PRIVACY AND CONFIDENTIALITY POLICY AND PROCEDURE
Purpose and Scope

This policy and procedure have been structured to communicate to workers the correct and appropriate means for the security of confidential information. This policy and procedure extend to all 'My Abilities Support Teams' workers, and failure to abide by this will result in strict disciplinary action. This Policy and Procedure also relates to the Records and Information Management Policy and Procedure.

This extends to all workers and meets relevant laws, regulations, and standards.

This policy and procedure have been structured to communicate to workers the correct and appropriate means for the security of confidential information. This policy and procedure extend to all 'My Abilities Support Teams' workers, and failure to abide by this will result in strict disciplinary action. This Policy and Procedure also relates to the Records and Information Management Policy and Procedure.

This extends to all workers and meets relevant laws, regulations, and standards.

Definitions

Health Information	Data related to a person's medical history, including symptoms, diagnoses, procedures, and outcomes.
Confidentiality	The state of keeping or being kept secret or private, professionals should not share personal details about someone with others unless that person has provided

	consent, or it is absolutely necessary.
Personal Information	Any information relating to an individual.
Sensitive Information	Sensitive information relating to the business, staff or participants that should not be shared with others unless consent is provided or absolutely necessary.
Privacy	The state of something being free from public attention.

Policy

M.A.S.T. supports the privacy and confidentiality of their workers and participants by utilising records and Information Management Policy and Procedure. M.A.S.T. is required to protect workers' and participants' privacy continuously. Every person has the right to decide with whom to share personal information. Workers remain responsible for the privacy and security of the participants and fellow workers. Before any data is gathered, M.A.S.T. must ensure that the information is used correctly and appropriately.

The procedures of privacy and confidentiality communicate with the lifecycle of data as follows:

- Create a collection of all forms of participant details, relevant information, and service agreements to ensure they have given both verbal and written consent.
- Store all information securely per the Records and Information Management Policy and Procedure and limit access.
- Use the information to update when applicable, disclose the information to staff members and report if necessary.
- Archive the documents securely once the participant has exited the service as per the Records and Information Management policy and procedure and limit access.
- Once the archive period is complete, dispose of documents securely as per the Records and Information Management policy and procedure.

Procedure

The M.A.S.T. owner/director is committed to ensuring that M.A.S.T. follows the 1988 (Cth) Privacy Act standards, as well as any other relevant government and territory laws and specifications.

All 'My Abilities Support Teams' workers must read and comply with the state and federal legislation concerning privacy and confidentiality, including this policy and procedure. This includes document and information:

- Collection/Creation
- Process
- Storage
- Utilisation
- Disclosure
- Disposal

M.A.S.T. is required to give workers appropriate training regarding their knowledge of systems in place for the confidentiality of company data; this will be done through performance reviews. If it is found that a worker does not encompass correct knowledge, suppose it is found that a worker does not contain correct understanding. In that case, extra training may be given to ensure consistency throughout M.A.S.T., in conjunction with the Human Resources Policy and Procedure. The M.A.S.T. Privacy Statement must be in the M.A.S.T. Participant Handbook.

Personal Information

M.A.S.T. is required to provide workers with consent forms for personal information, which will be considered respectfully, and no information will be used without consent.

Personal information includes but is not limited to the following:

- Photographs
- Films
- Recordings
- Personal information

Participant Information Collection and Consent

M.A.S.T. will only require confidential information to determine potential participants' suitability for plan management services and to monitor the services provided.
A participant is entitled to supply, access, update, and use any personal information if necessary to ensure correct information is in the system; they may refuse to disclose some information and have the right to revoke their consent to disclose personal information.
Before collecting personal information from participants or their advocates, 'My Abilities Support Teams' workers must clarify why the information is being collected, exactly how it is being stored and used, as well as why M.A.S.T. requires the information. M.A.S.T. only gathers the necessary personal information of participants for the protected and adequate provision of plan management services. All private and confidential information must be stored safely.
M.A.S.T. implements and employs Privacy Statements for participants, their family members, and advocates. The Privacy Statement is a document M.A.S.T. provided which has information on how M.A.S.T. abides by all privacy laws whilst protecting participants who are in direct communication with participants, or their related personnel must do the following:

- Ensure they have signed their own privacy statement annually and it is kept up to date.
- Provide written information to participants if requested (such as this Policy and Procedure).
- Provide verbal information to participants if requested.
- Understand and comply with participants' (or their related personnel) communicational requirements, such as overcoming any language barriers.

'My Abilities Support Teams' workers will support participants if they need to gain access to an interpreter if required. Participants, their family members, and advocates are accountable for ensuring the correct use of others' personal information, the return of the consent form, respecting people's wishes not to be captured on camera, and ensuring the communication of accurate information.
Following the information provided in this policy and procedure, 'My Abilities Support Teams' workers must use a Consent Form to verify and clarify the information stated in this policy and procedure. This consent form indicates whether participants have allowed M.A.S.T. to hold, retain and use vital information of the participant. This information may include the following; however, it is not limited to:

- Full Name
- Nationality
- Date of Birth
- Preferences
- Personal Goals
- Medical Information
- Referrals
- Case/Progress Notes

Personal Worker's Data

Personal Worker's data includes but is not limited to:

- Personal Information (Contact, Residence etc.)
- Payroll Information
- Qualifications
- Contract of employment
- Consent Forms
- Specifics regarding qualified registration
- Tax returns
- Medical Information
- Results of Background checks

Audits

An NDIS-approved quality auditor has the right to request an interview from any participant file that requires assessment. M.A.S.T. must ensure they are abiding by the standards outlined in the 2018 National Disability Insurance Scheme (Approved Quality Auditors Scheme) Guidelines. This automatically includes participants in the NDIS Practice Standards audits. However, a participant may refuse to participate in audits with a written notice directed to the M.A.S.T. owner/director.

Privacy and Confidentiality

Worker or participant personal information can only be disclosed in order to comply with legislative responsibilities such as mandatory reporting when required by law.

If an individual is in a situation where they are unsure about disclosing another's personal information, they should communicate and discuss it with the M.A.S.T. owner/director.

International: M.A.S.T. is required to ensure that any foreign participants do not violate any Australian Privacy Principles (APPs); this is under the Privacy Act 1988. However, this requirement will not apply if the foreign participant is dependent on legislation or a critical system that has the power to protect private and confidential information in an approach significantly equivalent to that delivered by the APPs.

Storage and Access

View 'My Abilities Support Teams' Records and Information Management Policy and Procedure for additional details on exactly how M.A.S.T. systems can ensure privacy for storing and protecting private data.

Both the M.A.S.T. owner/director and workers will only access the personal information if it is necessary to fulfil any responsibilities or services for the M.A.S.T.. All stakeholders can request access to any information regarding themselves. Any participant access or modification demands must be presented to the individual of M.A.S.T. who is responsible for monitoring the Participant's personal information. All workers have the same access to or requests for modification as participants.

The M.A.S.T. owner/director should be notified immediately, within two business days, for any access or correction of information. The individual responsible for the acceptance status of information will l either accept or reject it with reasoning as to why.

A request for access or correction may be rejected as it would have an unwarranted impact on the privacy and confidentiality of other individuals. The proposal is thoughtless and annoying. It may cause a dangerous threat to any individual's life or well-being. All participant requests for access or correction refused by the Director must be authorised and documented in the participant's file. Any workers who have been denied access or correction requests must be approved by the Director and recorded in the individual's file.

Notifiable Data Breaches Scheme

The Notifiable Data Breaches (NDB) Scheme is a federal scheme under the Privacy Act 1988 (Cth). M.A.S.T. is required to report any incidents to the Australian Information Commissioner. A data breach happens when the private information retained by companies is damaged, or exposure to it is not permitted. A data violation can occur due to the failure of Management or security systems, deliberate intent, or technical failure. Additionally, damage can be done that causes significant economic harm.

Violations

Violations include but are not limited to:

- Devices and documents containing private or confidential information are lost or stolen
- Unapproved entry by a worker to personal information
- Unintentional release of private or confidential information.
- Hacking of electronic devices

Identifying a Notifiable Data Breach

A Notifiable Data Breach occurs when M.A.S.T. cannot prevent the potential risk of harm through corrective measures. It also appears when the release or access to private information is not permitted, or data is lost in circumstances in which unauthorised access or release is probable to be present. Release or loss is expected to affect all individuals involved with the information.
Severe damage may include damage to credibility in the form of a breach of information which may result in:

- Physical damage
- Emotional damage
- Financial damage

Any suspected or current information breaches must be identified to the M.A.S.T. owner/director, who is responsible for assessing the action of M.A.S.T. and if the breach is to be registered under the NDB Scheme. It will not be considered a notifiable data breach if the Director of M.A.S.T. responds promptly to reduce the information violation.

Responding to a Data Breach

Should the situation arise where any persons of M.A.S.T. believe there has been a significantly damaging data breach, the M.A.S.T. owner/director is responsible for the immediate investigation of the incident. If required, the M.A.S.T. owner/director may liaise with external organisations to minimise the opportunity for reoccurrence, theft, and harm. If the data breach is considered notifiable by the M.A.S.T. owner/director, the Data Breach Response Team of M.A.S.T. must be advised.

The M.A.S.T. owner/director is responsible for the following:

- assessing the risk from infringement;
- supporting the Human Resources Manager where the worker's actions caused the infringement;
- providing media/communications knowledge and helping to communicate with impacted people and deal with media and external stakeholders;
- acting as Project Manager, coordinating the team and supporting its participants;
- acting as Senior Worker to introduce privacy knowledge to the team;
- acting as Team Leader, accountable for guiding the reaction team and reporting to the Director (unless they are the same person);
- legal assistance, identifying legal commitments and providing guidance;
- supporting information and communication technology (ICT) or forensics, helping to define the cause and effect of infringement involving ICT technologies.
- Providing information and documents management knowledge, assisting in the review of breach-related safety, tracking checks (e.g., access, authentication, encryption, audit logs) and providing guidance on recording data breach reaction.

All implicated individuals will be informed of the breach of information as promptly as possible by the Data Breach Response Team. M.A.S.T. must continuously utilise and refer to the Data Breach Response Plan should the situation occur. This event should be documented in the Incident Register, with information on which efforts were utilised to prevent the situation from occurring again.

Should a data breach event occur, M.A.S.T. follows a methodological process to minimise the damage of the event as well as appropriate input measures to prevent future occurrence.

The Data Breach Response Team or the M.A.S.T. owner/director is responsible for managing this incident. They must begin with controlling information violation, meaning they must put into effect appropriate measures to minimise which information may be viewed or leaked. This can be done by removing electronic files from the location of the breach into an external hard drive inaccessible to others. They then must formulate a conclusive list/record of which

information was breached and discuss or implement measures to minimise any associated or related threats to others. For example, M.A.S.T. may have to change personal financial or business details to ensure the safety and protection of the organisation and its workers. M.A.S.T. must then evaluate the overall threat and the possible extenuating circumstances that may arise due to the breach. For example, it may be notifiable to the Australian Information Commissioner or notifiable to Management, workers, or participants of M.A.S.T.. M.A.S.T. must then input preventative measures to minimise the risk of recurrence. This may include liaising with an external organisation, such as an IT company, for further assistance.

Other Reporting Requirements

Any breaches must be immediately reported to the NDIS Commission by the M.A.S.T. owner/director of M.A.S.T.. Violations of information may also affect reporting obligations beyond the Privacy Act 1988, such as:

- Government Departments of the Federal, State or Territory
- Insurance providers
- The Australian Securities and Investment Commission (ASIC)
- Australian Reporting and Analysis Centre (AUSTRAC)
- Australian Tax Office (ATO)
- Australian Prudential Regulation Authority (APRA)
- Australian Cyber Security Centre (ACSC)
- Australian Digital Health Agency (ADHA)
- The financial service sector of M.A.S.T.
- Professional and regulatory organisations
- The police or other law prosecution organisations

To ensure that M.A.S.T. cooperates completely with the Standards:

- The Director will collaborate with the Government on the implementation of risk-based reporting mechanisms and ensure that M.A.S.T. takes reasonable steps to protect all M.A.S.T. participant records.
- The Director will create an immediate measurement of information security.
- Subscribe to the Stay Smart Online website at https:/www.staysmartonline.gov.au.
- Review ‘My Abilities Support Teams’ compliance with Essential Eight and rectify any identified gaps.
- This website helps with knowledgeable online behaviour patterns as well as how to respond to internet threats.

Supporting Documents

Documents relevant to this policy and procedure include:

- Governance - Continuous Improvement Register
- Records and Information Management Policy and Procedure
- Participant Handbook
- Participant - Consent Form
- HRM - Privacy and Confidentiality Agreement
- Human Resources Policy and Procedure
- Incident Management - Incident Register

Policy Review

M.A.S.T. may make changes to this policy and procedures from time to time to improve the effectiveness of its operation. Generally, this entire policy will be reviewed in consultation with people using the service, their families, carers and workers every year.

All activities related to service planning, delivery, and evaluation will include workers, participants, and other stakeholders, and their feedback.

Acknowledgment

By signing this document, I acknowledge that I have read and understood the Privacy and Confidentiality Policy and Procedure. I agree to comply with this policy and procedure, and that M.A.S.T. management can change or update the policy if required.

Signed: _____

Endorsed by:	Reason/Section Update	Next Review
Director of M.A.S.T. – Cezanne Vennitti	Initial Release- V1.0 Dec 2023	April 2024