

## PURPOSE

The purpose of this policy is to:

- Promote a privacy-aware and compliant culture within the organisation
- Comply with legislative and compliance frameworks in the handling of personal information.
- Support All About Care Australia (AACA)'s capability to prevent, prepare, respond, manage and recover from any event that affects the confidentiality, integrity and availability of data. It applies to the full lifecycle of data.

AACA preserves all stakeholders' right to privacy protection under the Australian Privacy Act (1988), the QLD Information Privacy Act (2009), the Health Records Act (2001) and the Notifiable Data Breaches Act 2017 in regulating how we collect, use, store, disclose and dispose of personal information.

## SCOPE

This policy applies to all AACA employees, participants, participant representatives, volunteers, and contractors.

### Preamble:

Personal and sensitive information about participants is only collected as is necessary, for a function or activity, or to enable AACA to carry out its work and deliver services to the participant or participant's representative (e.g. NDIS Plans)

In the case of employee or volunteer information, AACA uses the information for operational functioning or business activity. This includes but is not limited to banking details for wages, tax file numbers for taxation, and personal contact details for emergencies.

Non-client-specific information may also be collected, including but not limited to commercial and legal information – agreements and contracts or financial information.

Occasionally AACA seeks information from participants or their representatives of a personal or sensitive nature. This may include, but is not limited to disability, medical and health, racial, ethnic origin, spiritual beliefs or family composition and living arrangements. AACA seeks this information to tailor and support individualised and sensitive service provision.

Participants or participant representatives may decide that they would prefer not to provide AACA with such information. They may also choose to change this information at any time or to access their personal file. Individuals may also opt out of providing personal information. It is to be noted that this may result in the withdrawal of AACA services as this data is often required for the safety of participants and staff and/or for compliance requirements linked to AACA's NDIS registration status. Families/participants may also use a pseudonym or be de-identified.

AACA will collect, store, use, disclose and dispose of such information in a non-intrusive, lawful and fair manner. It may be stored in hard copy or electronically. AACA prioritises secure cybersecurity protocols. Confidential information may be either **personal** or **sensitive** information. In addition to collecting personal information, AACA collects sensitive information regarding a person's health status and disability diagnosis and racial or ethnic origin.

**Personal information** as defined by the Privacy Act 1988 (as amended) is information or an opinion about an identified individual or an individual who is reasonably identifiable, whether true or not, and whether recorded in a material form or not.

**Sensitive information** as defined by the Privacy Act 1988 (as amended) is information or opinion (that is also personal information) about an individual's health, disability, racial or ethnic origin, political opinions,

membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices or criminal record or health, genetic, biometric information or biometric templates.

## ***The Australian Privacy Principles (APPs).***

AACA's Privacy Policy is aligned to and inclusive of the Australian Privacy Principles in how information is collected, used, accessed, stored and changed as outlined in the Privacy Act 1988. A quick reference guide about the APPs is available on the Office of the Australian Information Commissioner website <https://www.oaic.gov.au>. This provides information about the expectations of the legislation. (See 1.2a Privacy Policy attachment)

## POLICY

*The framework of this Privacy Policy is aligned with the Queensland Information Privacy Act 2009.*

### 1.1.1 Security Risk Management

AACA will identify, manage and where possible minimise risks to its information. Any identified risks will be managed by the AACA management.

### 1.1.2 Access Management

User registration and de-registration procedures are used to control access to AACA information systems and services. All personnel will have their own unique physical identifier (User ID). Each staff member is accountable for any activity under these access methods. Passwords are unique and are kept confidential – they are not shared with unauthorised users. Passwords are changed at least annually as a risk mitigation strategy. Access to AACA information is dependent on the role/position of each staff member. AACA will have information, personnel, and physical security controls in place to prevent unauthorised access.

