Data Protection Policy

Title	Version	Date	Changes	Authorised
Data Protection policy	1	13th June 2016		June 2016 Board
ditto	2	14th Sept 2016	Minor change to p 15	Sept 2016 Board

Review date Sept 2017

Contents

Data Protection Policy

1. Introduction

Healthwatch Surrey is the independent consumer champion for health and social care in Surrey. It is a Community Interest Company (CIC) limited by Guarantee (Registered Company No.8737632) - that is, a company that acts for the benefit of the community.

Healthwatch Surrey is required to maintain certain personal data[1] about living individuals for the purposes of satisfying its operational and legal obligations. These personal data, whether held on paper, computer or other media, are subject to the legal safeguards specified in the Data Protection Act 1988.

2. Purpose

Healthwatch Surrey recognises the importance of treating all personal data in a correct and lawful manner.

The purpose of this policy is to set out how Healthwatch Surrey will comply with the Data Protection Act 1988 in all its operations and thereby minimise the level of risk relating to the management of personal data within the organisation.

3. Data Protection Act 1988

The Data Protection Act 1988 (DPA) establishes a framework of rights and duties which are designed to safeguard personal data. This framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes against the rights of individuals to have respect for the privacy of their personal details.

Personal data covered by the DPA encompasses all information which is, or is intended to be, processed automatically (generally by a computer) or manually.[1]

The principles of the DPA are set out overleaf.

Further information about the DPA can be found on the website of the Information Commissioner's Office (ICO) at:

https://ico.org.uk/for-organisations/guide-to-data-protection/.

---

[1] **Personal data** are defined by the DPA as meaning any data which relate to a living individual who can be identified either from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller (see Page 4 of this document); and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. It is important to note that, where the ability to identify an individual depends partly on the data held and partly on other information (not necessarily data), the data held will still be "personal data".

Principles of the Data Protection Act 1998

The principles require that personal data shall:

1. Be processed fairly and lawfully and shall not be processed unless certain conditions are met;
2. Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose;
3. Be adequate, relevant and not excessive for those purposes;
4. Be accurate and, where necessary, kept up to date;
5. Not be kept for longer than is necessary for that purpose;
6. Be processed in accordance with the data subject's rights;
7. Be kept secure from unauthorised or unlawful processing and protected against accidental loss, destruction or damage by using the appropriate technical or organisational measures; and
8. Not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

4. Healthwatch Surrey's Business Model and the Data Protection Act

4.1 The Business Model of Healthwatch Surrey

Healthwatch Surrey CIC was set up in 2013 as a joint venture by a new partnership of three well-established not for profit organisations: Surrey Independent Living Council (SILC), Help and Care (H&C) and Citizens Advice in Surrey (CAS).

A 1+1-year contract (also referred to as the Head Contract) to provide the Local Healthwatch service in Surrey for the period April 2013 - March 2015 was awarded jointly by Surrey County Council in 2013. A new three-year contract was awarded in April 2015.

Healthwatch Surrey CIC has sub-contracted some of the provision of the Local Healthwatch service to its service delivery partners: SILC, H&C and five Citizens Advice Bureaux, plus Surrey Disabled People's Partnership for NHS Advocacy, all of whom are registered with the ICO. Their work is managed through service level agreements (SLAs).

Formatted: Indent: Left: 0 cm, Right: 0.31 cm, Space Before: 1.55 pt

In addition, SILC provides administrative support to the Board, as well as finance, human resources and information and communication technologies (ICT) support to the organisation. The provision of this support is also managed through an SLA.

Healthwatch Surrey CIC also uses LHM Media as a supplier of services. LHM Media is registered with the Information Commissioners Office.

Healthwatch Surrey CIC employs a Chief Executive Officer who assists the Board to formulate and regularly review the organisation's mission, strategy, policies and procedures, ensuring they are relevant, meet current standards and are fit for purpose. The Chief Executive Officer also meets with each of our service delivery partners every quarter to monitor the services they provide on behalf of Healthwatch Surrey CIC. The Chief Executive Officer reports regularly to the Board on progress.

