Headway Brain Injury Services and Support

Data Protection Policy

Safeguarding Personal Information

Purpose of this Document

This policy describes how Headway meets its obligations to individuals and the law regarding the safeguarding of personal data. The policy addresses the core principles set out by the Data Protection Commission for compliance and good practice within the current Data Protection Legislation, the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) of 2018.

The document is publicly accessible and for all Headway staff.

General Statement

The office of the Data Protection Commissioner outlines principles of data processing which are binding on all organisations who handle personal data. This policy describes how Headway adheres to those principles.

Document Data

Policy Title:	**Data Protection Policy**
Document Author	Richard Stables, Information and Support Manager
Date of Last Revision	**12/05/2026**
Date of Next Review	12/05/2027

Revision History

For list of revisions since publication, see the Appendix: “Revisions to this document”

Table of Contents

Introduction

Headway takes the safeguarding of personal information very seriously. In addition to the measures outlined in this policy, Headway takes particular care when handling the sensitive personal information entrusted to us by people who use our services. These measures can be found in an accompanying procedure:

- Client Records Management Procedure

Policy

1. Fairness, Legality, Transparency

Transparency and Fairness

i. Our data collection always aims to be open and transparent. At the time we collect information about individuals, they are made aware of the following information:

- The basis for gathering and processing the data, for example the person's consent.
- How long we intend to keep the data
- The right of complaint where clients are unhappy with our implementation of any of these criteria,
- Their individual rights to access, correct or delete records held by us.

ii. Examples include: for assessment of application for service, for planning service delivery, for provision of information, research, recruitment and for marketing and fundraising purposes.

iii. Headway will not use any automated decision making such as profiling.

The Legal Bases for Processing Personal Data

i. Headway uses **consent** as the principal basis for processing the data about its service users. Most of the information we gather from application forms or during the course of providing a service is subject to our clients' consent, which is recorded. This basis is also used for subscribers to our electronic mailing lists.

ii. Some personal data may be processed for the purpose of providing people who enquire about our service with information or materials, and this will be on the basis of **contract performance**.

iii. There are some circumstances where other grounds for processing data may occur, e.g. in an emergency to protect the **vital interests** of the client or a child or vulnerable adult. These are highlighted in the limits of our confidentiality and explained in our privacy notices.

iv. Certain data are subject to the use of **legitimate interest** as the basis for processing, for example, our funders require certain data to monitor the funding that it provides to Headway or in another example, HR data on Headway employees, next of kin details, CCTV footage. Where data is subject to this basis, we make the person aware via privacy notices that this data may be processed without consent.

Special Categories of Data

v. Headway maintains some personal data that falls into the category of that designated as “special” under Article 9 of the GDPR. This includes, for example, health data about service users and some limited health data on employees.

Explicit consent is used as the legal basis for processing data in the “special” category – for example gathering and maintaining any health-related information about service users.

Vital interest is used as the basis for processing such data in occasional circumstances, such as the disclosure of medical information to relevant personnel in a medical emergency.

2. Purpose Specification

Headway recognizes the need to hold personal data about individuals for the following purposes:

i. Rehabilitation Service Provision to People with ABI and family members

The data we collect for this purpose includes:

Name, address, date of birth, telephone, email address, emergency contact info, gp contact info, referral information, country of origin (optional), language (optional), ethnic background (optional), religion (optional), citizenship status, living and working situation, brain injury circumstances, details and hospitals attended, current needs and difficulties, medication, substance use history, brain injury service history, current medical status (including medication, allergies, seizure history), rehabilitation assessment and progress records, identified needs, photograph, consents (including email opt in and SMS opt in), images, including photographs for identification purposes, media such as recordings of consultations or therapy (made with consent).

The majority of the data collected for this purpose falls into the category designated as special under GDPR (ref Para v on page 6)

ii. Generation of service statistics and data to inform service improvement

All data for this purpose is anonymised fully prior to processing.

iii. Information mailings and events

Data gathered for this purpose includes:

Name, email address, postal address (where relevant), consents, reported relationship to brain injury, mobile phone number

iv. Fund-raising and development

Data gathered for this purpose includes:

Name, email address, postal address (where relevant), consents, reported relationship to brain injury, donation history.

v. Purchases and Donations

Name, email address, telephone number, order/donation details, delivery address.

vi. Website Optimisation and Functioning

Headway uses website cookies for tracking site visitors. The Headway website cookie policy explains which cookies we use for which purposes and is available at Cookies policy - Headway (https://headway.ie/cookies-policy/)

vii. Premises Security

Data gathered includes:

CCTV images from property entrances and carpark areas. See Appendix 8 – CCTV Policy and intent

viii. Research

Data gathered for this purpose includes:

Informed consent, name, address, date of birth, injury status, injury history.

ix. Human Resources

Data gathered for this purpose includes:

Employee data: Name, address, telephone, email address, next of kin contact, bank details, employment history and records.

x. At each point of data collection, we are clear to individuals about the purposes to which that information is being put. For example, the Headway application form states:

I give consent for Headway Ireland to maintain all personal data concerning my medical, educational and occupational history relevant ***to providing me with rehabilitative services***

xi. Privacy notices are displayed on the website, and on application forms where data is gathered.

xii. Permission to contact individuals in relation to participating in research is explicitly sought via the Headway service application form and separately for each research project undertaken.

