Data Protection Policy

Version	Date	Changes	Prepared by	Approved by
1	13th June 2016		KS	June 2016 Board
2	14th Sept 2016	Minor change to p15	KS	Sept 2016 Board
3	25th July 2017	Updated in light of LHM contract	KS	July 2017 Board
4	19th October 2018	Full review in light of GDPR and new UK legislation	Helen Anjomshoaa (DPO)	
5	23.09.19	Annual review	LS	October 2019 FPC & Board
6	28.09.20	Annual review – inclusion of guidance on storage and destruction of sensitive material when working remotely	LS	October 2020 FPC & Board

Review date: Oct 2021

Contents

1. Introduction

Healthwatch Surrey is an independent consumer champion created under the Health and Social Care Act 2012 that gives the people of Surrey a voice to improve, shape and get the best from health and social care services in Surrey by empowering local people and communities. It is a Community Interest Company (CIC) limited by Guarantee (Registered Company No.8737632) i.e. a company that acts for the benefit of the community.

In order to meet its legal and operational obligations, Healthwatch Surrey must collect and process some personal information about individuals who have accessed health or social care services. In doing so, Healthwatch Surrey provides clear information to those individuals about the ways in which their personal information will be stored and used at the time of collecting the information. The Healthwatch Surrey Privacy Notice is also available on the organisation's website.

Furthermore, as the Data Controller for this information, Healthwatch Surrey is strongly committed to data security, all internal processes are reviewed with this in mind and all the information that is collected is held in accordance with current data protection legislation.

This Data Protection Policy applies to all Healthwatch Surrey Directors, staff and volunteers and describes the steps that Healthwatch Surrey takes to protect this information from unauthorized access, loss, misuse, alteration or corruption.

Healthwatch Surrey has sub-contracted the provision of some of the Local Healthwatch services to other service providers. These service delivery partners are Data Processors for Healthwatch Surrey and their work is governed by Data Processing Agreements consistent with the ICO's Code of Practice on Data Sharing.

2. Purpose

The purpose of this policy is to ensure that Healthwatch Surrey will:

- comply with the current data protection legislation
- follow good practice
- protect the rights of staff, customers and service delivery partners
- be open about how it stores and processes individuals' information
- protect itself from the risks of a data breach

This policy also serves to protect Healthwatch Surrey from data security risks, for example breaches of confidentiality; regulatory action, fines and/or reputational damage.

3. Data protection legislation

Healthwatch Surrey adheres to the following principles in its approach to the collection, use, retention, transfer, disclosure and destruction of personal data:

- **Principle 1: Lawfulness, Fairness and Transparency.** Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the

data subject.

- **Principle 2: Purpose Limitation.** Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

- **Principle 3: Data Minimisation.** Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- **Principle 4: Accuracy.** Personal data shall be accurate and, kept up to date.

- **Principle 5: Storage Limitation.** Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

- **Principle 6: Integrity & Confidentiality.** Personal data shall be processed in a manner that ensures it is kept appropriately secure, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

- **Principle 7: Accountability.** Healthwatch Surrey will demonstrate that the above principles are met for the data it is responsible for.

4. Personal information processed by Healthwatch Surrey

Some examples of the types of personal information that may be processed by Healthwatch Surrey (depending on the reason why an individual comes into contact with the organisation) include:

- Experiences of individuals who have accessed health and social care services;
- Views and opinions of individuals about health and social care services;
- Contact details;
- Information relating to an individual's employment;

Some of this will be classed as Special Category Data and must be stored and processed with the utmost care. Such data includes:

- Race
- Ethnic origin
- Politics
- Religion
- Trade union membership
- Genetics
- Biometrics (where used for ID purposes)
- Health
- Sex life or
- Sexual orientation

Healthwatch Surrey uses the following legal bases for processing personal information.

Type of information	Legal basis for processing your information
Public feedback on health and care services	**Public Task** (Article 6(1)e of the GDPR) with the associated condition of **public interest in the area of public health** for processing special category data (Article 9(2)i of the GDPR)
E-bulletin mailing list	**Consent** (Article 6(1)a of the GDPR) with the associated condition of **consent** for processing special category data (Article 9(2)a of the GDPR)
Directors, staff and volunteers (current and prospective)	**Legitimate interests** (Article 6(1)f of the GDPR) with the associated condition of **consent** for processing special category data (Article 9(2)a of the GDPR)

Where personal information is processed on the basis of consent, the individual may subsequently opt-out of the processing by contacting Healthwatch Surrey.

Where Healthwatch Surrey would like to use personal information for purposes that go beyond the scope of the original legal basis set out above, Healthwatch Surrey will either make contact with the individual to obtain the necessary permission or the information will be sufficiently anonymised or pseudonymised to ensure that the individual cannot be identified.