### 1.1.3 Security Incident Management

All personnel are responsible for reporting any information security events of which they become aware. The AACA management will coordinate incident responses to ensure incidents are managed consistently and effectively. This will comply with the Privacy Act, OAIC's Privacy Breach Reporting protocols, and the Notifiable Data Breach legislation. AACA will maintain records of any IT security incident/s and review them regularly. AACA management will be briefed about any major security incidents as measured by the Notifiable Data Breach checklist severity matrix.

### 1.1.4 Business Continuity

The Business Continuity Plan for the organisation will include the need to continue to secure information in the event of a disruption to normal business.

### 1.1.5 External party management

AACA will ensure that due diligence is applied to selecting all external parties with access to AACA information including appropriate security requirements and adequate reviews of the external party. AACA will provide

appropriate training or instructions to external parties on the organisation's security requirements and obligations. AACCA will ensure that external parties report their compliance status when acquitting service agreements/ contracts. AACCA will undertake regular due diligence for external critical financial assets, i.e. banks and financial institutions.

## CLOUD POLICY

The use of cloud storage (and similar) must be for work purposes and in line with Australian Privacy Principles, any legislation relating to Privacy and Health Records and to AACCA's Privacy policy and procedures as it relates to AACCA's financial data, or any other data owned or collected by AACCA. Personal cloud services accounts may **not** be used for storing, manipulating, or exchanging AACCA-related communications or AACCA-owned data.

### 1.1.6 Information Value

AACCA will identify, assess and value its information's confidentiality, integrity and availability throughout its lifecycle and document this in the information asset register. All personnel are responsible for complying with AACCA's confidentiality ratings and handling information that the assigned security controls demand. The information register will be reviewed every two years with the value of information being reflected in revised security ratings.

### 1.1.7 Information management

AACCA will record and maintain its information types in the information asset register. AACCA will manage its information in line with the AACCA Records Management Policy and secure its information (regardless of format) throughout its lifecycle (cradle to grave). Security controls to secure the information will be commensurate with the value of the information.

### 1.1.8 Information Sharing

AACCA will ensure appropriate agreements are in place for the sharing of its information such as a Code of Conduct for staff. These agreements will include the information handling requirements and security obligations of any external party. These agreements will be reviewed on a regular basis.

### 1.1.9 Personnel Security

All personnel will undergo pre-employment checks upon engagement and ongoing checks according to their position, their need to access information and any mandatory security requirements. Personnel will uphold their obligations under the Code of Conduct, stay informed of their security obligations and undertake regular security training. Personnel will return all AACCA information and assets upon termination of employment and will continue to be bound by the principles of the Privacy Act in relation to information gained whilst in the employment of AACCA.

### 1.1.10 Information Communication Technology (ICT) Security

Technical security controls commensurate with the information's value will be applied to AACCA's ICT environment to minimise the associated risks for protecting information in electronic format. This includes electronic access, transmission, storage, removal and disposal. The Australian Signals Directorate (ASD) has developed prioritised mitigation strategies, in the form of ASD's [Strategies to Mitigate Cyber Security Incidents](#),

to help organisations mitigate cyber security incidents caused by various cyber threats. The most effective of these mitigation strategies for targeted cyber intrusions and ransomware is known as the [Essential Eight](#). AACA's IT provider will be contracted to strive to implement the Essential 8 guidelines on AACA staff workstations at all sites and on AACA's terminal server, over time, based on AACA's priorities and capacity. These guidelines include:

- a) mitigation strategies to prevent malware delivery and execution
- b) mitigation strategies to limit the extent of cyber security incidents
- c) mitigation strategies to recover data and system availability

## 1.1.11 Physical Security

Physical security controls commensurate with the information's value will be applied to minimise the associated risks for protecting AACA information whether in the office or remotely. This includes wiping processes to remove or destroy confidential data on electronic storage media such as USBs or hard drives. Software backups are conducted daily.

Hard copy files are to be stored as a backup, with scanning and electronic storage prioritised. Some historic hard copies of documents are stored in secure storage. A filed document and retention schedule are applied. All sensitive information is stored in locked filing cabinets in secure offices, and equipment is stored in secure, locked offices.