3. Adequate, relevant and limited to what is necessary

i. It is the policy of Headway to develop and maintain a complete and accurate record to ensure that all appropriate individuals have access to relevant clinical and other information regarding each client.

ii. We collect and maintain only sufficient information for the declared purpose in order to provide a fair and comprehensive service to each person.

iii. We only hold that information which is necessary to the purpose it serves. If we are in receipt of personal data e.g. in the form of medical records, which is extra to requirement, we ensure that the information is returned to the referring agent or destroyed as appropriate.

iv. The internal Headway working group on intake and referrals conducts annual reviews of the information collected on the referral form to ensure that it is sufficient and not excessive.

v. The individual record of each person is maintained in such a manner as to protect the confidentiality and integrity of the record.

vi. All records of staff client interactions are maintained in a professional manner are done so with the expectation that the information can be shared with the person served.

vii. Rules governing the use of information for research purposes are set out clearly by the Headway Ethics Committee. (see the document “Guidelines for Ethical Research, Procedures for Obtaining Ethical Approval & Operational Procedures for the Headway Research Ethics Committee”)

Person Responsible: Information and Support Manager, Service Managers and Individual Keyworkers.

4. Accurate and up to date

i. Headway employees who maintain personal data are responsible for correcting and maintaining that information on an ongoing basis. For example:

- Keyworkers are responsible for maintaining the contact information and the personal data held in the Penelope Case Management System. The secure maintenance and update of records is described in the internal procedure “Client Records Management procedure”.
- Fundraising admins are responsible for maintaining the accuracy of fundraising lists
- The Information and Support Manager is responsible for maintaining the accuracy of distribution lists for newsletters.
- The Human Resources Manager is responsible for maintaining the accuracy of the HR Management system and the management and secure storage of the CCTV footage.

ii. Headway undertakes regular checks on the records of the person served in the form of an annual audit to ensure the accuracy, relevance and current validity of the data.

iii. When errors are identified, these are rectified as soon as possible

5. Data Retention

i. Personal information (e.g. about a client) processed/kept for any purpose will not be kept longer than is necessary for that purpose.

ii. Headway follows HSE guidance for data retention periods. The minimum period set down for the retention of records is eight years generally, 20 years in the case of "mentally disordered persons". The general schedule for retention of records in Headway is as follows:

Purpose	Retention Schedule
Rehabilitation Service (except neuropsychology tests) Provision to People with ABI and family members	8 Years following final closure of case, or duration since final contact, whichever most recent. Exception to this is in case of death by suicide, in which case duration is 10 years after death. See appendix 2 and neuropsychology test results (below)
Neuropsychology test results	Retained for 15 years (provides a baseline for some clients returning to service following discharge).
Information mailings	For individual queries, data retained for one year. For mailing distribution lists where user has opted in, data is retained for as long as mailing list is maintained.
Fund-raising and development	Data is retained for as long as mailing list is maintained, then subsequently deleted.
Research	8 Years following completion of research

Human Resources	See appendix 1 HR record retention schedule.
Purchases and Donations	All accounting records held for a period of 6 years. Transaction data for purchases deleted after 1 month.

See also Appendix 1 and Appendix 2

iii. Purging of data occurs on an annual basis, and as once-offs on completion of purpose, e.g. completion of a research project. All records will be destroyed in accordance with Data Protection law and Headway's guidelines for retention and destruction as follows:

a. All records involved in any investigation, litigation, or audit will not be destroyed until legal counsel has confirmed that no further legal reason exists for retention of the record.

b. In the event a legal proceeding is initiated against Headway, the Data Protection Officer will be notified immediately by a relevant Service Manager to stop the destruction of files.

c. All records will be destroyed in a manner that eliminates the possibility of reconstruction of the information. Paper records will be destroyed by shredding. Any CD-RW disks that contain document imaging that cannot be overwritten will be destroyed through pulverization. Electronic records will be either deleted or fully anonymised to prevent future identification.

d. Any contracted services for the destruction of Headway's records will be provided according to the following contractual guidelines:

- The method of destruction will be specified.
- The time between the acquisition and destruction of the records will be specified.

