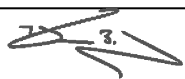


# Data Protection and the UK GDPR Policy

|                     |  |
|---------------------|--|
| <b>Owner:</b>       | <b>Chief Executive Officer</b>                       |
| <b>Relevant to:</b> | <b>Staff and stakeholders (including volunteers)</b> |

|                     |   |                  |
|---------------------|---|------------------|
| <b>Signed:</b>      |  |                  |
| <b>Approved by:</b> | Mark Trenavin-Body, Chair   | Date: 13/05/2025 |

| Dept: | Owner: | Approval/<br>re-approval<br>date: | Implementatio<br>n date   | Next<br>review<br>date: |
|-------|--------|-----------------------------------|---------------------------|-------------------------|
| SLT   | CEO    | 27 March 2025                     | 13 <sup>th</sup> May 2025 | March 2028              |

## New Policy or Substantive Policy Review

| Version | Date     | Policy Development Agreed by (SLT Owner) | Policy Development Author | Draft Policy Verified by | Policy Approval    | Impact Assessment (if applicable) |
|---------|----------|--|---------------------------|--------------------------|--------------------|-----------------------------------|
| 1.0     | Feb 2025 | Claire Boothby-Barnbrook                 | Claire Boothby-Barnbrook  | Michael Palmer           | Chair of the Board | Not applicable                    |

|   |  |
|---|--|
| <b>Rationale for new or substantive policy review</b> | No current policy. New policy needed to meet compliance. |
|---|--|

*Please make explicit if change/review relates to procedures, guidelines and associated documents only*

## Periodic Policy Review / Change History

| Version | Date of Review / Revision | Description of Change | Reviewed By | Approved By (SLT Owner) |
|---------|---------------------------|-----------------------|-------------|-------------------------|
|         |                           |                       |             |                         |
|         |                           |                       |             |                         |

|  |  |  |  |  |
|--|--|--|--|--|
|  |  |  |  |  |
|--|--|--|--|--|

**Communication**

To be agreed by the management team

|                 |         |                           |                   |
|-----------------|---------|---------------------------|-------------------|
| All Staff Email | 13.5.25 | Team Meetings & Staff Day | May 2025 & 9 June |
| Newsletter      | 1.6.25  | External website          | 1.6.25            |

**Contents**

1. Introduction.....3

2. What is personal data?.....3

3. Understanding the data protection principles.....4

4. Lawful basis for processing personal data.....4

5. What does this mean for Headway Norfolk and Waveney?.....6

6. Duty of confidentiality.....7

7. Individual rights.....7

9. Data breaches.....9

## 1. Introduction

Data protection is about giving people the right to have control over their own identity, but it is also about building relationships with those who use or support our services that are built on trust.

This document provides guidance to Headway Norfolk and Waveney (HNW) staff to assist the charity in meeting its data protection obligations.

Data protection law aims to make sure that personal data is gathered, stored and used responsibly and transparently. It gives people ownership of information about themselves. It works to limit how organisations use that data and forces them to use it responsibly.

The relevant law in the UK is the Data Protection Act 2018, which was updated in 2019 following the UK's exit from the EU. It is known as the UK GDPR as it aligns law in the UK closely to EU's GDPR.

The Data Protection Officer retains overall responsibility for ensuring we meet our obligations. However, the Board of Trustees must have oversight of this policy and ensure that we are fulfilling our obligations as a charity. In addition, all staff and volunteers are responsible for ensuring we collectively safeguard the personal data of our clients as well as any other sensitive information we handle as a charity.

Headway Norfolk and Waveney's Data Protection Officer is **Claire Boothby-Barnbrook**

## **2. What is personal data?**

It is any information relating to an identifiable living person, including but not limited to their name, address, phone number, email address or even National Insurance number.

From Headway Norfolk and Waveney's point of view, this could be clients, volunteers, committee members, donors, members of the public, event attendees, venue contacts or suppliers. These could be existing or former contacts whose data you no longer have reasonable cause to hold.

It is not only information about people that you are directly collecting that counts. It could also be information about people that others give you – or that you give to others.

Everyone has a fundamental right to privacy in their lives and an expectation that their data is treated respectfully and protected. This is because if personal data falls into the wrong hands, people could be harmed. Depending on the situation, they could become victims of identity theft, discrimination or even physical harm.