4.2 What this means in relation to the Data Protection Act

The Head Contract includes a requirement that both parties to the contract (Surrey County Council as the Lead Purchaser and Healthwatch Surrey as the Provider) observe their obligations under the DPA that arise in connection with the contract.

The Head Contract also specifies that

- Personal data, as defined in the DPA (see Page 2 of this document), supplied by and/or processed on behalf of the Purchaser (electronic and manual) is owned by the Purchaser, which is a Data Controller[2] under the terms of the DPA
- Healthwatch Surrey, as the Provider, is the Data Processor[3] under the terms of the DPA and is required to maintain appropriate confidentiality and security arrangements in respect of all personal data supplied by and/or processed on behalf of the Purchaser and to comply fully with the principles of the DPA when processing that personal data

[2] A **Data Controller** is defined in the DPA as a "person" who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. A data controller must be a "person" recognised in law, that is to say, either an individual, an organisations or other corporate/ unincorporated body of persons. Data controllers will usually be organisations. Even if an individual is given responsibility for data protection in an organisation, they will be acting on behalf of the organisation, which will be the data controller. In relation to data controllers, the term 'jointly' is used where two or more persons (usually organisations) act together to decide the purpose and manner of any data processing. The term 'in common' applies where two or more persons share a pool of personal data that they process independently of each other. Data controllers must ensure that any processing of personal data for which they are responsible complies with the Act. Failure to do so risks enforcement action by the Information Commissioner (who can impose penalties up to £500,000), prosecution, and compensation claims from individuals.

[3] A **Data processor**, in relation to personal data, is defined in the DPA as any person (other than an employee of the data controller) who processes the data on behalf of the data controller. Data processors are not directly subject to the Act. However, most data processors, if not all, will be data controllers in their own right for the processing they do for their own administrative purposes, such as employee administration or sales.

- The Provider must be able to provide evidence that it can comply with this obligation and must notify the Purchaser promptly of any breach of the security measures required to be in place.

As Healthwatch Surrey CIC has sub-contracted some of the provision of the Local Healthwatch service to its service delivery partners, Healthwatch Surrey CIC has delegated the data protection requirements set out in the Head Contract to its service delivery partners. Each of the SLAs with its service delivery partners includes a requirement that the service delivery partner concerned must comply with the requirements relating to Data Protection, as set out in the Head Contract, and also devolves to each service delivery partner the Provider responsibilities as Data Processor (under the terms of the DPA), as set out in the Head Contract.

Healthwatch Surrey CIC is also a Data Controller under the terms of the DPA (jointly with Surrey County Council) and is therefore registering as such with the ICO.

Healthwatch Surrey CIC also has an SLA with SILC for the provision of administrative support to the Board, as well as finance, human resources and ICT support to the CIC. All of these functions also have data protection implications and this SLA therefore also requires that SILC complies with the DPA in relation to these functions.

Personal data held by Healthwatch Surrey (either by the CIC or by one of its service delivery partners) includes information about:

- clients and service users;
- survey participants;
- current, past and prospective employees and volunteers;
- sub-contractors and suppliers; and
- other individuals/organisations with whom it communicates.

5. Satisfying the requirements of the Data Protection Act

In order to meet the requirements of the DPA principles, Healthwatch Surrey (both the CIC and its service delivery partners) will:

1. Observe fully the conditions regarding the fair collection and use of personal data;

2. Meet its obligations to specify the purposes for which personal data are used;

3. Collect and process appropriate personal data only to the extent that it is needed to fulfil operational or any legal requirements;

4. Ensure the quality of personal data used;

5. Apply strict checks to determine the length of time personal data are held - personal data will not be kept for longer than necessary and all personal data will be removed and disposed of after seven years;

6. Ensure that the rights of individuals about whom the personal data are held can be fully exercised under the Act;

7. Take the appropriate technical and organisational security measures to safeguard personal data; and

8. Ensure that personal data are not transferred outside the European Economic Area without suitable safeguards.

6. Acceptable use of personal data, transparency and consent

Personal data will only be sought and recorded if it is necessary for the delivery of the service and/or it is expressly in the interests of the person concerned to do so (for example, to enable better service delivery).

