healthwatch Cornwall

Data protection policy

October 2023

Definitions:

UK GDPR	Means the General Data Protection Regulations as incorporated into UK Law
Responsible Person	Means the Chief Executive Officer
Data Protection Officer (DPO)	A named person who monitors Healthwatch Cornwall (HC) but who is external to any involvement with the running of the organisation over the compliance with UK GDPR and other data protection laws, our data protection policies, awareness-raising, training and audits.
Information Asset Register	Means a register of all systems or contexts in which personal data is processed by HC and includes the information retention schedule

Statement

Healthwatch Cornwall (HC), in the course of carrying out its legitimate business, will process both personal and sensitive data, as described in the Data Protection Act 2018 and UK GDPR. . It is the policy of HC to only collect and retain personal data that is necessary to conduct its business, to respect the privacy of individuals and to ensure that any data held is secure, giving access only to those who have a lawful right to access. This applies to both automated and manual records. HC acts as both a Data Controller in relation to staff and volunteer records and a Data Processor, in terms of records collected in pursuit of its statutory functions. HC is registered with the Information Commissioners Office (ICO).

Involvement and responsibility

Everyone within HC has a responsibility to adhere to the standards of the Data Protection Policy. The Executive Board members, the HC Chief Executive Officer and all employees, including volunteers, have responsibility for the implementation and application of this policy and the associated procedure. This policy applies in all and any areas where staff or volunteers may be working. The Responsible Person shall take responsibility for HC's on-going compliance with this policy.

Involvement and responsibility

Everyone within HC has a responsibility to adhere to the standards of the Data Protection Policy. The Executive Board members, the HC Chief Executive Officer and all employees, including volunteers, have responsibility for the implementation and application of this policy and the associated procedure. This policy applies in all and any areas where staff or volunteers may be

working. The Responsible Person shall take responsibility for HC's on-going compliance with this policy.

Involvement and responsibility

Everyone within HC has a responsibility to adhere to the standards of the Data Protection Policy. The Executive Board members, the HC Chief Executive Officer and all employees, including volunteers, have responsibility for the implementation and application of this policy and the associated procedure. This policy applies in all and any areas where staff or volunteers may be working. The Responsible Person shall take responsibility for HC's on-going compliance with this policy.

Data protection principles

6.1 Complaints will always initially be processed at stage 1 except in the event of a complaint about the CEO which should be made to the Board of Directors (Stage 3) who can be contacted via admin@healthwatchcornwall.co.uk. The timescales referred to in section 3. above will still apply.

HC is committed to processing data in accordance with its responsibilities under UK GDPR. Article 5 of the UK GDPR sets out seven key principles which lie at the heart of the general data protection regime.

Article 5(1) requires that personal data shall be:

"(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

Article 5(2) adds that:

"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Key areas

Processing

To ensure its processing of data is lawful, fair and transparent HC shall maintain an Information Asset Register. This Register will be reviewed at least annually. Individuals will be informed whether and for what purposes personal information relating to them is being processed; the nature of the information and the people to whom such information may be disclosed if appropriate to do so and with explicit consent. Individuals have the right to access their personal data and any such requests made to HC shall be dealt with in a timely manner.

Collection and Maintenance

All data processed by HC must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interest. It is necessary for HC to collect and retain personal data about employees, clients, volunteers and members. Some of this data, such as health details, may be classified sensitive as defined by the Data Protection Act 2018 and UK GDPR. Personal data that is requested and kept on individuals will be relevant and not excessive in relation to the purpose for which it is required or processed. It will be accurate and kept up-to-date. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent will be clearly available and systems in place to ensure such revocation is reflected accurately in HC's systems.

Storage

HC will undertake to implement appropriate security, including technical and organisational procedures against unauthorised or unlawful processing of personal data and to prevent its accidental loss, damage or destruction. HC will ensure that personal data, both electronic and

manual, is stored securely and for no longer than necessary and disposed of appropriately. Records will be disposed of in line with the information retention schedule.
Access to information will be restricted to those who are required, as part of their work, to see that information. Disclosures will be made only where a legal or justifiable need can be proven. In most cases, consent will be obtained to disclose information to parties outside of HC. Exceptions to this would be when a person may be at risk and intervention is necessary for safeguarding, or when behaviour of that person may be criminal or put another at risk.