- Established safeguards to protect the confidentiality of the records will be described and noted.
- The contractor will provide proof of destruction

6. Integrity and Confidentiality

i. Personal data is held within a number of secure systems within Headway, according to the purpose of holding the data. Personal data for client service provision and research is held within an electronic case management system, and in paper files. Data for other applications is held within the Human Resource Management system, one of the Third-party processors listed in Appendix 4 or held on the firewall protected internal network.

ii. Clients are informed about Headway's record keeping practices including the creation, storage, security and retention of records.

iii. Staff access records on a "need to know" basis only.

iv. All personal data held on Headway clients for service provision and research is deemed sensitive, falling into the category of "special" data as defined under Article 9 of GDPR and maintained with high levels of protection. The following physical and software safeguards are in place to protect sensitive personal data:

Security of Confidential Client Records

Personal data for client service provision and research is held within a case management system, and in one or more paper files which are stored in the Central Location of each geographical area.

Electronic Client Records

The electronic client record maintained on the online Case Management System. This is a secure online system with the following security protocols in place:

- Access is controlled on role-based security – only those who need access to the data can access it.

- There are robust technical safeguards based on best practice risk management frameworks, including encryption and other technical safeguards. For further information refer to Penelope | Privacy and Security Information | Penelope Help Center (intercom.help) at

  https://intercom.help/ssgpenelope/en/articles/5342186-penelope-privacy-and-security-information

- Complex passwords and two factor authentication, to protect from unauthorized access.
- All data records maintained in electronic systems are backed up on a daily basis

Paper Based Records

- All Paper based client records are managed by the designated Coordinators of Referrals.
- All paper records are kept in areas that provide reasonable protections from fire, water damage, and other hazards.
- All paper records are stored in locked cabinets/areas with keys accessible by appropriate staff members only.
- Efforts are made to avoid removing any part of the paper record outside of Headway facilities. When required, only copies of the absolutely necessary documents are taken out. In these instances, the staff member will transport the documents in a locked case/container and they are marked as confidential.

Responsibility: Service Managers

Human Resource Management System

i. Human Resource paper files are maintained securely in locked cabinets. Access to Headway staff information is controlled and limited to Human Resources Personnel and the CEO. Access to volunteer

records is controlled and limited to the relevant Manager and Human Resources

ii. Electronic records are maintained securely on a network drive with secure password. Access is limited to authorised personnel.

Person Responsible: Human Resources Manager, Managers

Network Data

i. All data held on Headway Networks is maintained behind a secure firewall on password protected PCs and is restricted access only to authorized employees. Network data is also maintained in secure cloud locations, such as Microsoft One Drive – (see Third Party processors in Appendix 4)

ii. The Network server is held in a dedicated securely locked room.

iii. All domain registered devices are protected by an additional layer of security using the local operating system firewall, in addition to the organisational network firewall.

iv. A password policy and two factor authentication is in place to secure access to the internal network to authorised users only.

Person responsible: Human Resources Manager/Information and Support Manager.

Laptop and Mobile Device Security

i. All Laptops for use external to Headway with client personal data are encrypted.

ii. All mobile devices containing personal data are password protected. As a minimum, all mobile phone devices must be protected by the use of a Personal Identification Number (PIN). Where it is technically possible the mobile phone device must be password protected.

iii. The use of USB sticks for data transfer is not permitted except where the USB is fully encrypted and password protected

Person responsible – Human Resources Manager, All

CCTV Footage

i. All CCTV footage is held on the HR Manager's computer, behind a security firewall or on DVDs kept in a locked cabinet.

Third-Party Data Processors

i. Headway will validate the adequacy of security and data privacy in accordance with GDPR for any third-party processing data on its behalf **prior to** granting permission to access the data for processing. Examples of third-party processors include:

- Shredding companies
- Mailing Services
- Cloud data hosting companies

ii. Agreements with third party processors will provide evidence of data security controls and indemnify Headway against costs arising from any legal proceedings in relation to data loss.

Person responsible: Information and Support Manager, Relevant service managers.

Data Transfers Abroad

i. Headway uses third party processors for hosting personal data which involves transfers of that data to countries outside the EU. To comply with Data Protection Legislation, the countries must be considered as offering an adequate level of protection in accordance with Articles 45 and 46 of the GDPR.

ii. A list of third-party processors used by Headway is in Appendix 4

Disclosures

i. Headway commits to using the personal data gathered from individuals only for the purpose for which it is gathered. The maintenance of the client's record is covered by the internal procedure "Client Records Management Procedure". All clinical workers are made aware of this procedure through the induction process. It is the policy of Headway to ensure that all verbal and written information of clients is released in a manner that protects the individual's right to privacy. Headway will make all reasonable efforts to limit use, disclosure of, and requests for private or personal information to the minimum necessary to accomplish the intended purpose.

