Information Storage and Handling Policy

Document No:	Issue No:	Date of Issue:	Review Date:	Process Owner:	Authorised By:
POL-010	001	05/10/2022	05/10/2024	Director	Director

Background

ReadyUp Skills offers individual and group programs to develop the participants understanding in independent living, job readiness, work experience, community access, road safety, creativity and social skills building. ReadyUp Skills services the Newcastle, Lake Macquarie and Hunter Valley region.

ReadyUp Skills works within the NDIS standards and governing legislation as well as following up to date industry best practice guidelines.

Policy Statement

ReadyUp Skills collects and stores information so it can provide a safe working environment, high quality services and meet its legal requirements. Information security is important as we handle, transmit and store personal information on a daily basis. Under privacy laws, ReadyUp Skills is required to take reasonable steps to keep all personal information accessed safe from accidental or deliberate misuse. This policy and procedure aims to safeguard our information and our ICT (information and communications technology) resources from those with malicious intent.

ReadyUp Skills manages personal information in accordance with relevant legislation and disposal guidelines.

This policy supports ReadyUp Skills to apply National Standards Disability Services:

Standard 1: Rights and into the future,

National Disability Insurance Scheme Practice Standards:

1. Rights and Responsibilities (Privacy and Dignity); and
3. Provision of Supports (Access to Supports).

Scope

This policy describes ReadyUp Skills responsibilities for meeting legislative and NDIS guidelines around information storage and handling. The policy applies to all information and communications technology (ICT) used by ReadyUp Skills including computers, computer networks, internet connections, smart phones and email. Applies when unsolicited phone calls, emails or text messages are received.

This policy applies to all staff, contractors, volunteers or students/trainees. It includes security of information of information about the people ReadyUp Skills support and the people who work with ReadyUp Skills. The Managing Director is responsible for this policy.

Principles

- Personal information is collected with consent and is used where the information is needed to provide services and meet compliance requirements.

- Information is protected from misuse, loss and unauthorised access.
- Information not needed by ReadyUp Skills is destroyed as soon as practicable in a way that complies with all legal and compliance requirements
- Reasonable steps are taken to ensure information is complete, current and accurate.
- Personal information is only ever released if required by law, agreed to through the informed consent of the individual or if a person requests to see their own personal file.
- Personal information will not be disclosed to other parties or used for direct marketing without permission

Key actions/Procedures

People will be provided with this policy when they first use ReadyUp Skills services. The Managing Director will provide the policy at the first meeting with the person and ensure they have understood it. This action is recorded on the service agreement and held on their file.

Personal Information

All personal information, including that of participants and employee, must be:

- Stored securely with reasonable security precautions against misuse or unauthorised access (e.g. electronic information should be password protected, hard copies stored under lock and key).
- Readily accessible but only on a need-to-know basis.
- Retained for the required time (7 years).
- Destroyed securely when no longer required.
- Not shared with any third parties without correct consent.

General information security precautions

- Access to all personal information is strictly based on a need-to-know basis.
- When sending group emails, use the 'BCC' field rather than the 'To' field so email recipients cannot see other recipient's email addresses.
- When using personal devices, no files should be downloaded to and stored. Files should only be accessed through Cloud Software.
- Always password lock computers when unattended (shortcut to password lock a Windows computer is "Windows Key + L").
- Operating system updates (also called "patches") must be installed promptly after they become available.
- Active antivirus software must be installed and kept up-to-date on all computers.
- Internet modern routers must have security (i.e., firewall enabled).
- Internet modern routers and network security cameras must have a strong admin password.
- WiFi networks must have strong passwords to gain access.
- Only download or install software from trusted sources.
- Mail servers should be configured to use encryption.
- Computers should be configured so admin rights are restricted to key management personnel (i.e., so employee can't install software).

- When an employee leaves, their access to the organisation's computer network and email systems is removed promptly.

Passwords

- All computers which store or access personal information require unique and strong passwords to gain access.
- Passwords must not be shared or reused between computers, used, or different applications (e.g., password for Facebook should be different to the password for Google mail which should be different to the computer login password).
- Passwords should not be left written on paper left lying around, or stored in computer/browser history.
- Passwords should be regularly changed (i.e., every three months).
- Always use strong passwords with a minimum of 8 characters which include a combination of:

    - Lower case letters (abcdefghijklmnopqrstuvwxyz)
    - Upper case letter (ABCDEFGHIJKLMNOPQRSTUVWXYZ)
    - Numbers (1234567890)
    - Symbols (!@#$%^&*()-= +,.<>/?'"[]{}\|`~:;'")

- Do not use easy-to-guess passwords such as "123456", "password" or "qwerty" etc.