5. Responsibilities

Everyone who works at Healthwatch Surrey has some responsibility for ensuring that data is collected, stored and handled appropriately. Anyone who handles personal data on behalf of Healthwatch Surrey must ensure that they do so in line with this policy and the stated data protection principles.

The following individuals have key areas of responsibility:

- **Healthwatch Surrey CIC Directors** - the Board of Directors is ultimately responsible for ensuring that Healthwatch Surrey meets its legal obligations.

  The particular Director responsible for the oversight of this policy is the Chair/Deputy Chair. Operational responsibility for ensuring this policy is put into practice is delegated to the Chief Executive Officer (see below).

- **Chief Executive Officer (CEO)** – the CEO has responsibility for all matters pertaining to data protection. As such, he/she will:
  - Brief the Board on its data protection responsibilities,
  - Ensure all Directors, staff and volunteers receive data protection training prior to being given access to any personal data, as well as refresher training as appropriate,
  - Maintain this policy,
  - Ensure that Healthwatch Surrey's service delivery partners are adhering to data protection requirements, as set out in the SLAs with each service delivery partner, and that they are providing initial and ongoing training on data protection to all staff undertaking work on behalf of Healthwatch Surrey,
  - Check data protection compliance within individual projects before these are initiated and when they are reviewed,
  - Handle subject access requests; requests to prevent further use of an individual's personal data; and requests for any inaccurate personal data

held by Healthwatch Surrey to be rectified, blocked, erased or destroyed,
- Ensure that the processes in place relating to the security of the electronic information are consistent with this policy,
- Handle demands for disclosure of personal data to outside agencies (e.g. the Police),
- Monitor whether registration with the Information Commissioner's Office is required.

- **All Healthwatch Surrey directors, staff and volunteers** – each individual working or volunteering for Healthwatch Surrey must undertake the necessary data protection training, including refresher training, and comply with this policy at all times. Any failure to do so will be subject to disciplinary proceedings.

  Any questions or concerns about the interpretation or operation of this policy should be raised with a manager or the CEO.

- **Data Protection Officer (DPO)** – Healthwatch Surrey has appointed a DPO who reports to the Chief Executive Officer. The DPO's duties include:
  - Informing and advising Healthwatch Surrey about its obligations to comply with data protection legislation,
  - Monitoring compliance with data protection legislation and this policy through conducting internal audits,
  - Advising on undertaking Data Protection Impact Assessments where required,
  - Advising on data protection questions from Directors, staff or volunteers in regard to their work for Healthwatch Surrey,
  - Advising on any contracts or agreements with third parties that may handle the organisation's sensitive data,
  - Acting as a point of contact for Data Protection Authorities.

6. Guidelines on data security, recording and storage

In order to ensure that personal information is kept securely, precautions must be taken against the physical loss of, or damage to, the data in addition to ensuring access to the data is appropriately restricted.

Therefore, all Directors, staff and volunteers are required to adhere to the following guidelines as a minimum:

General Guidelines:

- Ensure due attention is given to training relating to data protection;
- Ensure personal information in any format is held securely at all times;
- Ensure personal information is not disclosed in any way to an unauthorized third parties;
- Ensure personal information is not shared informally. When access to confidential information is required, it can be requested from a line manager;
- Ensure access to personal information is restricted to only those who need it for their work.;
- Ensure all staff comply with the Healthwatch Surrey Information Technology Security Policy at all times; and
- Ensure guidance is sought from a line manager or the DPO if anyone is

unsure about any aspect of data protection.

Data Storage:

- Ensure all paperwork containing personal information is locked away when not in use and cannot be accessed by unauthorized people, for example left on a printer;
- Ensure paperwork containing personal information is securely shredded when it is no longer required;
- Ensure all electronic data is protected by a strong password that is changed regularly and not shared with anyone;
- Ensure data is only stored on designated drives and approved cloud computing services. It should never be saved directly onto mobile devices,
- Keep all mobile technology used to access Healthwatch Surrey data safe at all times and report any loss or theft of Healthwatch Surrey devices in a timely manner;
- Ensure that no commercial software or any other copyright materials belonging to others is uploaded, downloaded or otherwise transmitted using Healthwatch Surrey IT devices;
- Ensure these guidelines are adhered to when working using remote access as well as when working from the office;
- Return any devices that are no longer used to Healthwatch Surrey,
- Ensure all removable media is virus checked before use and kept locked away when not in use; and
  Ensure that only authorized personal devices are used to access Healthwatch Surrey data and that they are only used in accordance with the Healthwatch Surrey IT Security Policy.
- Ensure that paperwork containing personal information gathered via virtual engagement at home is stored in locked storage and shredded when no longer required.