Sensitive personal data will be treated with additional care in its storage, use and disclosure. Laptops may sometimes be used outside of the office. All laptops are password protected to restrict access to the user only. It is the responsibility of staff using these outside to ensure they are attended securely, kept with them at all times and only used where they may not be overlooked or read by members of the public. The same applies to mass storage hardware like memory sticks – it is the responsibility of the person using them to check they are secure - confidential information should never be transferred onto these devices. Managers or a delegated member of staff may be required in times of bad weather conditions or emergencies to take confidential client details home. This may be manual or computerised. That person will be held wholly responsible for that information which is not to be taken or left anywhere apart from their home and to be securely locked away when not in use. Any breaches of confidentiality direct, negligently or otherwise, or misuse of information may result in disciplinary action which could lead to the termination of their contract of employment. Appropriate back-up and disaster recovery solutions shall be in place.

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. Our Chair and CEO will be informed.

• Within 72 hours, we will inform the Information Commissioner's Office if we assess that there are negative consequences for the individuals involved. We will take proactive mitigation actions and commit to taking any further remedial action they require to address the breach.

• Within 24 hours, we will start to address the root cause of the breach so that no further data is lost and, wherever possible, retrieved.

• Within 48 hours, we will inform Healthwatch England of the data breach.

• Tell any individuals concerned if the breach is likely to result in a 'high' risk to their rights and freedoms without any undue delay.

• Undertake an exercise to ensure that we learn from the data breach to prevent the recurrence of this problem.

• Keep a record of all data breaches and our actions to deal with them

Confidentiality

Any employee, client, volunteer or members' personal information will be treated confidentially and, apart from those who have a lawful right to access it will not be given out to anyone without their express permission. However, there are four occasions when there is no choice about what remains confidential, they are:

- If there is a real concern that a third person is at risk e.g. Suspected adult or child abuse
- Where another law requires us to do something;
- When it is necessary to disclose information for 'crime and taxation' purposes;
- Should an employee, client, volunteer, or member, fall seriously ill while working and information needs to be given to medical personnel.

IT Communications and Monitoring

HC provides employees with access to various computer facilities for work and communication purposes. Technological safeguards exist to protect information stored on these devices being accessed by people other than the legitimate recipients. Further details can be found in the associated procedure.

Individual rights

Access

Everyone has the right to request to access any data held about them. Any such request should be made in writing and a response given within one calendar month. But if your request is complex or you make more than one, the response time may be a maximum of three calendar months, starting from the day after receipt. There are exceptions, which include where access could breach the confidentiality of a third party.

Alteration

Everyone has the right to expect that any inaccuracies should be corrected.

Prevention

Everyone has the right to prevent processing causing damage or distress and should write giving reasons so HC can take appropriate remedial measures.

HC does not sell data. Our only regular communication with people is via the newsletter, after they have given us explicit consent.

This is a controlled document. It should not be altered in any way without the express permission of the author or their representative. On receipt of a new version, please destroy all previous versions.

Document No.	QP017.2			Original issue date:	May 2018
Document Title:	Data Protection Policy			Author:	Business Support
Version:	1	Pages:	6	Last reviewed:	21/07/2021
Approved by:	Board of Directors			Next review:	21/07/2023

Appendix 1: Contact details for relevant personnel

If you require clarification around our process please contact:

Responsible Person: Debbie Gilbert, CEO
07525719847
Debbie.gilbert@healthwatchcornwall.co.uk

In the event of any concerns over potential breaches of data protection contact:

Data Protection Officer: (tba – awaiting agreement from Ian Jones, Volunteer Cornwall as reciprocal arrangement)

Healthwatch Cornwall
Suite 1, Calenick House, Heron Way, Newham, Truro, TR1 2XN

healthwatchcornwall.co.uk
t: 0800 038 1281
e: enquiries@healthwatchcornwall.co.uk
@HWCornwall
Facebook.com/HWCornwall

healthwatch Cornwall