healthwatch Shropshire

Information Governance Policy

Reviewed: May 2018

Next Review: June 2019

Contents

1. Data Protection Principles

Healthwatch Shropshire (HWS) individuals (employees, board members, volunteers, temporary staff, people on placements and contractors) accept their responsibilities to comply with the Data Protection Principles outlined in the Data Protection Act 1998 and the principles set out in the General Data Protection Regulation 2018 (GDPR). Henceforth 'HWS individuals' will be used to refer to the above list of people.

This policy also applies to contractors working for Healthwatch Shropshire. In this case Healthwatch Shropshire will be the Data Controller and the contractor will be the Data Processor.

Personal data is information relating to a living individual who can be identified either from that information on its own or from that and other information available to the Data Controller.

The principles are that data, either manual or computerised, which identifies an individual living person must be:

- processed lawfully, fairly and in a transparent manner
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- accurate and kept up to date
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- only be processed in accordance with the rights of data subjects under the Act
- processed in a manner that ensures appropriate security of the personal data
- not be transferred outside the European Economic Area (with some exceptions)

HWS is registered on the Information Commissioners Officer (ICO) Register of Data Controllers. The Chief Officer and Information Officer will oversee compliance with current data protection regulations. All HWS individuals who process this data will be made aware of and comply with this Data Protection Policy.

HWS can be subject to penalties including fines of up to £17,000,000 and individuals can face sanctions including prosecution, for breaches of the Data Protection Act.

2. Data Protection Impact Assessments

A data protection impact assessment (DPIA) is a process to help identify and minimise the data protection risks of a project. A DPIA is required by the GDPR for certain listed types of processing, or any other processing that is likely to result in a high risk to individuals' interests. HWS will carry out DPIA's as required for new projects.

3. Fair Processing

Data subjects refers to any people whose personal data is stored by HWS. Personal data is stored subject to HWS's Records Retention and Disposal Policy.

HWS will ensure that the data subject will:

- not be deceived or misled
- know the purpose for which the data is intended
- know when HWS is the Data Controller
- know the identity of the Data Controller when HWS is the Data Processor
- know when the data is likely to be passed to a third party.

4. Information Asset Register

The Information Asset Register details all of the information we process that contains personal information. It is published on our website.

5. Conditions for Processing Any Personal Data

Processing of personal data is legitimate (Article 6, GDPR) if at least one of the following conditions applies:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

All personal information should be kept securely and should only be shared with and available to those who have a legitimate interest in knowing it and cannot by accident or design be accessed by others.

If consent is the legal basis for processing personal data informed consent must first be gained from the individual, or where appropriate, their legal guardian or person with power of attorney. Children 13 years old and over can give consent for processing personal information if they have a clear understanding of what will happen to their personal data and what rights they have.

Consent must be:

- Freely given
- Specific
- Informed
- Unambiguous
- A positive opt-in and will not be inferred from silence, pre-ticked boxes or inactivity
- Separate from other terms and conditions
- Accompanied with simple ways for people to withdraw consent
- Verifiable

Consent Clauses - Marketing and Electronic Commerce

Data Protection Disclaimers

The following statements should appear on all marketing and electronic commerce documents (whether hard copy or electronic) with the appropriate wording being substituted for italics:

> "Data Protection
>
> Healthwatch Shropshire will use the information you provide on your [*booking form, order form, etc*] and additional information you may provide in the future, for [*insert purpose*]. We will not disclose this information to any other person or organisation except in connection with the above purpose."

The following opt in clause should also appear on the form/document:

> "If you would like to receive information about other Healthwatch Shropshire events, publications or services that we think may be of interest to you, please tick this box [ ]."

Consent Clauses - Photos or recordings at events

When wanting to take photos, video or audio recordings at events, ensure you obtain written consent from anybody included using the HWS Photo & Recordings Consent Form (Appendix 4). Also ensure that nobody else is included from whom consent has not been sought e.g. other people in the background of a photo.