A. Internal sharing of information

1) In Headway, rehabilitation is usually provided by an interdisciplinary team, Information pertinent to the rehabilitation needs of the client will be shared within this team. Clients are made aware of this in the privacy notice included with the relevant consent forms. Only information pertinent to the stated purpose (eg. Provision of rehabilitation) will be shared within the team.

2) We recognise that some of the information we maintain about clients is of a personal or sensitive nature. Permission to share information of this nature will always be sought where appropriate.

3) Staff will ensure a reasonable balance between maintaining the confidentiality of personal information and the need to communicate information relevant to the provision of a service via a team. In situations where there is any doubt about a clients expectation of confidentiality, we will assume that consent for disclosing the information should be explicitly sought.

4) Staff will have clear and detailed conversations with clients informing them about the limitations of confidentiality within Headway.

5) Clients are required to sign a written agreement indicating understanding of and consent to the terms of confidentiality.

B. Sharing information externally

ii. Individuals are made aware of all disclosures to third parties, and consent is always sought and recorded for such disclosures with exceptions as referred to in paragraph vii

iii. Disclosures are typically related to the further provision of service to an individual. Consent for some disclosures is explicitly sought using the application form, which states:

I give consent for Headway Ireland to maintain all personal data concerning my medical, educational and occupational history relevant to providing me with rehabilitative services.

I give consent for Headway Ireland to release reports and information on my rehabilitation and progress to my G.P or other professionals involved in my care

iv. Disclosures beyond “GP and other professionals involved in my care” will always be explicitly sought and recorded, with exceptions as referred to in paragraph viii

v. Particular care is taken in gathering consent for the use of photographic or video media, which are typically personal data. Clients must be made aware of the scope of disclosure for these materials, e.g. on social media and must give informed consent for their use.

vi. Information disclosed to third parties may be in written or verbal form. All requests for information by individuals for information held on them by Headway are made using the procedure described in section 8 in this policy.

vii. There are certain circumstances where Headway would be obliged to process data on a different basis than consent. These typically include in an emergency situation to protect the vital interests of the data subject or a child, vulnerable adult or member of the public. Another example would be at the request of Gardai investigating a crime. In such cases, full reference will be made to the current legislation via approval by the Headway Information and Support Manager.

Disclosure without consent

If we have to disclose information without client's consent, the following procedure will apply:

a. Staff will inform the relevant manager of the event as soon as possible.
b. Staff will take necessary measures to best ensure the safety of all concerned (e.g. contacting GP, family member, Gardaí as necessary)
c. If deemed safe to do so, the client will be informed of the disclosure.
d. Staff will record the event, including name, date, to whom the information was disclosed, reason for disclosure and any follow up actions.

Security during Disclosure

1) Headway will protect the confidentiality of private information when transferring data electronically by adherence to the following guidelines:
    a. All data sets containing individual names transferred by e-mail or any other electronic medium will be encrypted and password protected.
    b. The sending and receiving parties prior to transfer of the electronic data will negotiate passwords.
    c. Passwords will be at least eight characters in length, contain both letters and numbers, and must not be commonly used words.

d. Passwords for files may not be mailed in the same mail as the encrypted file.

2) Headway will adhere to the following guidelines when posting confidential private information:

   a. Stamp all envelopes containing records as confidential.

   b. Information released (e.g. reports, medical information) will be clearly marked as ‘copy’.

   c. Clearly indicate a particular office on the address where the envelope is to be delivered.

   d. Whenever possible, include in the address the name of the staff member authorised to open the envelope.

   e. All envelopes individually addressed will be clearly marked as confidential to the recipient.

3) Any information released verbally over the phone, can only be done when reasonable measures have been taken to ensure confidence as to the identity of the caller.

4) A log will be maintained on all records released by Headway. It will include the date, nature and purpose of each disclosure, the name of the party to whom the disclosure is made. This record will be maintained by completing the ‘Record Release Notification Form’ on the case management system.

7. Demonstrating our Compliance

i. The mechanisms by which we demonstrate our compliance with the requirements under the Data Protection Act include:

ii. Establishment of a Data Protection Officer (DPO) for the organisation, this is the Information and Support Manager.

iii. This policy is circulated amongst all employees and all employees undergo annual training in its content.

iv. All consents are recorded in the client records.

v. Data security is regularly reviewed, and paper files are subject to annual audit

vi. All privacy notices are available from the Headway website at headway.ie/privacy-policy

8. Supporting Individuals' Rights

i. All individuals have the right to access all the personal data held on them by Headway or to have that information corrected. If the data was given via the basis of consent, that consent may be withdrawn.

ii. Individuals may have the right to have their data deleted permanently. This will typically apply when Headway relies on your consent to process the data. A request for erasing data can be made using the procedure outlined below (see Personal Data Access Procedure).

iii. Headway takes the stance that individuals may need assistance to request access to their own personal data. Headway will provide advice on the easiest route to achieve this.

iv. Individuals also have the right to request any information we hold about them to be provided in a portable electronic format. In most cases, this will be in the form of adobe pdf (portable document format).

