

# Data protection policy

# Introduction

This document sets out the steps Healthwatch Darlington 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.

## Why we collect data

At Healthwatch Darlington 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.
- 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.
- Their ethnic origin.
- Their religion.
- Their sexual orientation.

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**

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

- your contact details, including your name, address, telephone number and personal e-mail address
- personal information included in a CV, any application form, cover letter or interview notes
- references
- information about your right to work in the UK and copies of proof of right to work documentation
- copies of qualification certificates
- copy of driving licence
- other background check documentation
- details of your skills, qualifications, experience and work history with previous employers

- information about your current salary level, including benefits and pension entitlements
- your professional memberships
- information about criminal convictions and offences.

We may also collect equality and diversity information like whether you have a disability for which we need to make reasonable adjustments during the recruitment process and/or information about your racial or ethnic origin, religious or philosophical beliefs and sexual orientation.

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 only retain your personal information for as long as is necessary to fulfil the purposes for which it was collected and processed.

If your application for employment or engagement is unsuccessful, we will generally hold your personal information for six months, after the end of the relevant recruitment exercise, but this is subject to any minimum statutory or other legal, tax, health and safety, reporting or accounting requirements for particular data or records,

If you have consented to us keeping your personal information on file in case there are future suitable employment opportunities, we will hold your personal information for a further six months after the end of the relevant recruitment exercise, or until you withdraw your consent if earlier.

Personal information which is no longer to be retained will be securely and effectively destroyed or permanently erased from our IT systems and we will also require third parties to destroy or erase such personal information where applicable.

## **Other purposes including e-newsletter mailing list, being a case study or for publicity photos**

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

When people sign up for our e-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 emailing us or using the e-newsletter link.

We collect:

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

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 Darlington 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 must 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. Wherever possible, we shall fully or partly anonymise any personal information.

## How we keep people's data safe

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

We use the following systems to store data:

- Healthwatch Darlington Microsoft 365 Sharepoint which our staff use as a secure online place to store, organise, share and access information.
- Smartsurvey which we use to store feedback, advice, information, and signposting. We also use it to store and analyse data from research or engagement projects.
- Mailchimp is the system we use to send our e-newsletter.
- Secure hard copy storage in the office for hard copy employment and volunteering applications and other correspondence.
- We implement appropriate security, including technical and organisational procedures against unauthorised or unlawful processing of personal data and to prevent its accidental loss, damage or destruction.
- We ensure that personal data, both electronic and manual, is stored securely and for no longer than necessary within the relevant departments and disposed of appropriately.
- Employees must discuss the method of disposal with our Board of Directors before any action is taken. See Policy 024 Archiving
- Access to information is restricted to those who are required, as part of their work, to see that information. Disclosures will be made only where a legal or justifiable need can be proven.
- Sensitive personal data is treated with additional care in its storage, use and disclosure.
- No confidential information is stored on any laptop that is used outside of the offices of Healthwatch Darlington.

- Laptops should not be removed from the office for any purpose without the prior consent of the Board of Directors.

## 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 via Smartsurvey.

### 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 have no data sharing agreements with any organisations at the moment.

## 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 or object to us processing their data

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**

We 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.




# healthwatch

Healthwatch Darlington  
Morton Park Business Training Centre  
Morton Park  
Yarm Road  
Darlington  
DL1 4PJ

[www.healthwatchdarlington.co.uk](http://www.healthwatchdarlington.co.uk)

t: 01325 380145

e: [info@healthwatchdarlington.co.uk](mailto:info@healthwatchdarlington.co.uk)

 [@healthwatchdton](https://twitter.com/healthwatchdton)

 [@healthwatchdarlington](https://www.facebook.com/healthwatchdarlington) [@youthwatchdarlo](https://www.facebook.com/youthwatchdarlo)