## PROCEDURES

### 1.1.1 Security Risk Management

AACA will develop and maintain an Information Asset register which is inclusive of a security risk profile that is reviewed quarterly. AACA's IT provider's quarterly reviews will be analysed with a targeted focus on the management of the IT security of AACA.

### 1.1.2 Access Management

#### *Passwords*

Staff are registered with AACA's Provider Application called ShiftCare. User identification and passwords to access computer services are for the sole use of the person to whom they are allocated. Passwords are to be regularly changed as per AACA's security policy and required format.

If staff are allowed access to Senior Management information, files or diaries, they are to confine their activities only to the task for which permission was granted. Inappropriate searching on computers, files or diaries can result in a Performance Management process being implemented. AACA applies for access via delegated passwords on its ICT systems.

Access to specific drives on the server includes management, HR and Finances. This will be restricted to selected personnel and require authorised credentials by the General Services Manager.

When accessing client information via company computer, this is to be done during business hours unless the management has granted prior alternative authorisation.

## *Remote access*

Remote access outside working hours is permitted ONLY for those staff who are authorised by the director. All remote access is monitored and recorded. On cessation of employment, access will be removed for that employee. Exiting staff emails will be redirected to a delegated staff member nominated by the director.

### **1.1.3 Security Incident Management**

#### *Incident Reporting*

In line with the Data Breach Notification Scheme, it is vital to report to senior managers all potential incidents as soon as possible so that their impact may be minimised.

Staff should be aware of the following:

- how to identify potential breaches of security incidents
- the reason for reporting incidents which are so the impact can be minimised
- the need to report all incidents to their manager as soon as they become aware of them.

Depending on the level of the Breach, an OAIC Privacy Breach Incident report may be required. The Police may also need to be notified if someone's safety is at risk.

Any request to staff from government bodies or external organisations for information regarding participants must be checked and approved by the director before it is released in line with legislation.

#### *1.1.4 Business Continuity*

AACA will ensure the inclusion of confidential electronic account information in the Business Continuity Plan such as access to the Information Asset Register. AACA will maintain its business contract with a highly reputable Information Technology business such as Google to ensure the reliability of the backup of files and drives and restoration of AACA's IT system in the event of a catastrophic event or prolonged interruption to business.

### **1.1.5 External party management**

#### *Volunteers & contractors*

All AACA employees, volunteers and contractors are to maintain confidentiality regarding any information gained through their work and not divulge personal or business information about participants, families, colleagues or staff. Staff and contractors of AACA are required to comply with the AACA Code of Conduct with respect to Privacy.

When handling confidential information, staff must:

- Confirm details before sending faxes, emails or any other electronic communication
- Ensure AACA disclaimers and privacy expectations are included in emails for recipient information

#### *Banks & Financial Institutions*

AACA will monitor the security arrangements around critical financial assets and maintain regular due diligence on their security. AACA's banks and investment companies will be required to meet AACA's standards around security systems and processes.

## *Downloading software and suspicious emails*

- software, emails and applications downloaded from the internet can contain viruses that threaten the security of information stored on users' computers. Emails from unknown senders are not to be opened, and unauthorised software is not to be downloaded.
- Training is provided to all AACA staff on the phenomena of PHISHING emails to increase awareness and to minimise the risk & likelihood of staff downloading virus-infected items.

## *Cloud storage*

Access to Cloud-based platforms must be authorised by the director on decisions about what data is stored in the cloud and must remain in the scope of the staff member's assigned role and task. Information on cloud storage systems should not be saved as a 'screenshot' or photographed (or alike) except with appropriate levels of authorisation for an authorised purpose.

- Employees must comply with authorised log-in protocols and generally must not share Log On credentials with co-workers or others.
- It is imperative that employees NOT open unauthorised cloud service accounts
- Employee must NOT enter into cloud service contracts for the storage, manipulation or exchange of company-related communications or company-owned data without the full knowledge and authorisation of the General Services Manager.
- Use of cloud computing services for work purposes must be formally authorised by the director. The director will certify that security, privacy and all other IT management and requirements will be adequately addressed by the cloud computing vendor.
- For any cloud services requiring users to agree to terms of service, the director must review and approve such agreements.