9. Training & Education

i. This policy is circulated to all new staff as part of their induction process

ii. Annual training is provided through the learning management system and is mandatory for all employees.

iii. Awareness of Data Protection issues is through updates from the Information and Support Manager.

10. Co-ordination and Compliance

i. All breaches of this policy will be reported to the Data Protection Officer following the Data Loss Notification Procedure below.

ii. A review by the co-ordinator of data protection activities within Headway will take place every two years across the organization

Procedures

Personal Data Access Procedure

- All requests must be made in writing with the consent of the person served (excepting the conditions outlined under section 3. Vi and 3.vii in this policy).
- All requests should be made using the form attached (appendix 3) and sent to

  Information and Support Manager
  Headway
  Blackhall Place
  Off Blackhall Green
  D7

- Where requests are received in writing not using the standard form, e.g. from solicitors, staff should check the validity of the request before notifying the Information and Support Manager. The request must quote the Data Protection legislation and also include the person served written consent. When in doubt, revert to the requestor with the standard form in appendix 3.
- The Information and Support Manager must be notified of all requests for disclosure of personal information.
- The Information and Support Manager will record the request and notify the Service Manager(s) connected with the case.
- The Service Manager or Referrals Coordinator will coordinate the file duplication and disclosure in line with the Policy on Management of Confidential Client Information.
- The information will be supplied within one month of the date of receipt of the request.

Procedure for Subject Access Requests

In the receipt of a valid request under GDPR for a subject to access their information,file preparation will begin as soon as possible following receipt of the request for date. This process includes;

a. Gathering all relevant data on file pertaining to the client

b. Redacting names and identifying information of all other clients

5) Files will be placed in a sealed envelope/box and clearly marked 'CONFIDENTIAL'

6) Unless otherwise determined by the recipient, courier services will be used to transport envelope/box. If appropriate the envelop/box can be collected by the client's solicitor or a nominated representative of the solicitor

7) At the point of release of information, the individual receiving the documents will sign the 'Information Release Form' (Appendix 1), acknowledging receipt of information. This form will be kept in the physical file from which the information is being released.

8) If request is for erasure (as permitted since GDPR), all records will be erased or anonymized completely, and checked/reviewed by the Information and Support Manager.

9) If the request is for a copy of materials in a portable format (as permitted since GDPR) all hard copy materials will be scanned and the files assembled as pdf files.

Requests made under the Freedom of Information Act (1997 and 2003)

i. Headway is not a prescribed body under the terms of the Freedom of Information Act. However, records that are created in dedicated services subject to contracted service level agreements with HSE are deemed to be held by the HSE and thus, may be subject to come within the scope of the act.

"Section 6(9) provides that the records of contractors to public bodies are deemed, insofar as they relate to the contracted service, to be held by the public body concerned."

ii. Headway's policy is to comply fully in a timely manner with all Freedom of Information requests made by the HSE under the terms of the service level agreements.

iii. If a request is received by Headway under the terms of the Freedom of Information Acts, it should be immediately forwarded to the Information and Support Manager for further action and processing.

Procedure for Data Loss Notification

A breach is a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, for an authorized purpose, have access or potential access to personal data in usable form, whether manual or automated.

This could mean:

- Loss of a laptop, memory stick or mobile device that contains personal data
- Lack of a secure password on pc's and applications
- Emailing a list of students to someone in error
- Giving a system login to an unauthorised person
- Failure of a door lock or some other weakness in physical security which compromises personal data

What happens if a breach occurs?

Actual, suspected, or potential breaches should be reported immediately to the Headway Data Protection Officer (DPO – the Information and Support Manager).

Any employee who becomes aware of a likely data breach and fails to notify the DPO will be subject to Headway's disciplinary procedure.

A team comprising the DPO and other relevant staff will be established to assess the breach and determine its severity. Depending on the resulting risk to the individual(s) involved, the Office of the Data Protection Commissioner and relevant regulatory bodies will be informed as quickly as possible following detection.

In certain circumstances Headway may (e.g. if required by the Office of the Data Protection Commissioner), inform the data subjects of the loss of their data and provide them with an assessment of the risk to their privacy. Headway will make recommendations to the data subjects which may minimise the risks to them. Headway will then implement changes to

procedures, technologies or applications to prevent a recurrence of the breach.

When will the Office of the Data Protection Commissioner be informed?

All incidents in which personal data has been put at risk will be reported to the Office of the Data Protection Commissioner. The exception to this is where the breach is unlikely to result in a risk to the rights and the freedoms of the individual.

This reporting will be made immediately and at most within 72 hours of the incident.