6. Conditions for Processing Sensitive Personal Data

Sensitive personal data is defined as information held about an individual which contains both personal and sensitive information. There are seven types of information detailed in the GDPR that are classified as sensitive. There are:

- Racial or ethnic origin
- Political opinions or beliefs
- Religious or philosophical beliefs

- Membership of a trade union
- Genetic or biometric data
- Health data
- Sexuality
- Criminal proceedings or convictions

The conditions under which HWS processes sensitive personal data are set out in the Information Asset Register. [LINK]

In order to share sensitive data explicit consent must be obtained from the individual, or where appropriate, their legal guardian. This means that the individual has been provided with detailed information to enable them to give an unambiguous expression of agreement. A signed consent form should evidence this.

7. Rights of the Data Subject

HWS has a duty to ensure that data subjects are aware of the information that is being collected and recorded about them and the reasons for doing so, including statistical/analytical purposes.

The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

HWS has a duty to ensure that individuals understand how to exercise their rights.

8. Exercising individual rights

If an individual would like to exercise a right under the GDPR they can do so by contacting the HWS Information Officer. All requests must be made in writing. By law a copy of the information must be provided within one month of receipt of the request unless the request is deemed manifestly unfounded or excessive with such cases being considered by the Chief Officer. If a request is refused, we will tell the applicant why and that they have the right to complain to the supervisory authority and to a judicial remedy. We will do this without undue delay and at the latest, within one month. To assist the process of exercising Data Subject rights a Personal Information access form is attached (Appendix 1).

All requests for access to personal data should be passed to the Information Officer. When an individual makes a request, HWS will tell them whether personal data about

them is being processed by, or on behalf of, HWS. If it is, HWS will give the Data Subject a description of:

- the personal data of which that individual is the Data Subject
- the purposes for which the data is being or is to be processed, and
- the recipients or classes of recipients to whom it is or may be disclosed.

HWS will also inform the Data Subject about:

- the content of the personal data, and
- any information available to HWS as to the source of the data.

When a Data Subject makes a request HWS will ask for reasonable information in order to check the identity of the person making the request and locate the information the person seeks.

If HWS cannot comply with the request without disclosing information relating to another individual who can be identified from that information, it will not comply unless:

- the other individual has consented to the disclosure, or
- it is reasonable in all the circumstances to comply with the request without consent.

9. Information Sharing Protocol

All partnership work with statutory authorities that involves access to personal or sensitive data should be covered by an appropriate Information sharing protocol and relevant information sharing arrangements. These should be an integral part of any funding/contractual process. This should provide an 'overarching framework' that enables HWS with its statutory partner organisations to use well established, comprehensive, transparent, and where appropriate, consensual information sharing systems and processes that place the individual at the centre of how their information is processed in the line with their data subject rights.

The Information Sharing Protocol will include detail as to when it may be necessary to share information with statutory partners without the client's agreement, for example where the "client" is at risk of harm or of harming someone else.

The following general values will be applicable to information sharing:

- Every proposal to share client identifiable information between partner organisations must have a defined and justifiable purpose.
- Any shared client identifiable information must be accurate and objective and minimum information required for the stated purpose.
- Access to client identifiable information will be restricted to a 'need to know' basis.

- Those accessing client identifiable information will be made aware of their responsibilities in relation to its handling.
- The procedures and systems for the sharing of data will be subject to an on-going review.

Telephone calls

When contacting an individual by telephone it is important to verify you are speaking to the individual, or, where applicable, their responsible guardian or person holding power of attorney. Personal data should not be given out to other members of the household.

If someone other than the individual answers the phone:

- State your name and that you are calling from HWS,
- Do not leave a message which could reveal any confidential information,
- Offer to ring back at a more convenient time.

E-Mails

E-mail accounts will be set up with a disclaimer clause to be inserted at the end of all outgoing e-mails stating that the information transmitted is confidential and intended for the recipient only. If the person receiving the e-mail is not the intended recipient it will ask them not to use, review, distribute, disclose, alter, print, copy, transmit or rely on the e-mail and any file transmitted with it.

Personal data should not be sent by email to non-HWS email accounts unless essential because this is not a guaranteed secure method of transfer of information.

Where there is a need to use email:

- Only the minimum necessary information should be sent
- Information should only be sent to recipients who have a “need to know”; checks should be made that information is being sent to the correct person.
- Ensure that any word documents are saved in pdf format to prevent alteration.

