provide guidance to **[insert organisation name]** in developing and implementing ICT activities to provide training and support to employees in complying with this policy and other ICT requirements.

This section ensures that:

* **[insert organisation name]** develops appropriate ICT training activities to support staff members
* Staff members are supported to use consistent and secure processes
* ICT activities are aligned with the organisation’s values, legal requirements, related policies, and code of conduct.

## 12.1 ICT support

The **[insert IT allocated position]** and the **[insert allocated administration position]** are responsible for providing staff members with support to access and use relevant ICT systems, hardware and software. This could include:

|  |  |
| --- | --- |
| **[insert IT allocated position]** | **[insert allocated administration position]** |
| Training the **[insert allocated administration position]** to act as the first point of contact for staff with ICT problems | Initial troubleshooting of phone, computer, printer, internet and email problems |
| Troubleshooting phone, computer, printer, internet and email problems where the **[insert allocated administration position]** is unable to assist, or is unavailable | Advice on “how do I…” in relation to Microsoft Word, Excel, website, creating PDFs, finding documents on the server, and using **[Insert organisation name]** style guides |
| Recovering files from back-up | Referral of complex IT issues to the **[insert IT allocated position]** |
| Dealing with ICT suppliers, including phone companies in relation to problems and when obtaining quotes for services |  |

## 12.2 ICT training

**[Insert organisation name]** staff members are entitled to receive ICT training when their position descriptions require them to use particular ICT tools. This means that they are entitled to receive onsite or third-party training that enables them to perform the tasks required for their position.

Staff members or their supervisors may identify a need to undertake training in relation to a particular software or ICT tool. Options for training should be canvassed first with the **[insert IT allocated position]**, who may be able to provide one-to-one training, and then, if this is not possible, with appropriate ICT training providers.

Options to consider include:

* Online training
* Onsite, face-to-face training provided by an ICT provider or contracted trainer
* Offsite training provided by an ICT provider
* ICT-related training is to be discussed as part of regular work-plan meetings and performance review and development meetings.

For further information on staff training, refer to the Human Resources Policy.

# SECTION 13: INTERNAL REFERENCES

## 13.1 Supporting documents

* ICT Consultation Survey template
* ICT Needs and Prioritisation Tool template
* ICT Plan template
* Electronic Records Map template
* List of Information Custodians
* Record Retention and Disposal Schedule
* Email Retention Guide
* ICT Equipment Database
* ICT Encryption Password Register template
* Creating Strong and Secure Passwords Information Sheet

**Part of the Financial Management Policy**

* Supplier Claim Form

**Part of the Human Resources Policy**

* Code of Conduct

## 13.2 Related policies

* Client Clinical Management Policy
* Organisational Development Policy
* Communications Policy
* Human Resources Policy
* Service and Program Operations Policy
* Risk Management Policy
* Financial Management Policy
* Program Management Policy

# SECTION 14: EXTERNAL REFERENCES

## 14.1 Legislation

* Privacy Act 1988
* Privacy Amendment (Notifiable Data Breaches) Act 2017
* Federal Circuit Court of Australia (Consequential Amendments) Act 2013
* Privacy Amendment (Enhancing Privacy Protection) Act 2012
* Copyright Act 1968 (Cth)
* Fair Work Act 2009 (Cth)
* A New Tax System (Goods and Services Tax) Act 1999 (Cth)
* Electronic Transactions Act 2000 (NSW)

## 14.2 Resources

* Privacy Law Reform, Resources
* Australian Communications Consumer Action Network

“Tips for creating strong, safe passwords”

* Australian Copyright Council – Resources

## 14.3 Websites

* Social Change Media
* Australian Government, Office of the Australian Information Commissioner
* Australian Privacy Law Reform Information
* Planet Ark – Recycling near you

## 14.4 Others

* Lifeline, Social Media Policy, Lifeline November 2012
* Lifeline, Social Media and Website Policy, Lifeline 2017
* iTaNGO Project, Social Media Workshop, Infoxchange Australia 25/11/2011
* ImproveIT, Infoxchange Australia 2014

1. This Guide has been adapted from information provided by the [Institute of Community Directors Australia](https://www.communitydirectors.com.au/icda/policybank/?articleId=5466) ‘Email Retention and Archiving Policy;’ [↑](#footnote-ref-1)