Data Loss Incident logging

All data breaches will be recorded in an incident log as required by the Office of the Data Protection Commissioner. The log will maintain a summary record of each incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record will include a brief description of the nature of the incident and an explanation of the assessment of risk to the affected individuals. Such records will be provided to the Office of the Data Protection Commissioner upon request.

Appendix 1 – Retention Schedule – HR records

General classes of records held HR	Default retention period	Final disposition
Annual/sick leave records	2 years	Destroy
Records of staff training	1 year	Destroy
Applications and CV's of candidates who are called for interview	Retain for 2 years after closing of competition	Destroy
Candidates short listed but not successful at interview or who are successful but do not accept offer	Retain for 2 years then destroy	Destroy
Interview Board marking sheet and interview Board notes	Retain for 2 years then destroy	Destroy
Finance/pension/ retirement records	Retain until pensioner and dependent spouse are deceased and dependent children are finished full time education plus 3 years.	Destroy
Staff Personnel Files	Retain for duration of employment. On retirement or resignation hold for a further six years but retain service records for finance/pension purposes. Destroy remainder listed below.	Destroy
Discipline records	Hold on personal file/disciplinary file for duration of employment plus six years after resignation/retirement, then destroy. Where the matter involved criminal activity these records should be retained indefinitely.	Destroy/Archive
Surveys/reports	Retain indefinitely	Archive
Union correspondence	Retain indefinitely	Archive

Individual industrial relations issues	Retain indefinitely	Archive
Labour Court Recommendations	Retain indefinitely	Archive

Appendix 2 Guidelines on Retention of Client Records

Type of information	Schedule	Comments
Records of people deceased by suicide	Retained for **ten years** following date of death	Notification of death by suicide must be made to Information and Support Manager
Records of people subject to unfinished court action, where known.	Retained **indefinitely**	Notification of applicable cases be made to Information and Support Manager
Individual records of the persons accessing Headway services following needs assessment (except neuropsychology test results)	Retained for **eight years** after the most recent discharge date.	Paper and electronic media
Individual records of the persons attending needs assessment but subsequently deemed ineligible for services **or** clients who have been invited to needs assessment but decline to attend	Retained for **eight years** following final closure of case.	Paper and electronic media
All preadmission application and screening records of persons deemed not eligible to Headway's services at that time	Paper file maintained for **one year**. Electronic record subject to same	

(i.e. not attending needs assessment)	retention period as other client records (8 years). Forms having no identifiable information regarding the person served will be destroyed in **one year**.	
External referral forms for referrals to Headway	To be included in the record for persons admitted and will be retained for the **same period** as the record itself (see above)	
Information for statistical/ Audit purposes	There will be **no time limit** on such information being retained at this generally will be anonymous.	Information to be held anonymously where possible. Exceptions may need to be made for purposes of funder reports, accreditation audits.

Appendix 3 – Personal Data Request Form

(see over)

Personal Data Request Form

Information Manager
Headway
Blackhall Green,
Off Blackhall Place
Dublin 7

[Date]

Dear Sir/Madam,

I wish to make an access request under Article 15 of the General Data Protection Regulation (GDPR)

	I wish to have a paper copy of any information you keep about me, on computer or in manual form.
	I wish to receive a copy of any information you keep about me in a portable electronic format
	I wish to have all information you retain about me deleted from your system
	I wish to have information you have about me corrected (please specify)

Regards

(signed)

[your name]

Name*: (please print)* _____

Email: (*please print*) _____

Address (please print)*:* _____

_____

_____

Request in writing should be made and signed by the applicant in person. Within the terms of the GDPR, Headway will respond to your request for personal data within one month of date of request. Requests should be submitted to: Information Manager, Headway, Blackhall Green, Off Blackhall Place, Dublin 7

Please Note:

1. Request in writing should be made and signed by the applicant in person.
2. Within the terms of the GDPR, Headway will respond to your request for personal data within one month of the date of the request.

Requests should be submitted to: Information Manager, Headway, Blackhall Green, Off Blackhall Place, Dublin 7

