Data Protection Policy

Introduction

This document sets out the steps Healthwatch Northumberland is taking to comply with data protection law, keep data safe and only use for stated purposes. It covers the following:

- How we comply with data protection law, including the lawful basis for us to collect data.
- How we will ensure that we collect what we need and use is solely for the intended purpose.
- How we will keep personal data safe and secure.
- How and when we share data with other organisations, including other Healthwatch and Healthwatch England, and where we need to share data with other organisations because of safeguarding concerns.
- What we'll do if someone ask us to provide them with the data that we hold about them.
- Healthwatch Northumberland is the Data Processor for this policy.

Why we collect data

At Healthwatch Northumberland, we collect and process personal data for a variety of reasons:

- To give advice and information on how to resolve individuals' health or social care issues.
- To improve health and social care services at a local, regional and national level, including research.
- When people apply for a job or to volunteer for us or if we employ them.
- To send people our newsletter or other publications.
- Photographs and case studies for publicity purposes.
- In the event of a safeguarding matter.

What data we collect and why we collect it

We'll only collect the data that we need for each stated purpose. It will depend on the situation in which we are collecting the data.

Research, engagement, feedback, advice and signposting

We can collect personal information without asking for people's permission first. We can do this under the UK GDPR legal basis called 'performance of a public task'. This lets us carry out a task in the public interest or part of our official functions and has a clear basis in law. The law sets out our role in obtaining people's views of health and social care and providing them with advice.

We'll only collect the data we need for that purpose and no more.

This might include:

- Name and contact details including postcode.
- Details of the health or social care services people want to talk to us about.
- Details of people's experience of health and social care services.

We'll also ask people for sensitive information so that we can help them and understand how their circumstances might affect their experience of health and social care. These include:

- Their health conditions and disabilities
- Their ethnic origin.
- Their religion.
- Their sexual orientation.
- Their sex
- Their gender
- Their relationship status
- Their maternity status
- Their caring responsibilities

We may not ask people about all of these, and the individual may volunteer additional information about other sensitive categories of data. We tell people they don't have to provide us with the data if they don't feel comfortable doing so.

We're allowed to collect sensitive information like this because it is connected with the provision of and management of health and social care services.

In connection with working with or volunteering for us

Note Healthwatch Northumberland is delivered by Adapt North East which employs all staff.

We need to use personal information to recruit people to work or volunteer with us and ensure our recruitment processes are inclusive. If people apply for a job with us or to volunteer with us, we ask for the following information:

Name and contact details

DBS checks

Equality monitoring data

Disabilities and the reasonable adjustments we need to make

Proof of the right to work in the UK

We don’t insist that individuals provide us with this information, but if they provide it, we'll treat any diversity information as strictly confidential. We'll anonymise this information and only use it to look at trends. We won't look at people’s information individually or compare it to other people, and we won't use it as part of the recruitment selection process.

We collect personal information through the application form, interview or references so we can process the application. Data protection law allows us to do this to establish a contract with an individual.

If we employ someone, we maintain personal data in connection with their employment, including but not limited to personnel matters, sickness, performance and remuneration and payroll. We have a ‘legal obligation’ to process employee data.

We’ll keep the following information for people who work or volunteer for us:

- Original application form and references
- Training records
- Photos for ID cards
- Contact details of next of kin (where appropriate)
- Bank details for payment of salary or expenses
- Other personal data to manage employment or volunteering, such as performance and disciplinary matters

For employees, this will also include:

- Sickness records

We hold the following demographic information on staff and volunteers to monitor diversity and to understand different experiences of using health and social care services:

- Age
- Ethnicity
- Sex
- Gender identity
- Identity and belief
- Disability or long-term condition
- Family situation
- Housing
- Occupation

Other purposes including newsletter mailing list, being a case study or for publicity photos

We use MailChimp a third-party supplier to provide our newsletter service. The third-party supplier handles the data purely to provide this service on our behalf. This supplier follows the requirements of the Data Protection Act 1998 in how they obtain, handle and process your information and will not make your data available to anyone other than Healthwatch Northumberland.

We ask for individuals' consent to store personal data for all other purposes.

When people sign up for our newsletters, we collect personal information so we can:

- Send the information they've asked for.
- Let them know when and how we'll be contacting them in the future.

People can sign up by

- Ticking a consent box on a sign-up form.
- Completing a form or survey on our website.
- Asking our staff to add them to a mailing list.

We provide a means for people to unsubscribe at any time by including an unsubscribe link in all email communications and our contact details on paper consent forms.

We collect:

- First and last names.
- Organisation (if appropriate).
- Email address

We ask individuals' written consent to use their image. We explain images will represent a fictional person unless agreed otherwise in printed publications for promotional purposes, in press releases, on videos, on social media channels, in presentation materials and our website. It may also appear in our advertising and in the local/ national media.

The form explains how to withdraw consent.

For other purposes, we'll ask people to sign a consent form explaining how we intend to use their information and how they can withdraw their consent.

How we use people's information in accordance with the law

At Healthwatch Northumberland, we commit to:

- Only asking for what data we need for each purpose.
- Only using the data for the stated purpose.
- Providing people with:

    - A clear explanation of how we'll use their data.
    - The legal basis for processing it.
    - How they can access their data.
    - How they can withdraw consent (if applicable).
- Training our staff and volunteers on safe data handling in compliance with data protection law:
    - The training is tailored to Healthwatch's unique legal status.
    - Staff and volunteers have to undertake the training within two weeks of starting with us.
    - We ask them to repeat the training every year.
    - Ensuring that the data we store about people is accurate and that they have the opportunity to correct it.
    - Having a data protection officer to advise us on how to comply with data protection legislation.