Healthwatch Surrey is committed to making the way it retains any personal data transparent. Individuals about whom personal data are to be recorded will be made aware about what information about them will be retained and that this information will be held securely.

Their consent to record and retain these personal data will be obtained - wherever possible, a signature from the individual concerned (or their parent, guardian or carer, where appropriate) confirming their agreement to the recording and retention of these personal data will be obtained.

The methodology of any new projects which require the collection of personal information (eg surveys, training events, etc) will ensure that data collection forms also contain an appropriate consent statement.

7. Handing personal data

The need to ensure that personal data are kept securely means that precautions must be taken against the physical loss of, or damage to, the data. Measures must also be taken to ensure that both access to, and disclosure of, personal data are restricted.

All directors, staff and volunteers are responsible for ensuring that:

- Any personal data which they hold is kept securely;
- Personal data are not disclosed either orally, in writing or otherwise to any unauthorised third party; and
- All personal data held in electronic form is protected by the use of controlled passwords and other access security provisions, as deemed to be required.

All staff are responsible for ensuring that personal data are not kept for longer than necessary.

7.1 Controlling access to personal data

The 'need to know' principle of minimised access to personal data will be employed across the organisation. This will ensure that all directors, staff and volunteers will only ever have access to the minimum amount of personal data required to enable them to perform their valid business role and for which appropriate consent exists.

This 'need to know' access principle will be implemented

- through the establishment of effective ICT user account management processes;
- by limiting the number and use of privileged accounts; and
- by monitoring the use of ICT systems and limiting access to other physical areas which house personal data.

7.2 Classification of documents containing personal data

In order to enable directors, staff and volunteers to easily identify which documents contain confidential personal data, all documents concerned will be clearly labelled in the header as 'CONFIDENTIAL'.

7.3 Physical security of personal data

All records relating to individuals, including day books, files, correspondence, card indexes with names and addresses and computer data, will be stored securely at all times, particularly when the office is not staffed.

Particular care will be taken in the handling of records when the office is open. Confidential material will not be placed or left where it can be overlooked by members of the public or by staff who are not involved in that particular enquiry or case.

7.4 Security of ICT

All appropriate measures will be implemented to ensure the security of ICT networks and systems used by Healthwatch Surrey.

Only ICT equipment and media authorised by the Manager with responsibility for ICT will be used to handle, transport, store or process personal data. Privately owned ICT equipment will not be used unless approved in advance by the Manager with responsibility for ICT.

All remote computer processing of personal data will be protected with an identification and authentication mechanism (such as user logon and password).

7.5 Home working and mobile working

All directors, staff and volunteers will receive training to enable them to understand their personal responsibilities relating to confidential data when working from home and in outreach locations.

7.6 Use of removable media

Personal data will only be stored on a portable device if this has been authorised by a Line Manager and a secure protocol for data recording has been agreed with the Manager with responsibility for ICT. Where an alternative protocol is agreed, all files to be stored on mobile storage devices must always be password protected.

7.7 Security of personal data while in transit: email, fax, post

All directors, staff and volunteers will be made aware through initial and refresher training that Healthwatch Surrey is legally responsible for the security of personal data sent whilst in transit, including data sent via email, fax and post.

7.8 Secure disposal of personal data

All copies of confidential data will be securely erased or destroyed at the end of their business 'life'. Feedback forms or other paper records of health and social care experiences will be destroyed after one year.

Paper records and confidential material will be shredded or stored in confidential waste sacks, or otherwise physically destroyed, to ensure that no-one can link the name and address of an individual with other specific information held about them.

