2. Data Protection Policy

Introduction

This document sets out the steps Healthwatch Worcestershire 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 Worcestershire, 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 ask for the following information:

Application form or CV including contact details

We also collect equality and diversity information such as people's age, gender, ethnicity and disability. 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:

Name, contact details, date of birth, bank account details, DBS checks, learning records.

Other purposes including 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 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 either by clicking on the unsubscribe box on the Mailchimp correspondence or by contacting the office either

- by email at info@healthwatchworcestershire.co.uk,

- or by writing to Healthwatch Worcestershire, Civic Centre, Queen Elizabeth Drive, Pershore. WR10 1PT.
- or by telephoning 01386 -550264

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 Worcestershire, 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. Retention & Disposal Policy

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. Healthwatch Worcestershire takes cyber security seriously and has achieved the Cyber Essentials accreditation, and is registered in the national database which can be found here.

We use the following systems to store data:

- Day to day work is carried out using **Microsoft 365**. All data is encrypted and strict access policies are applied with passwords conforming to NCC guidance. This includes The HWW CRM which is used to record details of patient experiences and signposting anonymously. All services are cloudbased. Firewalls, antiviral and anti malware software plus automatic patching are installed, enabled and updated regularly.
- **Survey Monkey**: Research and engagement projects are carried out using Survey Monkey. Surveys are collected anonymously.

  All Survey Monkey's content is encrypted at rest as per industry standards. Data that is passed between users via their web browser and the Smart Survey systems are fully encrypted over HTTPS connections via the latest TLS security.

  Data submitted to Survey Monkey will be downloaded on a regular basis. Data will only be used for the aggregate analysis of trends unless you expressly consent to us sharing your data with partner organisations. All data submitted to Survey Monkey will be permanently deleted no longer than five years after receipt.

- We use **'Mailchimp'** to carry out email marketing this includes registering to receive our newsletter and those who belong to our Reference and Engagement Group. Your data may be transferred

to Data Centres located in the USA. To comply with GDPR regulations Mailchimp incorporates the EU's Standard Contractual Clauses in their Data Processing Addendum which automatically forms part of their Standard Terms of Use and applies to customer data protected by EU laws.

Mailchimp handles the data purely to provide this service on our behalf. Mailchimp follows the requirements of data protection legislation in obtaining, handling, and processing your information and will not make your data available to anyone other than Healthwatch Worcestershire.

Payroll processing is subcontracted to Wychavon District Council with whom HWW has a 3rd Party Data Processor agreement to ensure that the Data Processor complies with the applicable data protection and privacy legislation (the "Applicable Law"), including in particular The Data Protection Act 2018 implementing the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) and all other subsequent regulations.

Personal data shall not be transferred out of the EEA unless the organisation storing the data is subject to an adequacy arrangement supported by the information Commissioners Office.

Only business provided computers may be used for the business of Healthwatch Worcestershire. Only devices owned by HWW are used to connect to company networks or systems.

Access to personal data shall only be granted to staff and contractors who require such access to fulfil their role or a necessary business function. A system of user accounts and passwords is employed to limit access to data to those who require it to carry out their business role.

HWW are aware that mobile working and remote access extends the transit and storage of information outside the HWW infrastructure – typically over the internet. We have clear policies and procedures laid out in our Home Working Guidelines including when accessing the internet only secured wifi routers should be used. Public access networks should never be used to access HWW data/systems. Although encrypted data kept on mobile devices should be limited as far as possible. Further details are available in our Home working guidlelines.8ITHomeworkingAddendum

All data is disposed of in accordance with the Retention & Disposal Policy. A deletion/disposal log is maintained.

Paper documents are shredded and then disposed through the Wychavon District Council Confidential Waste process.

Digital Records are deleted and removed from the recycling bin after 30days.

Devices for disposal are returned to factory settings and then disposed via an official organisation and a certificate of disposal obtained.

When employees/volunteers leave HWW's employment accounts are disabled on the day they leave and are then deleted after 30days.

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 on a Quarterly basis. The data is anonymised.

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 a data sharing agreements in place with Wychavon District Council who process payroll on our behalf and with whom HWW has a 3rd Party Data Processor agreement to ensure that the Data Processor complies with the applicable data protection and privacy legislation (the "Applicable Law"), including in particular The Data Protection Act 2018 implementing the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) and all other subsequent regulations.

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.
- 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.
- We will inform Healthwatch England of the data breach if considered appropriate.

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.

Document Details & Version Control

Version	Comments /Reason for Amendments	Lead Director	Author / Editor	Date	Review by
1	Approved	JR	LH	11/19	11/21
1.1	Amendments drafted	JR	LH	11/21	
2.0	Approved	JR	LH	11/21	11/23
2.1	Amendments drafted	JR	JR	8/23	
2.2	Further amendments drafted	JR	JR	11/23	
2.3	Further amendments to incorporate HWE guidance	JR	PH	2/24	
2.4	Add version control info and other minor formatting amends	JR	PH	15/05/24	
2.5	Amendment clause re data breach reporting to HWE (page 8)	DB	PH	17/06/24	
3.0	Approved at CBM	DB	PH	20/06/24	06/25