Healthwatch Cambridgeshire Data Protection Policy

This policy applies to all staff, volunteers and board members of Healthwatch Cambridgeshire (HWC).

1. Introduction

The purpose of this policy is to enable Healthwatch Cambridgeshire (HWC) to:

- Comply with the law in respect of the data it holds about individuals;
- Follow good practice;
- Protect HWC's clients, staff, volunteers, board members and other individuals
- Protect the organisation from the consequences of a breach of its responsibilities.

2. Brief introduction to Data Protection Act 1998 and 2003

The Data Protection Act gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly.

The Act works in two ways. Firstly, it states that anyone who processes personal information must comply with eight principles, which make sure that personal information is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with the rights of Data Subjects
- Secure
- Not transferred to other countries without adequate protection

The second area covered by the Act provides individuals with important rights, including the right to find out what personal information is held on computer and most paper records.

3. Policy statement

HWC will:

- Comply with both the law and good practice
- Respect individuals' rights
- Be open and honest with individuals whose data is held

Healthwatch Cambridgeshire, The Maple Centre, 6 Oak Drive, HUNTINGDON, PE29 7HN

- Provide training and support for staff and volunteers who handle personal data, so that they can act confidently and consistently

HWC recognises that its first priority under the Data Protection Act is to avoid causing harm to individuals. Information about staff, volunteers and members of the public will be used fairly, securely and not disclosed to any person unlawfully.

Secondly, the Act aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account. In addition to being open and transparent, HWC will seek to give individuals as much choice as is possible and reasonable over what data is held and how it is used.

HWC is the Data Controller and all processing of personal data will be undertaken in accordance with the data protection principles.

4. Definitions

The Data Subject is the individual whose personal data is being processed. Examples include:

- employees – current and past
- volunteers
- job applicants
- users
- suppliers.

Processing means the use made of personal data including:

- obtaining and retrieving
- holding and storing
- making available within or outside the organisation
- printing, sorting, matching, comparing, destroying.

The Data Controller is the legal 'person', or organisation, that decides why and how personal data is to be processed. The data controller is responsible for complying with the Data Protection Act.

The Data Processor - the data controller may get another organisation to be their data processor, in other words to process the data on their behalf. Data processors are not subject to the Data Protection Act. The responsibility of what is processed and how remains with the data controller. There should be a written contract with the data processor who must have appropriate security.

The Data Protection Officer is the name given to the person in organisations who is the central point of contact for all data compliance issues.

5. Responsibilities

The Board recognises its overall responsibility for ensuring that HWC complies with its legal obligations.

The Data Protection Officer is the CEO who, in liaison with the HWC Information Officer, has the following responsibilities:

- Briefing the board on Data Protection responsibilities
- Reviewing Data Protection and related policies
- Advising other staff on Data Protection issues
- Ensuring that Data Protection induction and training takes place
- Handling subject access requests
- Approving unusual or controversial disclosures of personal data
- Ensuring contracts with Data Processors have appropriate data protection clauses
- Electronic security

Each member of staff and volunteers at HWC who handles personal data will comply with the organisation's operational procedures for handling personal data (including induction and training) to ensure that good Data Protection practice is established and followed.

All staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work.

Significant breaches of this policy will be handled under HWC's disciplinary procedures.

6. Confidentiality

Because confidentiality applies to a much wider range of information than Data Protection, HWC has a separate Confidentiality Policy. This Data Protection Policy should be read in conjunction with HWC's Confidentiality Policy.

HWC has a privacy statement for clients, setting out how their information will be used. This is available on request, and is also published on our website.

Staff and volunteers are required to sign a short statement indicating that they have been made aware of their confidentiality responsibilities.

On occasions, it may be that HWC will need to share a member of the public's personal data with other agencies (Third Parties). Verbal or written agreement will always be sought before data is shared.

Where anyone within HWC feels that it would be appropriate to disclose information in a way contrary to the confidentiality policy, or where an official disclosure request is received, this will only be done after discussions with the HWC CEO and/or Chair. All such disclosures will be documented.

7. Security

This section of the policy only addresses security issues relating to personal data. It does not cover security of the building, business continuity or any other aspect of security.

Any recorded information on clients, volunteers and staff will be:

- Kept in locked cabinets
- Protected by the use of passwords if kept on computer
- Destroyed confidentially if it is no longer needed

Access to information on the main database is controlled by a password and only those needing access are given the password. Staff and volunteers should be careful about information that is displayed on their computer screen and make efforts to ensure that no unauthorised person can view the data when it is on display.

Notes regarding personal data of clients should be shredded or destroyed.

8. Data Recording and storage

HWC has a database holding basic information about all contacts and volunteers.

HWC will regularly review its procedures for ensuring that its records remain accurate and consistent and, in particular:

- The database system is reviewed and re-designed, where necessary, to encourage and facilitate the entry of accurate data.
- Data on any individual will be held in as few places as necessary, and all staff and volunteers will be discouraged from establishing unnecessary additional data sets.
- Effective procedures are in place so that all relevant systems are updated when information about any individual changes.
- Data will be corrected if shown to be inaccurate.