Appendix 4 – List of Third-Party Processors

Salesforce Customer Relationship Management (US)	Salesforce complies with the EU-U.S. “Privacy Shield” Framework which the EU considers to offer an adequate level of protection for personal data. A full breakdown of data privacy tools can be found at https://www.salesforce.com/company/privacy/ and details specific to the GDPR can be found at https://www.salesforce.com/gdpr/overview/ A data processing agreement addendum in place (DPA) Person Responsible: Information and Support Manager
Penelope Case Management System (Canada)	Penelope Case Management system uses Amazon Web Services based in Canada for the secure hosting of client records. Canada’s Data privacy regime is approved by an adequacy decision of the EU. The physical security of the data server is described in document Penelope_Privacy_and_Security_Whitepaper.pdf available on the I drive and online at https://www.athenasoftware.net/wp-content/uploads/2018/03/Athena_Software_Privacy_and_Security_Whitepaper.pdf In terms of the external security, it is encrypted, and access is protected by usernames and passwords The server level access is controlled by a firewall and intrusion detection monitoring system in place. As some of the data held on the case management system is of a sensitive nature, extra internal security is configured within the system to limit access to personal information to those working with the case. Person Responsible: Information and Support Manager, Service Managers, Keyworkers
Microsoft Office 365 (US)	Headway uses Microsoft Office 365, part of the Microsoft Cloud to host email and shared network resources. Office 365 incorporates privacy by design, and Microsoft has robust policies, controls, and systems built into Office 365 to help keep personal data private. The commitment to compliance with the General Data Protection Regulation (GDPR) from Microsoft is explained in the document at

	https://blogs.microsoft.com/on-the-issues/2017/04/17/earning-trust-contractual-commitments-general-data-protection-regulation/ All processing with Microsoft office based software is conducted under the terms of the Data Processing Addendum, text of which is available at Licensing Documents (microsoft.com) (https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA) Person responsible: HR Manager
e-Commerce system (Mals-e, US)	Headway uses Mals-e ecommerce system for handling purchase transactions from our website store. Data on this system is regularly purged and order data is retained only for a period of 1 month following transaction. The financial transactions are processed through Paypal (see below). See https://www.mals-e.com/privacy.php Person Responsible: Information and Support Manager
Paypal (US)	Paypal's Binding Corporate Rules (BCR) provide the security for compliance with GDPR. Refer to Paypal's privacy statement at https://www.paypal.com/en/webapps/mpp/ua/privacy-full Person Responsible: Information and Support Manager
Mailchimp (US)	Mailchimp is used for bulk email communication and is GDPR compliant, see their Data Processing Addendum for details, Mailchimp Data Processing Addendum Preview | Mailchimp Person Responsible: Information and Support Manager
SurveyMonkey (US)	SurveyMonkey is used for gathering feedback from the public. Their GDPR compliance is explained in a white paper at https://cdn.smassets.net/assets/cms/cc/uploads/SurveyMonkey-GDPR-Whitepaper-Dec19.pdf Person Responsible: HR Manager

Tidio Website Chat (US)	Tidio website chat is used for providing instant support via the website. The system is fully compliant with GDPR, see https://www.tidio.com/knowledge/faq/gdpr-compliance/ for details. Person Responsible: Information and Support Manager
Eventbrite (US)	Eventbrite is used for invitation lists and event management, and is fully GDPR compliant, see https://www.eventbrite.co.uk/support/articles/en_US/Troubleshooting/eventbrite-privacy-policy?lg=en_GB Person Responsible: Information and Support Manager
Pearson Clinical Q-Interactive Systems	Headway uses some technological tools to administer some of its psychological evaluations. Data for these is processed by Pearson Clinical UK, and information is stored using Amazon Web Services (AWS) in Canada. See AWS Amazon Web Services Hosting FAQs for Q-global and Q-interactive (pearsonassessments.com) Link text: (https://www.pearsonassessments.com/content/dam/school/global/clinical/us/assets/q-interactive/AWS-FAQ.pdf) for more information. The Pearson Q privacy policy details exactly what information is gathered at Privacy Policy (qiactive.com) Link text https://qiactive.com/choose-share/pearson/managePolicyTypes/showPolicy?id=13C73E5A5916BE2EE050A00A32A955AE

Appendix 5 – Example Privacy Notice

Privacy Notice - Please read this important information

Protecting your personal information

Headway staff will always treat your personal information with respect.

We will keep your data confidential and secure and **only use it for the purpose of providing you with a service**.

We will not share your information with other people without your permission unless we have to.

When Headway has to break confidentiality

The rare times we have to share your information include:

- if it is necessary to prevent harm to you
- if it is necessary to prevent imminent harm to someone else
- if you tell us that a person under the age of 18 is in danger of harm or may be
- if you tell us that a vulnerable adult is in danger of harm or may be
- if we must by law - for example: if a Court, or the Gardaí, tells us to share your information
- if it is necessary to keep the public safe.

Your rights

Under the the law, you have the right to:

- access the information Headway has about you
- have the information changed if it is wrong
- get the information in electronic format such as a pdf file
- ask Headway to delete your information.

To avail of your rights, you can download a **Personal data request form** from our website: **headway.ie/privacy-policy/** or phone us on 01 6040 800.

Comments and complaints

You can make a complaint or comment about any aspect of Headway or its services. Forms and our **Comments and Complaints** policy are available from

any member of staff, by phoning 01 6040 800 or from our website: **headway.ie/about-us/our-codes-policies/**

More information

You can get the full version of the **Headway's Data Protection Policy** from any member of staff, by phoning 01 6040 800, or from the our website: **headway.ie/privacy-policy/**

Appendix 6 – Information Release Form

Information Release Form

I _____ confirm that I am authorised to collect the Headway files and notes of_____ on behalf of _____.