8. Sharing and divulging personal data

8.1 Sharing personal data within Healthwatch Surrey

Personal data will be treated in confidence and will only be shared with another individual within Healthwatch Surrey on a "need to know" basis. For example, it may be necessary to share personal data with a manager, or with colleagues within the Healthwatch Surrey family, in order to provide the best possible help to the person concerned.

8.2 Sharing and divulging personal data outside Healthwatch Surrey

Personal data will only be passed to another agency/organisation or to other individuals outside the organisation with the consent of the person concerned - where possible this will be with written consent. If a member of staff or volunteer intends to get information from another agency to help the person, or to refer them to another agency, then this must be explained to the person concerned and their permission given.

Personal data about staff, volunteers or people using the service will not be divulged to anyone outside the organisation, including a member of their family, without the consent of the person concerned, unless extenuating circumstances exist (see 7.4 below).

8.3 Assured data sharing

Data sharing agreements consistent with the ICO's Code of Practice on Data Sharing will be put in place where the business need to share confidential personal data with external organisations exists and where consent or other legal authority exists for the data sharing. This will include the sharing of personal data between partner organisations within the Healthwatch Surrey family. All data sharing partner organisations will be required to confirm annually that they are adhering to this agreement.

8.4 Limits to the confidentiality of personal data

In certain circumstances Healthwatch Surrey reserves the right to break a person's confidentiality and to divulge personal data should this be deemed necessary. These circumstances 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;
- When a person is felt to lack the mental capacity to make a decision - in such cases, staff and volunteers will discuss the issue with a senior manager; they will only act in the person's best interest;
- When the person gives information which indicates a possible terrorist threat.

The decision whether to break a person's confidentiality and to divulge personal data will be decided on a case by case basis and always in conjunction with a senior manager.

8.5 Use of personal data for publicity, reporting or training purposes

Healthwatch Surrey does need to be able to share information, where appropriate, about the impact of our services. If one of our services has a story relating to a particular individual, which would provide useful material for publicity, reporting or training purposes, then wherever possible the permission of the person will be sought in writing before their story is told to anyone else in the event that we plan to use personally identifiable information. If permission cannot be obtained, then any details that would enable the identification of the person concerned will be anonymised.

9. Right of access to personal data (Subject Access)

Data subjects[4] have the right to access any personal data that is being kept about them. Any person who wishes to exercise this right should be asked to make a request in writing, addressed to the Chief Executive Officer. This right is subject to certain exemptions, which are set out in the DPA. The Act will be referred to by the Chief Executive Officer before any requests are processed.

Healthwatch Surrey aims to comply with requests for access to personal data as quickly as possible and will ensure that the personal data kept about the individual concerned are provided within 21 working days, unless there is good reason for a delay. In such cases, the reason for the delay will be explained in writing to the data subject, explaining that the request and the legal time limit of 40 calendar days will be complied with.

In the case of requests from individuals who are neither staff nor volunteers, the Chief Executive Officer will establish, before any disclosure, the identity of the individual by requesting two forms of proof of identity.

Healthwatch Surrey will make a charge of £10 for a disclosure under this right of access.

In accordance with the DPA, an individual who make a written request and pays the required fee is entitled to be:

- Told whether any personal data are being held about them by Healthwatch Surrey;
- Given a description of the personal data held about them, the reasons this information is being held and what it is used for, and whether it will be given to any other organisations or people;
- Given a copy of the personal data held about them and details of the source of this information (where this is available).

Any request for personal data under this policy will be reported to the Board on completion of the appropriate action.

An individual can also prevent further use of their personal data if they can demonstrate that this is causing, or is likely to cause, unwarranted or substantial damage or distress. An individual who wants to exercise this right must put their objection in writing to the Chief Executive Officer and state what they require to be done to avoid causing damage or distress. The Chief Executive Officer will refer to the DPA when dealing with any such requests.

Individuals also have a right under the DPA, in certain circumstances, to have any inaccurate personal data held about them by Healthwatch Surrey rectified, blocked, erased or destroyed.

The **data subject** is defined in the DPA as the individual who is the subject of personal data - ie the individual whom particular personal data are about. The Act does not count as a data subject an individual who has died or who cannot be identified or distinguished from others.