Letters

When sending a letter containing personal data, HWS will write Addressee Only on the envelope.

Faxing

Fax machines should only be used to transfer personal data when absolutely necessary. Ensure that it is checked by phone before sending that the correct fax number is used and that the recipient is aware a fax will be arriving. The fax cover sheet should be used (Appendix 2) which states that the fax is confidential and for the attention of the named recipient only. Ask the recipient to acknowledge and confirm receipt of all pages detailed on the cover sheet.

When giving out HWS's fax number, request that a sender contacts HWS prior to sending any personal data. This is in order that an HWS individual can wait by the machine for receipt because the fax machine is in an open area of the building which is accessible by non-HWS people. When receiving notification of a forthcoming fax containing personal data, check the sender has the correct fax number. Upon receipt of the fax, phone the sender to confirm safe receipt.

10. Disclosing Data for other reasons

In certain circumstances, the Data Protection Act (1998) and the GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, HWS will seek and act on advice from the DPO (or Chief Officer if DPO no longer a requirement).

11. Corporate Data

Corporate data is any data which relates to the business of Healthwatch Shropshire e.g. accounts, reports, Enter & View notes. Although this data is not about individuals it may be classed as commercially confidential. They may also be regarded as generally sensitive due to the content. Although not covered by the Data Protection Act, HWS individuals should take similar actions to protect corporate data where necessary.

12. Information Security

HWS has policies and procedure in place to ensure that information is managed securely and uses the following framework and supporting controls to secure day to day handling of information.

On HWS premises:

- Physical and environmental security to ensure unauthorised access, damage and interference to the business premises and information.
- Access control via computer passwords, secure door entry, visitor passes to control access to information.
- Asset classification and control to identify assets and appropriately protect them.
- Business continuity management to counteract interruptions to service activities and to protect critical service processes from the effects of major failures or disasters.

Away from HWS premises:

- HWS recognises that not all of the above precautions will be possible when working away from HWS premises. However, HWS individuals are expected to take all reasonable precautions regarding physical and electronic security of

information e.g. not leaving documents unattended where others may be able to access them, password protection of electronic information.

- Personal data should not be held on non-encrypted memory sticks. Particular care should be taken when using a laptop or other electronic device away from HWS premises which contains personal data.

Details of security arrangements for individual information assets are set out in the Information Asset Register [LINK]

Scanning

When scanning a document containing personal data for internal HWS use, the RCC scanner should be used by logging in with an ID badge. Once sent, the scan must immediately be 'cut' from open folder 'scans' in CCS2003 and 'pasted' into HWS's secure storage area.

Documents containing personal data should not be scanned and emailed to non-HWS email accounts unless essential because this is not a guaranteed secure method of transfer of information.

IT and printing

PCs or laptops not in use should be switched off or locked. Information should be stored on the HWS server, not on local hard drives.

Personal data should not be transferred onto personal mobile devices or personal laptops. Particular care should be taken when using social media not to disclose any personal data.

Care should be taken when printing information. Special care is needed in relation to the shared printer to ensure all documents printed have been collected and that printing is not left unattended.

13. Disposal of personal information

Personal Information is held in accordance with the retention schedule outlined in the Information Asset Register.

When disposing of printed or handwritten documents containing personal data, HWS individuals will use a cross cut shredder. Electronic data will be completely erased. When disposing of electronic devices, e.g. PCs or laptops, HWS will take particular care to ensure all data is removed from drives and storage.

14. Making the Data Protection Policy known

All HWS individuals will be given a copy of the policy when they join Healthwatch Shropshire. As part of their induction all HWS individuals will be trained on the Data Protection Policy and its application to their work. All HWS individuals will be required to sign a declaration (Appendix 3) that they have read and will comply with this policy.

Healthwatch Shropshire will ensure that existing individuals understand its application through regular updates and training.