How long we keep people's data for

We keep personal data for no longer than is necessary for the purpose we need it. Our data retention schedule sets out the time limits for keeping each type of personal data that we collect.

How we keep people's data safe

We have rigorous technical and organisational measures to keep people's data safe.

Only staff or volunteers with a legitimate business need have access to personal data relevant to the required task.

We use the following electronic systems to store data for our core activities:

- Engagement, Signposting, Information and Insight
- We use Smart Survey to collect feedback, advice, information or signposting. SmartSurvey does not access it for any purpose, except in the circumstances of account support with the permission of us as the account holder or for security purposes. All collected data can be deleted by HWN, via our response clearing tool by deleting individually or in bulk.
- Data is downloaded regularly and stored on secure folders on the organisation's server.
- Demographic data is downloaded and stored separately to the narrative feedback and in secure folders on the organisation's servers. We use Excel to store and analyse data from research or engagement projects.
- Details of ongoing enquiries are stored in a secure folder on the organisation's server and password protected. Passwords are only

available to HWN staff for continuity and records deleted in line with the retention policy.

Remote Access - HWN staff have remote access to the organisation's system using a secure VPN.

- Paper records - Paper records, predominantly surveys collected at engagement events or through the post or employment/volunteering records are kept in locked cabinets/drawers and care is taken to that it is not left unattended or in clear view during the working day. Paper records are destroyed in line with our retention policy.
- Information taken out of the office - The nature of our work means that information and records may be taken out of the office or collected and transported to the office base. Staff are required to keep these records to a minimum and securely as if it were in the office. This includes not in open view or left unattended. Documents should be locked out of sight in the boot of a car in a securely closed bag which has Healthwatch Northumberland's contact details in it.

Our electronic devices are professionally maintained to ensure security with updating, encryption and antivirus software.

Staff and volunteer permissions to access systems physically and remotely are withdrawn when they leave the organisation.

All data is cleansed from devices before they are disposed of.

Sharing data with other organisations

Healthwatch England

The law requires us to share data with Healthwatch England so that they can carry out their statutory functions.

We share the following data with them:

- Feedback and signposting data.
- Survey data.

We share this with them via a secure system directly into their Central Data Store.

Other organisations

We will share data with other organisations if there is a lawful basis for doing so, and we have a signed data-sharing agreement in place with them.

We are developing a data sharing agreement with the 14 Healthwatch organisations in the North East and Cumbria (the NENC Healthwatch Network) to help you

The NENC Healthwatch Network will collect and analyse public insight and in order to work collaboratively across the NENC Integrated Care Systems.

Data will be anonymised and shared securely

What we do if there is a data breach

We will make every effort to prevent a data breach, but should one occur, we will do the following:

- Within 24 hours of becoming aware of the data breach, we will assess the possible negative consequences for individuals as a result of the data breach.
- Within 72 hours, we will inform the Information Commissioner's Office if we assess that there are negative consequences for the individuals involved. We will take proactive mitigation actions and commit to taking any further remedial action they require to address the breach.
- Within 24 hours, we will start to address the root cause of the breach so that no further data is lost and, wherever possible, retrieved.
- Within 48 hours, we will inform Healthwatch England of the data breach.
- Tell any individuals concerned if the breach is likely to result in a 'high' risk to their rights and freedoms without any undue delay.
- Undertake an exercise to ensure that we learn from the data breach to prevent the recurrence of this problem.
- Keep a record of all data breaches and our actions to deal with them.

If someone requests access to data or objects to us processing the data that we hold about them

If someone makes a subject access request for details of the information that we hold about them, we will:

- If they are unknown to us, ask for reasonable proof of their identity.
- Once we have this, we will make all reasonable efforts to provide, in a secure permanent or electronic format, all data that we hold on them within a month of the request.
- Tell them about their rights about their data under Article 15 of the UK GDPR:
    - the purpose of processing their data.
    - The types of personal data concerned.
    - To whom we will disclose their data.
    - How long we'll keep their data for.
    - Their right to ask us to correct their data or stop processing it.
    - Their right to complain to the Information Commissioner's Office.
    - Whether any data is processed in countries outside the UK (for example, where you are using an online survey tool whose servers are based in another country).
- Not charge a fee for providing the information.

- Deal promptly and fairly with requests for inaccurate personal data to be corrected or deleted If someone asks us to correct or delete data that we hold about them, we will act on their request where:
- Processing is based on consent, and that consent is withdrawn.
- Processing is based on our legitimate interests.
- The personal data is no longer required
- The personal data has been unlawfully processed.
- Where there are no overriding reasons to continue processing the data.

The organisational policies that we have in place to ensure that we comply with data protection law

Adapt North East and Healthwatch Northumberland will maintain sufficient policies to ensure that we can show that we comply with data protection legislation. This includes

- Keeping and maintaining a register of all our data and where it is held (an information asset register).
- A register/record of any data subject access requests made.
- A log of any data breaches.
- Evidence of consent where required.
- A historical list of privacy policies and permission statements.
- Training records on data protection for each member of staff/volunteer.
- Evidence of secure destruction of documents and devices.

Reviewed September 2025

Next review September 2026