HWC stores archived paper records of clients and volunteers securely in the office.

Documents will be retained for the time periods as set out in Appendix A.

9. Access to data

All staff, volunteers and members of the public who contact HWC have the right to request access to all information stored about them. Any subject access requests will be handled by the Data Protection Officer within the required time limit.

Subject access requests must be in writing. All staff and volunteers are required to pass on anything which might be a subject access request to the Data Protection Officer without delay.

All those making a subject access request will be asked to identify any other individuals who may also hold information about them, so that this data can be retrieved.

Where the individual making a subject access request is not personally known to the Data Protection Officer their identity will be verified before handing over any information.

The required information will be provided in permanent form unless the applicant makes a specific request to be given supervised access in person.

HWC will provide details of information to service users who request it unless the information may cause harm to another person.

Staff have the right to access their file to ensure that information is being used fairly. If information held is inaccurate, the individual must notify the Chief Executive so that this can be recorded on file.

10. Transparency

HWC is committed to ensuring that in principle Data Subjects are aware that their data is being processed and:

- for what purpose it is being processed;
- what types of disclosure are likely; and
- how to exercise their rights in relation to the data.

Data Subjects will generally be informed in the following ways:

- Staff: in the staff terms and conditions
- Volunteers: in the volunteer welcome/support pack
- Members: when they complete application form
- Public: when they request (on paper, on line or by phone) services.

Standard statements will be provided to staff for use on forms where data is collected.

Whenever data is collected, the number of mandatory fields will be kept to a minimum and Data Subjects will be informed which fields are mandatory and why.

11. Consent

Consent will normally not be sought for most processing of information about staff. Although staff details will only be disclosed for purposes unrelated to their work for HWC (e.g. financial references) with their consent.

Information about volunteers will only be made public if it is necessary to their role, and consent will be sought for (a) the means of contact they prefer to be made public, and (b) any publication of information which is not essential for their role.
Information about members of the public who contact HWC will only be made public with their consent (this includes photographs).

'Sensitive' data about clients (including health information) will be held only with the knowledge and consent of the individual.

Consent should be given in writing, although where this is not practicable verbal consent will always be sought to the storing and processing of data. In all cases it will be documented on the database that consent has been given.

All Data Subjects will be given the opportunity to opt out of their data being used in particular ways.

12. Staff training and acceptance of responsibilities

All staff who have access to any kind of personal data will be given copies of all relevant policies and procedures during their induction process, including the Data Protection policy, Confidentiality policy and the operational procedures for handling personal data. All staff will be expected to adhere to all these policies and procedures.

Data Protection will be included in the induction training for all volunteers.

HWC will provide opportunities for staff to explore Data Protection issues through training, team meetings, and supervisions.

13. Policy review

The policy will be reviewed at least annually by the CEO and Data Protection Officer and approved by the Board. It will also be reviewed in response to changes in relevant legislation, contractual arrangements, good practice or in response to an identified failing in its effectiveness.

Approved by Healthwatch Cambridgeshire Board of Directors
Date: 20 January 2016

For Review
Date: January 2017

Responsible Officer
Chief Executive Officer of Healthwatch Cambridgeshire

Appendix A

Document Retention Periods	
Governance Processes	
Board Meetings: • Minute Books • Handwritten Notes from Meetings	 Permanent Dispose once minutes approved at next meeting
Strategy and Reporting: • Annual Reports • Annual Statement of Accounts • Strategic processes and resolutions	 Permanent Permanent 3 years after last action
Financial Management	
Accounts and Audit: • Auditors Reports/Final Letters • Audit of Accounts • General Audit Correspondence	 6 years + current 6 years + current 2 years + current
Financial Transactions: • Budget Monitoring • Invoice copies	 6 years + current 6 years + current
Payroll: • Salary records • SSP records • Maternity Pay records	 6 years + current 3 years after tax year to which they relate 3 years after tax year to which they relate
Human Resources	
Appointments – Staff, Board and Volunteers: • Successful • Unsuccessful	 6 years after employment ceases 2 years after appointment of successful candidate
Personnel administration: • Accident Book • Correspondence • Expense claims • Pensions • Personal Development Reviews • Register of Interests	 3 years 6 years + current 6 years + current 6 years after employment ceases 6 years after employment ceases 6 years + current

Training and Development: • Training records – Staff, Board and Volunteers	6 years + current
Management and Administration	
Correspondence: • General • Board	2 years + current 2 years + current
Complaints	6 years
Consultation: • Surveys and summaries of findings	5 years after closure
Enter and View Visits: • Reports • Correspondence • Complaints	Permanent 3 years + current 6 years
Information Management: • Gifts and Hospitality Records • Information Retention and Disposal Register	6 years + current Permanent
Legal and Contracts • Insurance • Service Level Agreements • Shared Agreements	7 years after last action 2 years after contract expiry 2 years after agreement expiry
Media Relations: • Press cuttings • Media Reports	Permanent Permanent
Policies and Procedures	Permanent
Publications • All	One copy to held Permanent