Data Use:

- Ensure all electronic devices are locked when you are not present, requiring a strong password to unlock them,
- Ensure Egress Switch or similar is used to encrypt emails containing personal information that are being sent outside the Healthwatch Surrey domain,
- Ensure personal information is not transferred outside the European Economic Area,
- Ensure personal information is not disclosed in any way to an unauthorized third parties,
- Ensure data is only stored on designated drives and approved cloud computing services. It should never be saved directly onto mobile devices.

Data accuracy:

- Ensure data is held in as few places as necessary,
- Ensure every opportunity is taken to ensure personal information is correct and updated as required,
- Ensure personal information is archived or securely destroyed or deleted in line with the Healthwatch Surrey Retention Policy.

Failure to observe these guidelines is a serious disciplinary offence and Healthwatch Surrey will take appropriate disciplinary action where necessary. This may result in dismissal for serious infringements.

As an organisation, Healthwatch Surrey ensures the protection of data as follows:

- Access to IT accounts and secure areas is allocated and revoked in a timely manner for Directors, staff and volunteers starting with or leaving the organisation,
- All documents containing confidential personal information are labelled as 'CONFIDENTIAL',
- Secure storage is made available for confidential and personal information, for both office working and working from home
- All appropriate measures will be implemented to ensure the security of ICT
- networks and systems,
- All directors, staff and volunteers receive an induction and appropriate training to enable them to understand their personal responsibilities relating to confidential data when working from home and in outreach locations,
- Support is accessible to all Directors, staff members or volunteers who have queries regarding data protection issues;
- Facilities for the secure destruction of personal information will be made available as required for both office working and working from home

7. Subject Access Requests

A Subject Access Request is a written request made by, or on behalf of, an individual for the information which he/she is entitled to under the current data protection legislation.

Any such requests submitted to Healthwatch Surrey will be forwarded to the CEO for their attention. The CEO will respond to the request within 30 days of receiving it, providing the type of personal data involved is not exempt from the right of subject access.

In the event that more information from the individual is required in order to identify the person making the request, the CEO will wait until that information has been provided before dealing with the request.

Information will be provided in written form unless otherwise agreed with the individual.

No administration fee will be charged for considering and/or complying with such a request (unless the request is deemed to be unnecessary or excessive in nature).

It should be noted that situations may arise where providing the information requested would disclose personal data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

8. Commitment to transparent data handling

Healthwatch Surrey recognizes that people may wish to know that their personal information is being processed, how it might be shared and how they can exercise their rights in relation to the data. This is set out in the Healthwatch Surrey Privacy Notice that is available on the Healthwatch Surrey website or from the person who is recording the experience on behalf of Healthwatch Surrey. Additionally, the Healthwatch Surrey Helpdesk can also provide this information by telephone.

In the event that someone provides personal information on behalf of another individual, for example a family member they care for, the person providing the information to Healthwatch Surrey has the responsibility for ensuring the individual whose information they are providing has agreed to this. If this is not possible, then the information will not be collected.

Healthwatch Surrey only sends out E-bulletins or digital marketing materials to those people who have specifically requested that they be included on our mailing list. In the event that anyone on the mailing list requests that they be removed from it, Healthwatch Surrey will do so with immediate effect. The minimum details necessary will be held on a suppression list with a record of the opt-out decision.

Staff members are informed about the way that their personal information is processed in the Employee Handbook.

Volunteers are informed about the way their personal information is processed in their Volunteer agreement.

9. Exceptional circumstances

Healthwatch Surrey recognizes that exceptional circumstances may arise when staff need to breach confidentiality where there is a threat a person's safety. Some examples include:

- When a member of staff believes that a person could cause danger to themselves or to others;
- When a member of staff suspects abuse or has knowledge of abuse;
- When the person gives information, which indicates that a crime has been committed;
- When disclosure is required by law, for example, by the police;

The decision whether to break confidentiality will be decided on a case by case basis and always in conjunction with the CEO, or the Co-Chair(s)

10. Breach reporting

Anyone who suspects that a personal information breach has occurred must immediately notify the CEO, providing a description of what occurred.

The CEO will investigate all reported incidents to confirm whether or not a breach has occurred. If it is confirmed, the CEO will follow the relevant authorised procedure based on the criticality and quantity of the personal data involved, including reporting the breach to the Information Commissioner's Office if appropriate.

For severe breaches, the Healthwatch Surrey Chair will initiate and chair an emergency response team to coordinate and manage the personal information breach response.