Avoiding scams and ransomware

- Do not pay the ransom if your computer is infected with ransomware.
- Be aware of current scams targeting individuals and businesses by following government sites such as SCAMWATCH.
- Be suspicious of any unsolicited emails or text messages purporting to be from government agencies, banks, delivery, services or other similar organisations – check the sender's email address for clues (scammer will try to fool you with a very similar email sender's address) and delete any suspicious emails or look up the organisation's main phone number and call if unsure.
- Be suspicious of unsolicited phone callers purporting to be from Telstra, Microsoft, the Australian Tax Office and do not provide any information, instead end the call – if unsure, look up their main number and call to confirm.
- Do not allow remote access to any computer or network recourse by a third party unless it is arranged with a known and trusted IT services provider.

Portable Devices

- No client information should be stored on a portable device.
- Staff may access emails and client data on portable devices during work hours, but ensure they log out when not in use.
- Smart phones and mobile computer must not be left unattended in public.
- Smart phones and mobile computers must not be left in vehicles (locked or unlocked).
- Smart phones and mobile computers must not be stored in checked-in baggage when flying.
- Portable storage devices (e.g. USB drive, USB flash drives) should be vetted and checked for viruses prior to their use.

- Portable storage devices require password protection if they are used to store any personal information (such as employees or participant information).

Social Media

- Only those authorised to do so should represent the organisation on social media.
- Personal information and confidential company information must not be posted or shared on social media.
- When an employee leaves, their access to the organisation's social media must be promptly removed.

Printed material

- Personal information in printed format must be stored securely when not being used.
- Personal information in printed format must not be left lying around.
- When no longer required, printed material that contains personal information must be shredded or removed by a secure document destructions service.

Incidents

- A data breach or privacy and confidentiality is an incident, follow the Manage Incident Internally Process to manage and resolve the incident.
- Incidents where individuals are at serious risk of harm as a result of the breach must be advised of the breach and assisted with ways to reduce their risk of harm from the breach.
- Incidents where individuals are at serious risk of harm as a result of the breach are reportable to the Office of the Australian Information Commissioner.

Definitions

Adware Software that automatically displays or downloads advertising material such as banners or pop-ups.

Backdoor A technique to bypass a computer system's security undetected in order to access a computer or its data.

Bot (Malicious Bot) Self-propagating malware that infects its host and connects back to a central computer. Malicious bots can be used to spy on user activity, steal passwords, relay spam, open backdoors, or perform attacks on other computers, websites or resources.

Data Breach An incident where personal and/or sensitive information has been accidentally or deliberately accessed and/or disclosed in an unauthorised fashion. Some common examples off data breaches include:

- Personal information accidentally mailed or emailed to the wrong recipients.
- A locked filing cabinet containing personal file is broken into or left unlocked and accessed by unauthorised persons.
- A computer or storage device used to store personal information is compromised as a result of a security breach, malware or poor security practices.

- Personal information in printed form or on an insecure storage devise is left in a public place.
- Personal information accidentally or deliberately shared on social media.

Malware Software which is specifically designed to disrupt, damage, or gain authorised access to a computer system. Includes viruses, ransomware, spyware, adware and other.

Patch See "Update".

Phishing Fraudulent emails purporting to be from reputable companies sent to fool users into revealing personal information such as passwords, bank account details or credit card numbers.

Ransomware A type of malicious software designed to block access to a computer system until a sum of money is paid.

Spam Also known as junk email, spam is unsolicited email usually to containing advertising, malware, or phishing.

Update (or Patch) An update to a computer, tablet or smart phone operating system usually to correct security flaws (vulnerabilities) or correct errors.

Virus A type of malicious software that installs without the user knowing. A virus can replicate itself, modify computer programs, corrupt data, open backdoors, or install adware, bots or ransomware.

Vulnerability A flaw in a system that can leave it open to attack.

Related Policy and Procedures

Service Agreement
Code of Conduct
Incident Report Form
Confidentiality Procedure

Related Legislation and Policy

- Carers' Recognition Act 2004
- Disability Services Act 1993 (NSW)
- Equal Employment Opportunity Act 1987
- New South Wales Anti-Discrimination Act 1977
- New South Wales Mental Health Act 2007
- Crimes Act 1900 (NSW)
- United Nations Convention on The Rights of Persons with Disabilities
- National Standards for Disability Services
- National Disability Insurance Scheme Quality and Safeguarding Framework

Approvals

Date of approval: 05/10/2022
Date of review: 05/10/2024
Signature of Managing Director: