SD - Collection, Storage & Use of Information

Headway Gippsland Inc. has a legal obligation to disclose personal information to the government or under health regulations, or where such disclosure is permitted by law, including under privacy laws.

This policy document is available on the staff portal or available at the request of participants.

Collection of Personal Information:

To provide our service and conduct business, we are required to collect a range of personal information. We primarily collect information to assess, plan and manage participant's needs in providing services to them. If a participant provides incomplete or inaccurate information to us, we may not be able to provide them with the services they require.

Definitions:

Privacy breach	Is any disclosure or confidential information in a written, verbal, ICT or loss of ICT devices. Whether the disclosure is accidental or deliberate and regardless of whether the member is paid, volunteering or contracted.
ICT/cyber breach (Information and Communications technology)	Is defined as when the computer network is breached by an external party or a third party attempts to breach the system. Examples could include: ▪ Staff downloading information that they are unauthorised to have or downloads information for malicious purposes. ▪ A virus. ▪ Workers sharing passwords.
Notifiable data breach	Unauthorised access to, or disclosure of, personal information (or if information is lost in circumstances where this could occur); and; A reasonable person would conclude that this would, or could be likely to result in serious harm to any of the individuals to whom the information relates.

SD - Collection, Storage & Use of Information

	It does not matter if the above occurs due to human error or if the act is deliberate. The extent of the breach does not relate to if the breach is reportable or not. The breach can affect one individual or multiple and if it meets the above criteria would still be reportable to the OAIC (the Office of the Australian Information Commissioner).
Serious Harm	What a reasonable person on the street would believe would cause harm. It is not determined by the reaction of the individual that has been affected. Serious harm includes physical, psychological, emotional, economic and financial harm and serious harm to reputation. The likelihood of harm is also assessed by the vulnerability of the individual affected, length of time it took to report the breach, where the information was lost and the sensitivity of the information.
Remedial action	The organisation response and the plan put in place to contain an accessed breach.
Data breach statement:	The document that must accompany a notifiable data breach to the OAIC.
OAIC	Office of the Australian Information Commissioner.
Personal information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.' Examples include: • Name, address, birth date, telephone number • Age, sex, marital status • Biometrics • Educational, financial, criminal or employment history and

	• Photograph and voice recordings.

Participants:

If a participant receives our services, we may need to collect personal and medical information about client status, occupational health and safety, work processes, and other relevant information. The information from clients is only used for the purpose for which it was collected in connection with the delivery of services.

Staff:

We need to collect personal details from staff, including but not limited to name, address, contact details, qualifications, banking details, study, visa/residency status, Working with Children's Check and NDIS Worker Screening Check. In some cases, we must also collect health information about a person's health or disability. We use information collected from staff only in connection with the delivery of service.

Family & Friends:

We need to collect next-of-kin details from participants. We use this personal information only in an emergency.

Sometimes we are legally required to collect personal information, including where there is a threat to public health, or in connection with the monitoring of health services provided by Headway Gippsland Inc. Our use of personal information in such instances will be in accordance with our obligations under applicable privacy and health acts.

Although Headway Gippsland Inc. primarily collects personal information to assist participants' needs in providing our service to them, we may also collect, use and disclose personal information about participants for other related purposes, such as:

- To meet government and regulatory requirements in relation to activities such as quality assurance, compliance issues and complaint management.
- For invoicing, billing and account management.

Use & Disclosure:

SD - Collection, Storage & Use of Information

Headway Gippsland Inc. may at times disclose personal information about participants where it is necessary to deliver services. We will not rent, trade or sell personal information about participants to third parties. Personal information may only be disclosed outside of Headway Gippsland Inc. in circumstances where:

- Participants have consented to the disclosure, and
- Disclosure is in accordance with the purpose for which we collected the information.

To meet service needs Headway Gippsland Inc. may be required to discuss a participant's personal information with other agencies or service providers. Should this be required the participant's consent to share information will be acquired using the Consent to release of confidential information form.

Headway Gippsland Inc. has a legal obligation to disclose personal information, such as to government or under health regulations, or where such disclosure is permitted by law, including under privacy laws.

Security of Personal Information:

Headway Gippsland Inc. takes all reasonable steps to safeguard the security of personal information we have collected and hold. We may store personal information electronically on our computer database and/or in hard copy documents kept at our premises.

We have procedures in place to protect personal information from unauthorised access, use, modification, or disclosure. Headway Gippsland Inc. staff who handle personal information have a duty to protect that information and are granted access to personal information on a 'need to know' basis.

Headway Gippsland Inc. ensures that personal information no longer required is destroyed appropriately.

Data Breach Plan:

Key points:

- A Privacy breach must be reported to the Department of Health and Human Services within one working day.
- A privacy breach that impacts a client's safety and wellbeing may need to be reported as a client incident under CIMS as well as through a privacy incident report.
- A Notifiable data breach defined above: must also be reported to the OAIC. The report must have within it a Data breach statement and action plan.
- If a breach occurs externally via another provider consult with the provider to determine where the breach occurred.
- Management of staff involved in a data breach will be managed in line with Human Resource process.

Process for reporting a data breach:

SD - Collection, Storage & Use of Information

Data Breach Response Team	Responsibilities
Staff Member	Reports any privacy concern to their manager or most senior person on duty as soon as possible.
Manager	Take detailed notes of the incident. If it is an ICT issue, alert Glen from Edcomp I T Services. Determine whether the incident requires notification to the CEO e.g., is serious harm likely to occur and how the breach can be contained. Determine how long the incident took to be uncovered. The longer the information has been exposed the greater the risk of harm. Staff performance management if required (can only be conducted by Headway Gippsland Inc. CEO).
CEO	Notify the participant about the breach and provide support as required. Notify the police as required for example a physical breach. Complete CIMS report as required. Complete date breach report to Office of the Australian Information Commissioner as required. Notify the DHHS as required. Report to the Board of Management. Ensure review of the Data Breach plan occurs as part of internal audit. Implement actions following review of a breach for example procedure review, staff training.
Board of Management	Review and assessment of the data breach response and the effectiveness of the data breach response plan.

Examples of Privacy Breaches & Privacy Risks:

- Staff conversations that are overheard via a third party that could reasonably identify a client
- Leaving behind documentation at case conferences or meetings that hold participants' information or business information
- Sending an email to the wrong recipient
- Accessing information that a worker does not have a need to know
- Handing the wrong documentation to an individual
- Disclosing information about a client to a third party without their consent (unless under other legalisation such as the best interest of the child or FV information sharing, harm to the client, harm to others, etc.)
- Leaving information on desks where contractors or other individuals can see it.
- Leaving the computer screen visible containing client information that third parties can see.
- Loss of ICT (Information and Communication Technologies) device
- Saving documents to the desktop and not the server
- Publishing of a photograph without written/verbal consent.
- Server being hacked or getting a virus
- Contractors being present and exposed to confidential information
- File cabinets not being locked
- Documentation being transported without a manilla folder
- Worker sending confidential information to their personal Hotmail, Gmail, etc. accounts
- Sharing of computer passwords
- Passwords being left in a visible place

Access & Correction:

SD - Collection, Storage & Use of Information

Staff and participants have a right to request access to personal information that Headway Gippsland Inc. holds about them and to update or change personal information about them if it is inaccurate, incomplete or outdated.

If a staff member or participant wishes to exercise their right to seek access to the personal information that Headway Gippsland Inc. holds about them; they must contact HR Department at the Morwell office (03) 5127 7166 or by emailing hr@headwaygippsland.org.au. A request for access to personal information must be made in writing stating exactly what personal information you wish to access or correct.

Headway Gippsland Inc. will respond to all requests for access to personal information within 14 working days; depending on the type of personal information the staff member or participant have requested access to.

Concerns About Privacy:

Any concerns or comments about this privacy policy, the practices of Headway Gippsland Inc. or requests for access to personal information can be made via:

Mailing Address: CEO
Headway Gippsland Inc.
219 Prince Drive
Morwell Vic 3840

Telephone: 03 5127 7166

If a person cannot seek redress through the organisation's grievance procedures, they can lodge a complaint with the Office of the Victorian Information Commissioner:

Mailing Address: PO Box 24274
Melbourne VIC 3001

Email: enquiries@ovic.vic.gov.au

Retention & Disposal of Personal Information:

It requires the organisation to retain information where it is required and to dispose of it securely when it is no longer required.

Headway Gippsland Inc. shreds all personal information that is no longer required.

REFERENCES

SD - Collection, Storage & Use of Information

Charter of Human Rights and Responsibilities Act 2006 (Vic)

Protects all human rights, including the right to privacy.

Privacy Principles March 2014

Information Privacy Act 2000 (Vic)

IPA - promotes the responsible and transparent handling of personal information and balances the free flow of information with the protection of personal information.

Health Records Act 2001 (Vic)

Protects the health information of an individual

The Privacy Act 1988 (Commonwealth)

Covers the handling of personal information

Privacy Amendment (Enhancing Privacy Protection) Act 2012

Privacy Amendment (Notifiable Data Breaches) Act 2017

The Notifiable Data Breaches (NDB) scheme introduced an obligation to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm. This notification must include recommendations about how individuals should respond to the breach. The Australian Information Commissioner (Commissioner) must also be notified of eligible data breaches.

RESOURCES

Data Breach Statement
https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach/

What is Personal Information?
https://www.oaic.gov.au/agencies-and-organisations/guides/what-is-personal-information#how-does-the-privacy-act-define-personal-information

Identifying eligible data breaches
https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/identifying-eligible-data-breaches

Department of Health and Human Service reporting
Privacy Team on 03 9096 8449 or email privacy@dhs.vic.gov.au for advice.