10. Duties of Healthwatch Surrey CIC Directors and staff

Overall and ultimate responsibility for ensuring that Healthwatch Surrey CIC and its service delivery partners (through the SLAs) are complying with the Data Protection Act lies with the Board of Directors.

The Director responsible for the oversight of this policy is the Director for Governance and Compliance.

Operational responsibility for ensuring this policy is put into practice is delegated to the Chief Executive Officer (see below).

All Directors and staff employed by the CIC, including temporary workers, will undertake data protection training prior to being given access to any personal data - this will be provided upon appointment as part of their induction training, when a copy of this policy will be provided as part of the induction checklist. In addition, refresher training will be undertaken at least annually. The training provided will be sufficient to ensure all directors and staff understand their personal responsibilities relating to personal data and have a good awareness of general data security principles and potential threats.

Healthwatch Surrey CIC directors and staff must ensure that they comply with this policy at all times. Any failure to comply with this policy will be subject to disciplinary proceedings.

All Directors and CIC staff have Healthwatch Surrey email accounts on an ICT system which is managed, on behalf of Healthwatch CIC, by SILC. All Directors and CIC staff are required to agree that they will comply with the Terms and Conditions of the system when allocated their accounts. Allocation of accounts is controlled by SILC.

In addition, all Directors and CIC staff have access to an electronic document storage system. Access rights are also controlled by SILC.

Currently, the only personal data to which Directors have access are the contact details of Directors and the Chief Executive Officer.

If any director or member of staff advises Healthwatch Surrey CIC that this policy has not been followed in respect to personal data held about themselves, this will be dealt with under SILC's Dispute Resolution and Grievance Procedure.

11. Duties of the Chief Executive Officer

The Chief Executive Officer has, on behalf of the Board of Directors, the responsibility for all matters pertaining to Data Protection and is, for the purpose of compliance with the DPA, acting as the Data Controller[1] on behalf of Healthwatch Surrey CIC. As such, they will:

- Brief the Board on its Data Protection responsibilities
- Ensure all Directors and staff employed by the CIC, including temporary workers, receive data protection training prior to being given access to any personal data, as well as annual refresher training
- Maintain this policy
- Ensure that our service delivery partners are adhering to DPA 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 CIC and to Healthwatch Surrey volunteers, which is appropriate to their role and needs and is provided
- Check DPA 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 policies relating to the security of the electronic information held by Healthwatch Surrey are consistent with this policy[2]
- Handle demands for disclosure of personal data to outside agencies (e.g. the Police)
- Continue to monitor whether registration with the Information Commissioner's Office is required.

The **Data Controller** is responsible (either alone or jointly or in common with other persons) for determining the purposes for which and the manner in which any personal data are, or are to be, processed. Data controllers will usually be organisations. Even if an individual is given responsibility for data protection in an organisation, they will be acting on behalf of the organisation, which will be the data controller. Data controllers must ensure that any processing of personal data for which they are responsible complies with the DPA.

SILC is responsible for the security of the electronic systems used by Healthwatch Surrey Directors, the Chief Executive Officer and other CIC staff;

LHM ~~**Healthwatch Surrey CIC**~~ is responsible for hosting the Healthwatch Surrey Website; Healthwatch Surrey CIC is responsible for security of records that are sent via the website.

~~**H&C** is responsible for the Consumer Relations Management System (CRM); and ICT used by staff employed by H&C to undertake work on behalf of Healthwatch Surrey CIC and Healthwatch Surrey volunteers.~~

LHM
LHM is responsible for the security of the Informatics System and records stored

within it.

CABx are responsible for the security of the electronic systems used by staff employed by CAiD and Bureaux staff and volunteers who undertake work on behalf of Healthwatch

Any questions or concerns about the interpretation or operation of this policy should, in the first instance, be taken up with the Chief Executive Officer.