As part of staff training, they will also review the Information Asset Register to ensure:

- All listed items are relevant
- There are no omissions
- All information is correct
- The retention is fully adhered to
- Consent is being correctly and fully obtained

The following simplified statement will be used for consumers

"Healthwatch Shropshire works to strict Data Protection and Confidentiality policies in accordance with the Data Protection Act 1998 and the General Data Protection Regulation 2018. All personal information shared with us stays within Healthwatch Shropshire, unless we have specific consent to share it or unless somebody would be put at serious risk by us withholding the information."

Privacy statement

We have a privacy statement that complies with GDPR and can be found on our website, where it must be published.

15. Data Protection Officer

As a public authority Healthwatch Shropshire is required to have a Data Protection Officer (DPO).

The DPO will:

Provide advice to the organisation on compliance obligations and when a data protection impact assessment is required

- Monitor compliance with the GDPR and organisational policies
- Co-operate and liaise with the Information Commissioner
- Take into account information risk when performing the above
- Report directly to the highest management level of the organisation
- Be involved in all data protection issues
- Be supported by the necessary resources and able to maintain expertise
- Not be pressurised by the organisation as to how to perform his or her tasks, and is protected from disciplinary action when carrying out those tasks
- Have no conflict of interest where they perform other roles

Contact details of the DPO will be published on the HWS website.

As of 25 May 2018, the DPO is Mark Guest, who is an employee of Healthwatch Sandwell. This role is provided to Healthwatch Shropshire under reciprocal arrangements.

16. Notification of Breaches

If HWS individuals suspect there has been, or there is the potential for, a data breach they are required to inform the Information Officer, Chief Officer and Chair of the Board immediately. They will assess the issue and in accordance with the regulations set out in the GDPR they will notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, HWS will also notify those concerned directly.

17. Application and review

This policy applies to all paid staff, volunteers, Board Members, temporary staff and people on placements at Healthwatch Shropshire. The policy will be reviewed annually.

This policy should be read in conjunction with the following related policies:

- ICT & Social Media Policy
- Child Protection and Adult Safeguarding policy
- Confidentiality Policy
- Records Retention Policy
- Privacy Statement

Appendix 1

Personal Information Access Request Form

Healthwatch Shropshire

Application for Access to Personal Information under the General Data Protection Regulation 2018

- All applicants must complete Sections 1, 2 and 5
- If you are applying on behalf of someone else, then they must complete Section 4 and you will also need to complete Section 3.

Section 1.

Name of Applicant ……

Address of Applicant……

……

……

Previous address if moved in the last three years

……

……

Date of birth……

Telephone Number(s)……

Section 2.

To help us locate any personal information which we may hold can you please supply:

A description of the service you received from HWS

……

……

……

……

……

……

When you used our service? ……

Any other information which you think might help us locate your personal Information:

……

……

……

……

Section 3.

Please complete this section if you are authorised to act on behalf of the applicant:

I have been authorised to act on behalf of (name of person which received the service)……

I declare that I will not disclose any information that I am supplied with other than to the person on whose behalf I am acting, unless they give me their permission.

Name: ……

Signed ……Date……

Section 4.

If an agent is acting on your behalf, then please complete the following:

I,…… (Name of user of services)

Authorise …… (Name of person or agent acting on your behalf)

to seek access to personal information held by Healthwatch Shropshire.

I declare that this authorisation was freely given.

Signed……Date……

(User of Service)

Section 5.

All applicants must sign and date the following:

I wish to request access to personal information held by Healthwatch Shropshire on (name) …….

In accordance with the General Date Protection regulation 2018 I understand that to ensure confidentiality it may be necessary for Healthwatch Shropshire to obtain further information to confirm my identity and to locate the information sought.

I would like the reply to this request to be (Tick as appropriate)

Sent to my home address (as above) ☐

Collected from your offices (you must bring evidence to confirm your identity) ☐

Signed……

Date……

Please return this form to:

Private & Confidential

Information Officer

Healthwatch Shropshire

4 The Creative Quarter

Shrewsbury Business Park

Shrewsbury

SY2 6LG

When disclosing the information we will require proof of identify by production of a passport or photo card driving license.

Appendix 2

FAX COVER SHEET

From (Name):

Telephone Number:

Date:

Time:

Fax Number:

To:

Organisation:

Telephone:

Fax Number:

Total Number of Pages (Including this sheet):

IMPORTANT MESSAGE:

This fax is confidential and may also be privileged. If you are not the intended recipient, please notify us immediately. You should not disclose the contents to any other person, nor should you copy it without appropriate authority.

Appendix 3

DATA PROTECTION DECLARATION

Name:

Position:

I have read the Data Protection Policy of Healthwatch Shropshire, which has been discussed with me by the staff member(s) responsible for overseeing my role. I understand that I must comply with the directions of the policy both during my time as a HWS individual and after I cease to be a HWS individual, unless failure to do so would be likely to result in serious risks to other people or organisations.

Signed:

Date:

Appendix 4

Consent form for the use of your image

About us
There is a local Healthwatch in every area of England. We are the independent champion for people using local health and social care services. We listen to what people like about services and what could be improved. We share their views with those with the power to make change happen.

We also share them with Healthwatch England, the national body, to help improve the quality of services across the country. People can also speak to us to find information about health and social care services available locally. Our sole purpose is to help make care better for people.

Through our work we will collect and share peoples' experiences as a way of driving change and improvement. These experiences could be shared in different ways including photographs, film footage, presentations and case studies.

Giving consent to use your image
This form asks you to consent to the use of your image by Healthwatch Shropshire.

Your image shall be deemed to represent a fictional person unless agreed otherwise.

Your image may be used in our 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.

We will not include your personal details (such as postal addresses, or telephone numbers) on our website, printed materials or other promotional materials. Please note that that our website and social media channels can be accessed from outside the United Kingdom.

We will only use images that identify you with your further, explicit consent to do so, and we will not use the images for any purpose other than those mentioned above or as otherwise agreed.

***This form can only be signed by persons aged 18 years and over. If you are under 18 years of age, this form should be completed on your behalf by a parent or guardian.**

You may withdraw your consent at any time by contacting us at the address below.

If you withdraw your consent, Healthwatch Shropshire will not use your image in any new publications or materials and will delete your image from our records.

However, your image may be retained on existing publications and materials where a) there is a legitimate interest for Healthwatch Shropshire to maintain the public availability of those publications and materials, b) this legitimate interest is not

overridden by any prejudice (damage or harm) to your own interests or fundamental rights or freedoms, and c) where it is not reasonable and proportionate in the circumstances for the publications or materials to be withdrawn.

You may request the withdrawal of any publication or material containing your image, for reasons of prejudice to your own interests, fundamental rights or freedoms, by contacting us at the address below. Any such request will be considered by Healthwatch Shropshire and you will be informed of the outcome.

Healthwatch Shropshire will retain and use images for five years, after which they will be deleted and no longer used. However, if used, your image may remain in publication for longer than five years. You can request a copy of your personal data held by Healthwatch Shropshire by contacting us at the address below.

Please answer the questions below, then sign and date the form as indicated:

I give consent to be photographed to provide my image to Healthwatch Shropshire. The purpose for which the photograph/s may be used has been explained to me. I understand that the photographs remain the property of Healthwatch Shropshire.

I grant Healthwatch Shropshire the absolute right to use my image and any other reproductions or adaptation as indicated below:

☐ I consent for my image to be used to represent a fictional person

☐ I consent for my image to be used for the following purpose(s):
In Healthwatch Shropshire and Healthwatch England publications, on our website, in advertising and with the media

☐ I consent for my image to be used by Healthwatch Shropshire

☐ I consent for my image to be kept by Healthwatch Shropshire for five years

☐ I am over 18 years of age*

Name .....

Place .....

Contact number .....

Signature:

Date:

For further information or clarification

Please send this consent form to enquiries@healthwatchshropshire.co.uk or 4, The Creative Quarter, Shrewsbury Business Park, Shrewsbury, Shropshire. SY2 6LG. If you have any questions at all please call 01743 237884.

Healthwatch Shropshire is the data controller for personal data held by Healthwatch Shropshire. The Data Protection Officer can be contacted using the details above, for any complaints or concerns about the processing of your personal data.

You also have the right to lodge any complaint about the processing of your personal data with the Information Commissioner's Office (ICO).

THANK YOU