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 eight 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	**08/01/2020**
Date of Next Review	08/01/2021

Revision History

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

© Headway 2020

Table of Contents

© Headway 2020

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 accompanying policies:

- Client Records Policy and Procedure
- Management of Confidential Client Information Policy and Procedure

© Headway 2020

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**.

© Headway 2020

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 that this data may be processed without consent.

© Headway 2020

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).

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

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.

© Headway 2020

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 https://headway.ie/cookies/

vii. Premises Security

Data gathered includes:

CCTV images from property entrances and carpark area in the Dublin premises.

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***

© Headway 2020

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.

© Headway 2020

3. Adequate, relevant and limited to what is necessary

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

ii. 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.

iii. Reviews are conducted of the information collected on the referral form to ensure that it is sufficient and not excessive.

iv. 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.

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

© Headway 2020

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,
- 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

© Headway 2020

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 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.
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	Subject to same retention schedule as Client Records (see above and appendix 2)
Human Resources	See appendix 1 HR record retention schedule.

© Headway 2020

Purchases and Donations	All accounting records held for a period of 6 years. Transaction data for purchases deleted after 1 month.

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

© Headway 2020

6. Security

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 a case management system, Penelope, and in hard copy client files. Data for other applications is held either 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. All personal data is maintained in a secure manner. The following physical and software safeguards are in place to protect personal data:

Confidential Client Records

i. Information about clients kept in the Primary and/or Secondary paper file will be handled as indicated in the internal policies on Management of Confidential Client Information and the Client Records Policy and Procedure. These policies govern access, security and transportation for this information.

ii. See the policy on Management of Confidential Client Information for the procedure regarding secure disclosure to third parties of client information.

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

© Headway 2020

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.

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

Person responsible: Human Resources Manager

Laptop and 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.

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.

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.

© Headway 2020

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. Headway transfers some personal data to two countries outside the EU, the USA and (following 31/01/2020) UK.

iii. 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 rules governing use of data for day to day service provision are covered in the Headway Policy on the Management of Confidential Client Information. This is a detailed internal policy covering all aspects of handling sensitive client information for the purpose of providing a clinical service. The maintenance of the client's record is covered by the internal policy on Client Records Policy and Procedure.

   All clinical workers are made aware of these policies through the induction process. Additional information governing procedures for the disclosure of personal information are also found in the policy on Management of Confidential Client Information.

ii. 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")

© Headway 2020

iii. 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 vi.

iv. 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

but disclosures beyond “GP and other professionals involved in my care” should be explicitly sought and recorded.

v. Particular care should be 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. If disclosure of personal data to a third party is required which exceeds the terms of the provision within the consent declaration on the Headway application form (see para ii), consent will always be sought and recorded in such cases.

viii. 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

© Headway 2020

subject or a child or vulnerable adult. 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.

© Headway 2020

7. Demonstrating our Compliance

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

- Establishment of a Data Protection Officer (DPO) for the organisation, this is the Information and Support Manager.
- This policy is circulated amongst all employees and all employees undergo annual training in its content.
- All consents are recorded in the client records.
- Data security is regularly reviewed, and paper files are subject to annual audit
- All privacy notices are available from the Headway website at headway.ie/privacy-policy

© Headway 2020

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).

© Headway 2020

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.

© Headway 2020

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 annually across the organization

© Headway 2020

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 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.

© Headway 2020

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

i. Headway is not 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.

© Headway 2020

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

© Headway 2020

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.

© Headway 2020

Appendix 1 – Retention Schedule – HR records

General classes of records held HR	Default retention period	Final disposition
Annual/sick leave records	1 years	Destroy by confidential shredding
Time sheets	1 year	Destroy by confidential shredding
Records of staff training	5 years	Destroy by confidential shredding
Applications and CV's of candidates who are called for interview	Retain for 2 years after closing of competition	Destroy by confidential shredding
Candidates not qualified or short listed	Retain list of candidates who applied, but destroy material such as application forms and CV's after 2 years.	Destroy by confidential shredding
Candidates short listed but not successful at interview or who are successful but do not accept offer	Retain for 1 year then destroy	Destroy by confidential shredding
Interview Board marking sheet and interview Board notes	Retain for 2 years then destroy	Destroy by confidential shredding
Finance/pension/ retirement records	Retain until pensioner and dependent spouse are deceased and dependent children are finished full time education plus 3 years.	Destroy by confidential shredding
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 by confidential shredding

© Headway 2020

	Destroy remainder listed below.	
Parental leave	Retain for 8 years	Destroy by confidential shredding
Discipline records	Hold on personal file/disciplinary file for duration of employment plus six years after resignation/retirement, then destroy. Where disciplinary policy provides for earlier removal destroy but keep a record that a warning was issued. Where the matter involved criminal activity these records should be retained indefinitely.	Destroy by confidential shredding
Allegations and complaints	Where the complaint is found to be untrue or unwarranted make a note on personal file index that a complaint was made, but there is no need to keep detailed documentation or refer back to previous cases if further separate allegations are made in the future.	
Occupational health records	Depending on the types of materials to which the staff member was exposed (e.g. carcinogens) the health screening reports may need	

© Headway 2020

	to be retained for up to 40 years. Consult with your local Health & Safety Officer about retention periods for this class of record.	
Industrial relations files	Hold policy documents and the history of their evolution indefinitely.	Archive
Agreements-pay and others	Retain indefinitely	Archive
Leave policy	Retain indefinitely	Archive
Employment policy	Retain indefinitely	Archive
Surveys/reports	Retain indefinitely	Archive
Union correspondence	Retain indefinitely	Archive
Individual industrial relations issues	Retain indefinitely	Archive
Labour Court Recommendations	Retain indefinitely	Archive
Contracts for services Examples of contracts for services that may be held by Personnel/HR departments include EAP contracts with service providers and contracts with healthcare professionals.	Retain for the duration of the contract plus six years	Destroy by confidential shredding

© Headway 2020

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	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 **five years,** together with a note explaining the reason for non-	

© Headway 2020

(i.e. not attending needs assessment)	admittance (e.g. “does not meet criteria”). 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.

© Headway 2020

Appendix 3 – Personal Data Request Form

(see over)

© Headway 2020

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

© Headway 2019

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/ Person Responsible: Information and Support Manager
Penelope Case Management System (UK)	Following Brexit, the UK will retain alignment with EU Data Privacy legislation until the end of 2020. The situation regarding transfers to UK will be monitored in the event of a “no deal” Brexit and advice sought on compliance from the Data Protection Commission. 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

© Headway 2019

	https://blogs.microsoft.com/on-the-issues/2017/04/17/earning-trust-contractual-commitments-general-data-protection-regulation/ 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
Mailjet (EU)	Mailjet is used for bulk email communication and is fully GDPR compliant, see their privacy policy for details, https://www.mailjet.com/privacy-policy/ 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

© Headway 2019

Appendix 5 – 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

© Headway 2019