This is even more important when handling data of vulnerable people, such as brain injury survivors.

There are also special categories of personal data known as personal sensitive data. This is data regarding an individual's racial or ethnic origin, political opinion, religious or philosophical belief, trade union membership, genetic data and biometric data (fingerprints, eye scans etc.) for the purpose of uniquely identifying a person, data concerning health or data concerning a person's sex life or sexual orientation.

As special categories of personal data are more sensitive, there are extra safeguards in place to ensure the safe use and sharing of this information.

## **3. Understanding the data protection principles**

You need to know and understand what the legal principles of data protection are and what they mean for your branch. They are as follows:

- Lawfulness, fairness and transparency: Use data legally under a permitted lawful basis. These include consent, vital interests, and legitimate interests.
- Use data fairly, being clear, open and honest with people whose data you hold.
- Purpose limitation and data minimisation: Collect only what you need and use it as you planned and communicated you would.
- Accuracy: Keep your records up to date.
- Storage: Store all data securely and confidentially.
- Accountability: Take responsibility for what you do with data.
- Keep records that show what you're doing with data.

#### **4. Lawful basis for processing personal data**

There are different lawful reasons for processing personal data and special categories of personal data. Headway Norfolk and Waveney always uses at least one lawful basis for processing personal information and at least one lawful basis for processing special categories of personal data.

The six lawful reasons for processing personal data are:

- i. Consent – An individual has given consent for the processing of their personal data;
- ii. Contract – The charity has a contract with a person and needs to process their personal data to comply with our obligations under the contract; or we haven't yet to process the personal data to do what they ask;
- iii. Legal obligation – The charity is obliged to process personal data to comply with a legal obligation;
- iv. Vital interests – The processing of personal data is necessary to protect someone's life (vital interests);
- v. Public task – The processing of personal data is necessary under public functions and powers set out in law; or the charity needs to perform a specific task in the public interest;

- vi. Legitimate interests – The processing of personal data is in the legitimate interests of the charity, where we use an individual's data in ways that people would reasonably expect and that have a minimal privacy impact.

The lawful basis for processing special categories of data are:

- i. An individual has given explicit consent to the processing of personal data for one or more specified purposes, except where limited by law;
- ii. Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the charity or a person under employment, social security and social protection law or a collective agreement under law
- iii. Processing is necessary to protect the vital interests of a person or where the person is physically or legally incapable of giving consent
- iv. Processing relates to personal data which have been made public by a person;
- v. Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- vi. Processing is necessary for reasons of substantial public interest;

Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health, social care, treatment, or the management of health or social care systems and services on the basis of law or pursuant to contract with a health professional and subject to the duty of confidentiality.

## **5. What does this mean for Headway Norfolk and Waveney?**

There are a number of practical steps Headway Norfolk and Waveney staff should take in order to ensure compliance with the UK GDPR. Guidance is also available from the Information Commissioner's Office (ICO):

<https://ico.org.uk/for-organisations/business/assessment-for-small-business-owners-and-sole-traders/>.

Any Headway Norfolk and Waveney staff responsible for managing personal data should consider:

- *What personal data do we currently store?*

Remember, this is not just a contact list of service users. It also means any text messages or emails, meeting attendance records, and hard copies of correspondence, for example.

- *Where is it stored?*

Again, personal data is anything that could identify a living individual. So, for example, personal data could be stored in the form of a text message sent by a staff member to any member of the service delivery team or shared in a group WhatsApp chat.

Also, do not discount paperwork containing personal data, such as letters or copies of medical records. You need to have good reason to have such data, which must be stored securely.

- *How did we collect that data?*

Have our clients or those whose data we are storing given their explicit consent to the processing of their personal data? Do they know we have it and understand how we use it?

- *Who has access to the data?*

Limit access to any databases containing personal data relating to the branch to only those who need it. If you are storing or accessing a personal or shared computer, ensure that the database is password protected, with the password regularly updated and not shared with others.

- *How long do we need to keep the data?*

Funders may request that we store relevant information as part of our funding requirements. Similarly, information relating to safeguarding issues or other sensitive data may need to be held longer. Refer to the Data Retention section below and speak to the Data Protection Officer for more guidance.