In addition, the Chief Executive Officer is responsible for recording the following personal data:

- their contact details and those of the Healthwatch Surrey Directors - the document in which these data are recorded is filed in the electronic documents storage system maintained by SILC on behalf of Healthwatch Surrey CIC; access to these personal data is controlled

- details about complaints received about Healthwatch Surrey - these are also recorded in a document filed on the electronic documents storage system maintained by SILC on behalf of Healthwatch Surrey CIC.

12. Duties of staff employed by service delivery partners

Staff undertaking work on behalf of Healthwatch Surrey CIC (as set out in the relevant SLAs), but who are employed by ~~H&C or~~ Surrey CAB's, are subject to their own organisation's data protection policies.

All staff, including temporary workers, will undertake data protection training prior to being given access to any personal data - this will be provided upon appointment as part of their induction training. In addition, all staff will undertake refresher training at least annually. The training provided will be sufficient to ensure all staff understand their personal responsibilities relating to personal data and have a good awareness of general data security principles and potential threats.

Data protection training will also be provided within the context of new projects, etc, when staff will be briefed about the collection of personal data.

Healthwatch Surrey is responsible for recording the following personal data:

- Data recorded in HR and Finance systems about current and past Healthwatch Surrey Directors and CIC staff

- Data recorded on any database ~~the CRM~~ and in Finance systems about current and past
  Healthwatch Surrey volunteers

CA Woking, LHM and Healthwatch Surrey~~H&C~~ are~~is~~ responsible for recording the following personal data:

- Data collected when people call the Healthwatch Surrey helpline on 0300 303 0023 ~~68~~
~~3000~~ for advice about accessing health and care services - these data are held securely by CA Woking.
  ~~recorded directly on to the Consumer Relations Management System (CRM)~~

- Data collected when people call the Healthwatch Surrey helpline on 0300 303 0023 ~~68~~
~~3000~~ to give feedback on local health and care services - these data are also recorded by CA Woking and transferred securely by email to Healthwatch Surrey CIC

Formatted: Indent: Left: 0 cm
Formatted: Font: 11 pt, Font color: Black, Not Raised by / Lowered by
Formatted ...
Formatted: Indent: Left: 0 cm
Formatted: Indent: First line: 0 cm
Formatted ...
Formatted: Font color: Black
Formatted: Space Before: 0 pt
Formatted ...
Formatted: Font: (Default) Trebuchet MS, Font color: Black
Formatted: Right: -0.04 cm, Space Before: 0 pt, Line spacing: single
Formatted: Font: 11 pt, Font color: Black, Not Raised by / Lowered by
Formatted: Indent: Left: 0 cm
Formatted ...
Formatted ...
Formatted: Indent: Left: 0 cm, Line spacing: single
Formatted: Indent: Left: 0 cm, Space Before: 0 pt
Formatted ...

where records are held securely on a password protected database and by LHM. ~~directly on to the CRM~~

• Data extracted from comments submitted by people about local health and care services on Healthwatch Surrey's website www.healthwatchSurrey.co.uk - these data are subsequently recorded by CA Woking and transferred securely by email to Healthwatch Surrey CIC where records are held securely on a password protected database and by LHM. ~~on the CRM; a~~ A copy of the Healthwatch Surrey Website Privacy Policy is included on the website

• Data extracted from comments about local health and care services submitted by people to Healthwatch Surrey in paper form (and usually posted to Healthwatch Surrey), either on feedback forms, on comments cards or by letter - this data is also subsequently recorded and held securely on a password protected database and by LHM. ~~on the CRM.~~

• Data collected when people give feedback on local health and care services during ~~—~~Healthwatch Surrey community engagement events and other outreach activities - ~~—~~these data are also subsequently recorded and held securely on a password protected database and by LHM. ~~on the CRM~~

~~• Data recorded in HR and Finance systems about current and past Healthwatch Surrey Directors and CIC staff~~

~~• Data recorded on the CRM and in Finance systems about current and past Healthwatch Surrey volunteers~~

~~• Data collected when people give feedback on local health and care services during Healthwatch Surrey community engagement events and other outreach activities - these data are also subsequently recorded on the CRM via a secure CRM portal.~~

~~H&C is also responsible for the CRM; and ICT used by H&C staff and volunteers when undertaking work on behalf of Healthwatch Surrey.~~

SILC is responsible for ensuring the security of the email and electronic document storage systems used by Healthwatch Surrey Directors and CIC staff; the Healthwatch Surrey website; Data recorded in HR and Finance systems about current and past Healthwatch Surrey Directors and CIC staff; Data recorded in HR, on databases and in Finance systems about current and past Healthwatch Surrey volunteers.