### 1.1.6 Information Value

Information Assets will be compiled by the director and kept current and reviewed annually. Information (of all types and across its life cycle) will be assessed & rated according to its value and integrity & assigned a level of confidentiality status. All AACA personnel must comply with all systems and processes within AACA to ensure security controls are upheld according to confidentiality ratings.

### 1.1.7 Information management

In consultation with Google and the AACA staff, the management team will regularly refer to the Information Assets register for training and induction purposes and to inform document control & information retention policy. AACA is moving increasingly to a paperless working environment; however, documents of historical value and documents stored in secure locations will continue to be monitored.

## *Handling Confidential Information*

Confidential information may only be collected, accessed and used for a valid work purpose.

- Hard copies of confidential information to be kept securely
- Staff/volunteers must be aware of surroundings and people nearby such as clearing printer copies – management to monitor
- Staff must limit taking hard copy information away from secure sites
- Staff must secure hard copy information when travelling

- Staff must dispose of hard copy information in a timely and secure manner such as via shredding or confidential bin or file appropriately
- Management and key staff are to ensure that information is available to people who need access to it.

## INFORMATION DISPOSAL

Ensure record retention requirements have been met prior to the disposal of any business information.

When disposing of confidential information:

- Place unneeded working documents or copies of information in secure bins or other methods authorised by AACA management occasionally.
- Ensure any electronic media including computers, hard drives, USB keys etc are sanitised when no longer required. Staff are required to comply with AACA's sanitising schedule, which occurs quarterly for USB sticks.
- It is noted that with remote working environments, the need to comply with regular disposal of confidential information, which is no longer required, must be prioritised and discussed with your manager in line with the AACA document disposal schedule.

### 1.1.8 Information Sharing

#### Sharing confidential information

Any request to staff from government bodies or external organisations for information regarding participants must be checked and approved by the director before it is released in line with privacy protocols and legislative requirements.

All AACA staff and volunteers sign the Confidentiality Statement with specific information about maintaining the privacy and confidentiality of shared information. This is reviewed annually.

Contractors and external parties operate via Service Agreements, which outline how confidential information will be handled and AACA's expectations concerning this shared information.

Confidential information may be shared only:

- when a formal agreement exists in relation to information or data sharing between parties such as funding bodies requiring participant data
- in the circumstances permitted under Privacy Legislation. e.g., Court orders, Disability Royal Commission or circumstances supported by Freedom of Information protocols.
- when Consent is gained from the person or a person's authorised representative to share.

Images or information about participants are not to be shared with members of the public or at public forums without the consent of the management once consent has been received by the participant or their family.

The management is to ensure that AACA has gained written consent from the participant or as appropriate (e.g., authorised participant representative) which in most cases will be the primary carer or designated persons under Guardianship and Administration rulings. If there is ambiguity in consent, AACA will seek advice from the Office of the Public Advocate. In circumstances where written consent is not possible, verbal consent may be sought. The designated staff member is to make participant file notes as appropriate, noting who gave consent, what the consent was for, and the date.



**Images of participants** (including uploading to our website, newsletters and Annual Report – hard and soft copy) may be posted on social media and AACCA's website occasionally. Only appropriate, respectful images with the participant/family's prior consent will be featured.

## 1.1.9 Personnel Security

AACA staff and volunteers undergo NDIS Worker Screening Check and Working with Children Checks during the term of their employment with the organisation. Internal monitoring systems ensure that out-of-date security status for staff or volunteers automatically bars them from employment until up-to-date security checks are completed.

Regular training is offered to staff regarding their security obligations (including cyber security obligations) and the Code of Conduct is revisited annually.