- *Do we only collect and store personal data that we need?*

Review the personal data you hold and delete anything that you either have no lawful basis for holding or is not needed for the purposes of running the service including informal chats over WhatsApp, text or email.

- *Do we have a simple way for people to withdraw their consent – or ‘opt out’ – for their data being stored?*

See [Appendix 1 GDPR Request Flowchart](#)

- *Do all staff understand their personal obligations to the UK GDPR, including the sharing of any personal data with third parties?*

All new staff must complete Data Protection training as part of their induction training. All staff are required to refresh this training annually.

## **6. Duty of confidentiality**

Headway Norfolk and Waveney complies with a common law duty of confidentiality. This means that personal information that has been given to a member of staff by an individual should not be used or disclosed further, except as originally given by that individual, or with their permission.

Confidentiality clauses are included in all Headway Norfolk and Waveney contracts of employment.

## **7. Individual rights**

Individuals whose data is processed by Headway Norfolk and Waveney have a number of rights in law.

- i. Access – Providing the request is not manifestly unfounded or excessive, the charity will respond to a subject access request by an individual for access to the information we hold about them. There is normally no charge for this service. We will endeavour to respond within one month. We may take longer than one month and up to three months if the request is complicated. If extra time is required we will inform the individual of this prior to the deadline for a response.

- ii. Rectification – The charity will respond within one month to a request from an individual to have inaccurate personal data rectified (corrected), or completed if it is incomplete. Where the charity can lawfully refuse to rectify the data, we will explain why;
- iii. Erasure – The charity will respond within one month to a request from an individual to have personal data erased. Where the charity can lawfully refuse to erase the data, we will explain why.
- iv. Restrict processing – The charity will consider a request from an individual asking to restrict the processing of their personal data in the following circumstances:
  - a. An individual has contested the accuracy of the information and is waiting for us to respond or change the information;
  - b. An individual has objected to the processing and we are considering whether we have a legitimate reason to process the information;
  - c. The processing is unlawful but the individual concerned would prefer the charity to restrict the data rather than erase it;
  - d. The charity no longer needs the data but the individual requires it to establish, exercise or defend a legal claim.
- v. Data Portability – The charity will respond within one month to a request from an individual to move, copy or transfer personal data from the charity's computer network to another in a safe and secure way. We will do this in a structured, commonly used and machine readable form and free of charge.
- v. Object – The charity will consider a request from an individual objecting to the processing of their personal data in relation to:
  - a. processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
  - b. direct marketing (including profiling); and
  - c. processing for purposes of scientific/historical research and statistics.

## 8. Data Retention

The need to store data will be regularly reviewed based on the following guidelines:

- **Donor Records (e.g., Gift Aid Declarations)** – will be kept for at least **6 years** after the last donation.
- **Volunteer and Employee Records** – Typically **6 years** after leaving, but may be longer for safeguarding purposes.
- **Beneficiary Data** – Retain only as long as necessary; sensitive cases (e.g., safeguarding) may require longer retention.
- **Event Participation Data** – Usually **1-2 years**, unless required longer for reporting.
- **Marketing Consent Records** – Retain as long as you rely on consent, plus a short period for audit purposes.
- **Contracts and Agreements** – **6 years** from termination.

We commit to regularly reviewing and deleting/anonymising data no longer needed. We will ensure that all data is stored securely and disposed of correctly

## 9. Data breaches

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This could mean sharing personal email or home addresses without clear consent to do so, for example by sending out a mass email with the address shown in the To or Cc boxes. We suggest always putting email address in the Bcc box when sending emails to multiple recipients.

We all have a duty to protect the personal data of those who come into contact with the charity and report either internally or to the ICO any breaches that may occur.

If you suspect or are alerted to a data breach or suspected breach, please complete the [Data breach reporting form](#) and contact the Data Protection Officer (DPO) for Headway Norfolk and Waveney, Claire Boothby-Barnbrook

[claire.boothby@headway-nw.org.uk](mailto:claire.boothby@headway-nw.org.uk) **as soon as you become aware of the potential breach.** Personal data breaches that pose a risk to individuals' rights and freedoms must be reported to the ICO within 72 hours.

In addition, the ICO provides a self-assessment form to aid the decision-making process when assessing whether or not a data breach should be reported to the ICO: <https://ico.org.uk/for-organisations/report-a-breach/pdb-assessment/>