Date: _____

Signature: _____

Witness: _____

Appendix 7 – Website cookie policy

Cookies policy

In a similar way to most websites the Headway site makes use of cookies. Cookies are small data files that are stored by your web browser on your computer. You can find out all about cookies and their uses on Wikipedia .

Headway uses cookies to:

- measure how people use our website so we can improve the content, structure and layout
- remember settings and preferences so we can tailor content to your specific needs
- help determine the effectiveness of online advertising and the targetting of those advertisements

Our cookies are not used to identify you personally. They are used to improve the effectiveness of Headway's online work and to provide you with a better end user experience on our websites.

Cookies used on the Headway site

By using the Headway website you may get first party cookies (i.e. set by the headway.ie domain) in addition to third party cookies (i.e. set by an external domain such as facebook.com). The following categories describe the range of cookies that can be used during your visit to our site.

Remembering settings and preferences

We use cookies to store preferences and settings from your visit. This includes the cookie used to check whether you have viewed our cookie banner so we don't show it to you again for thirty days.

Measuring website usage (Google Analytics)

We use Google Analytics to collect information about how people use this site. We do this to make sure it's meeting its users' needs and to understand how we could do it better.

Google Analytics stores information about what pages you visit, how long you are on the site, how you got here and what you click on. We do not collect or store your personal information (e.g. your name or address) so this information cannot be used to identify who you are.

Google provides details on the cookies used as well as a plugin that can be used to opt out of Google Analytics .

Social networks

Headway maintains active social network accounts particularly on Facebook and Twitter. We embed widgets from these networks to provide follow buttons, like boxes and stream embeds. This may result in cookies being set by these networks while using our site.

Twitter's privacy policy provides information on the data they collect, along with instructions on how to disable website tracking . Facebook's use of cookies is detailed on their help center.

Third party services

Headway makes use of a wide range of third party online services to provide features such as embedded video and social sharing. These services may set cookies when visiting our website:

- YouTube : embedded video : privacy policy (on Google)
- Vimeo : embedded video : privacy policy , cookie policy
- Issuu : embedded documents : privacy policy
- Tidio: Live chat – See Tidio Privacy Policy

- Learnupon: Online learning materials – Privacy policy

Managing and deleting cookies

It is possible to view, manage and delete cookies within your web browser. We have provided links to instructions on how to do this for the most common web browsers below. For all other browsers you should look for a section called ‘privacy’ or ‘security’ within the application settings or preferences.

- Microsoft Internet Explorer
- Google Chrome
- Apple Safari
- Mozilla FireFox
- Android Browser
- iPhone Safari
- Opera

Appendix 8 – CCTV Policy and Intent

The CCTV system comprises a number of fixed and dome cameras located around the company site and is wholly owned by the Company.

Objectives of the System

(a) To act as a deterrent against criminal activity affecting property belonging to the company.

(b) To increase the safety of staff, clients, and visitors.

(c) The System will not be used to monitor the movements of staff, clients, or visitors.

Intent

- The Company will treat the System and all information, documents and data images obtained and used therefrom as data which may be deemed personal data requiring protection under legislation.
- It is intended that the CCTV cameras will be used to capture images of intruders or individuals damaging property or removing goods without authorisation and release this information to and at the request of, the Gardai.
- Information captured as a result of the use of the System will not be used for any commercial purpose. The recorded images shall be stored on DVDs, maintained securely which will only be released to third parties for use in the investigation of a specific crime and with the written authority of the Garda Siochana. DVDs containing personal data will never be released to the media or other third parties for any purpose that is not permitted under the Policy without the Data Subject's consent.
- The planning and operation of the System has been designed to ensure that it provides maximum effectiveness and efficiency insofar as is reasonably practicable, but it is not possible to guarantee that the System will cover or detect every single incident taking place in the areas of coverage.

Appendix 9 – Revisions to this Document

Type	Author	Nature of Change	Date
Initial Release			**06/06/2013**
Addition	RS	Procedure on Data Loss Notification	08/08/2013
Review	RS	Section on Third party processors, device security and minor updates. Amendment to section on disclosure without consent.	23/01/2015
Review	RS	Incorporate requirements of GDPR	03/04/2018
Review	RS	Incorporate further details re legal bases and restructure policy in line with revised DPC principles	23/4/2019
Review	RS	Modify list of 3rd party processors and purposes	08/01/2020
Review	Richard Stables /Sonya Gallagher	Combination with Confidentiality Policy/Client Records policy and incorporation of CCTV policy	17/05/2023
Review	Richard Stables	Minor change to consolidate retention schedule of client records	08/05/2026