Surrey Citizens Advice Bureaux are responsible for recording the following personal data:

- Data collected by Bureaux staff and when people visit one of the Citizens Advice Bureaux in Surrey for face-to-face advice about accessing health and care services - each enquiry is recorded on the CAB Petra system with the name of the client and assigned a Petra number; ~~subsequently, these enquiries are extracted from Petra and, after being pseudonymised[1], are passed on to H&C for recording on to the CRM (maintained by H&C) via a secure CRM portal~~

- Data collected by Bureaux staff when people visit one the Citizens Advice Bureaux in Surrey to provide face-to-face feedback on local health and care services - each 'story' is also recorded on the CAB Petra system with the name of

Formatted ...

Formatted ...

Formatted ...

Formatted: Indent: Left: 0 cm, Space Before: 0 pt

Formatted ...

Formatted: Font: 11 pt, Not Raised by / Lowered by

Formatted ...

Formatted: Indent: Left: 0 cm

Formatted: Indent: Left: 0 cm, Line spacing: single

Formatted ...

Formatted: Font: (Default) Trebuchet MS

Formatted: Line spacing: single

Formatted: Font: 11 pt, Not Raised by / Lowered by

Formatted: Indent: Left: 0 cm

Formatted ...

Formatted: Indent: Left: 0 cm, Line spacing: single

Formatted ...

Formatted ...

Formatted: Indent: Left: 0 cm, Line spacing: single

the client and assigned a Petra number; subsequently, these 'stories' are also extracted from Petra and, after being pseudonymised[5], are passed on securely to the CIC and to LHM.

~~H&C for recording on to the CRM (maintained by H&C) via a secure CRM portal.~~

SDPP is responsible for recording information about clients who use its NHS Advocacy service. SDPP records the information onto its own database. Subsequently the name of the service provider and details of the "story" are passed to Healthwatch Surrey CIC ~~H&C~~ after personally identifiable information has been removed.

~~A Data Sharing Agreement will be in place between Citizens Advice Bureaux and H&C where appropriate.~~

Formatted: Indent: Left: 0.21 cm, Hanging: 0.42 cm, Right: 0.15 cm, Space Before: 0 pt, Line spacing: Multiple 1.01 li

[5] Key aspects of these enquiries and 'stories' are entered on to the transferred securely to the CIC ~~CRM~~ and are logged by their Petra number and originating bureau. The client's profile data and partial postcode are also recorded. This means that if, at a future date, it is deemed necessary by ~~H&C (acting on behalf of~~ Healthwatch Surrey CIC~~)~~ to follow up a particular client, the client can be identified and contacted by the originating bureau

13. Duties of Healthwatch Surrey volunteers

Healthwatch Surrey Volunteers are subject to Healthwatch Surrey's data protection policy.

Volunteers with Surrey Citizens Advice Bureaux undertaking work on behalf of Healthwatch Surrey CIC are subject to the relevant organisation's data protection policies.

All volunteers will undertake data protection training prior to being given access to any personal data - this will be provided as part of their induction training. In addition, all volunteers will undertake refresher training at least annually. The training provided will be sufficient to ensure all volunteers understand their personal responsibilities relating to personal data and have a good awareness of general data security principles and potential threats.

Data protection training will also be provided within the context of new projects, etc, when volunteers will be briefed about the collection of personal data.

Formatted: Right: -0.04 cm, Space Before: 0 pt, Line spacing: single