Personnel files are stored as electronic files in restricted access hard drives on AACCA computer systems. Some historical financial data in hard copy is stored securely. These are stored in line with our document storage retrieval and destruction procedures. This data is destroyed at the designated destruction date.

Staff undertake online training in mandatory areas via authorised online training platforms, training completed by staff and volunteers is monitored and recorded by AACCA.

An exit/termination checklist is completed for all personnel leaving the organisation. This includes the return of keys, role-related resources, blocking access to electronic files, and changing any security passwords.

## 1.1.10 Information Communication Technology (ICT) Security

Our IT Service Provider will implement the following IT strategies to comply with the Essential 8 mitigation strategies to prevent malware and mitigation strategies to limit the extent of cyber security incidents.

### Mitigation strategies to prevent malware

- Application whitelisting
- Patch applications
- Configuration of Microsoft Office macro settings
- User application hardening (web-browser applications and macros are disabled or blocked), firewalls and virus protection

### Mitigation strategies to limit the extent of cyber security incidents

- Restrict administrative privileges
- Patch operating systems
- Multi-factor authentication
- Ransomware (Sophos)

### Mitigation strategies to recover data and system availability

- Daily backup of important data
- Ransomware (Sophos)



## 1.1.11 Physical Security

Confidential information should NOT be recorded in the subject line of emails. All confidential information should ONLY be transmitted via authorised AACCA mailboxes.

### Physical Security and Conversation

1. Staff must clear desks and screens
  2. Maintain an environment clear of sensitive information when unattended
  3. Be mindful when conversing with others, of the risk of private or confidential information being overheard and shared in contravention of the privacy protocols of AACCA
- These points especially apply when staff work in the community or open space environments.

## Portable Storage Devices (including USBs, mobile phones, and tablets)

Portable storage devices are usually small and capable of storing large amounts of information, and in some cases, can be used to copy, transmit or share information.

Using portable storage devices to access, store or transport confidential information involves considerable risk because:

1. they can be easily lost or stolen and then accessed by unauthorised people
2. using portable storage devices in public or non-agency premises increases the chance of accidentally disclosing confidential information to unauthorised people.

To minimise the information security risks associated with using portable storage devices:

1. only use password-protected portable storage devices to store confidential information
2. avoid storing confidential information on portable storage devices, where possible
3. secure portable storage devices when unattended, e.g. lock them in a drawer
4. report lost or stolen portable storage devices immediately to your manager
5. record all devices on a central IT Information asset register

## Personal storage devices (including personal mobile phones)

Information/images should be transferred to an AACCA-authorised location such as a designated computer as quickly as practicable, preferably that day, and then deleted and should not be saved on an unauthorised external computer or other devices such as personal mobile or tablet.

AACCA acknowledges that the ability to have photographs taken and information stored of the participants is of tremendous benefit to participants and their families. It is also mindful of the challenges and opportunities that image usage, recording and sharing present, e.g., outcome measurement.

Information or images of participants recorded on personal devices should be temporarily kept securely and password protected. Such information or images should not be shared with any unauthorised person and importantly should not be shared with people outside AACCA. The transfer and destruction of any image must be in line with the AACCA storage policy as outlined above.

*AACCA will comply with any revisions or developments in relation to privacy and confidentiality, including cyber security through regular monitoring and review of the above policy.*

---

## RELATED REFERENCES

- Australian Privacy Principles
- Privacy Amendment Notifiable Data Breach Act 2017
- “Data breach notification: a guide to handling personal information security breaches” Office of the Australian Information Commissioner
- Guide to securing personal information January 2015
- The Information Privacy Act 2009 (QLD)
- Privacy and Data Protection Act 2014
- Health Records Act (2001)
- Essential Eight “The Australian Signals Directorate’s (ASD) Strategies to Mitigate Cyber Security Incidents”
- Standards Australia's "Information Security Management - implementation guide for the health sector" HB 174-2003;
- Electronic Communication and Social Media Policy
- Information Management Policy and Procedure
- Consent Policy and Procedure