2. Data Protection Policy

Introduction

In order to carry out its activities, Healthwatch Worcestershire needs to gather and use information about individuals including customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. This information may include personal data.

This policy sets out our commitment to protecting personal data and describes how we shall use and handle personal data.

We are committed to:

- Complying with GDPR and the Data Protection Act 2018
- Ensuring all data is held for a lawful purpose
- Protecting the rights of staff, customers and partners in relation to their personal data
- Being open about how we store and process individual's data
- Ensuring that personal data is stored securely

Data Protection Law

The Data Protection Act 2018 describes how organisations – including Healthwatch Worcestershire – must collect, handle and store personal information. This law implements the requirements of the General Data Protection Regulation (EU) 2016/679

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly for defined purposes, stored securely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These state that personal data must

- Be processed fairly and lawfully and in a transparent manner
- Collected for specific, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and where necessary kept up to date
- Retained only for as long as necessary
- Processed in an appropriate manner to maintain security

Healthwatch Worcestershire is committed ensuring we comply with these principles in our day-to-day activities.

In line with GDPR Healthwatch Worcestershire have moved to a risk-based approach with a regular assessment of data and the risks to Data Subjects associated with holding that data. Healthwatch Worcestershire will design processes and procedures which ensure that risk mitigations and privacy are

achieved through standard work processes in line with the ISO 9001 (2015) standard.

Scope

This policy applies to the whole company of Healthwatch Worcestershire. It applies to all data that the company holds relating to identifiable individuals. This can include:

- Names
- Postal addresses
- Email addresses
- Phone numbers
- IP addresses
- Descriptive information covering Healthwatch Worcestershire intentions regarding identifiable individuals

The Data Protection Act 2018 and GDPR classifies this information as personal data and requires that it is treated in accordance with the six data protection principles.

Healthwatch Worcestershire will at least annually or when there is a significant change in business, review the data to check for increases or decreases in scope.

The risk assessment will dictate the exact practices that Healthwatch Worcestershire will put into place and these will be documented in the Data Protection Impact Assessment (DPIA).

Responsibilities

Everyone who works for or with Healthwatch Worcestershire has responsibility for ensuring data is collected, stored and handled appropriately.

- The Board of Directors is ultimately responsible for ensuring that Healthwatch Worcestershire meets its obligations regarding privacy. Healthwatch Worcestershire is registered with the Information Commissioners Office. The Directors have appointed the Managing Director as the registered Information Controller.
- The Managing Director (MD) is responsible for privacy on a day to day basis; responsible for:
    - Keeping the board up to date about data protection responsibilities, risks and issues, this will be a standing board agenda.
    - Ensuring that risks are reviewed at least annually or when there is a significant change in business.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from staff or partners
    - Dealing with requests from individuals to see the data Healthwatch Worcestershire holds about them (Subject Access Requests).
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- The Data Protection Officer (DPO) is responsible for:
    - Informing and advising HWW and its employees about any obligations to comply with the GDPR and other data protection legislation.
    - Monitoring compliance with the GDPR and other data protection laws including managing internal data protection procedures, raising awareness of data protection issues, training staff and conducting internal audits.
    - Advising on and monitoring data processing impact assessments.
    - Cooperating with the supervisory authority.
    - Providing the first point of contact for the supervisory authority and individuals whose data is processed.

    - Ensuring all systems, services and equipment used for storing data meet security standards relevant to the identified risks.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly
    - Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services.

- The Managing Director is responsible for:
    - Approving any data protection statements attached to communications such as emails and letters.
    - Addressing any data protection queries from journalists or media outlets.
    - Ensuring consent is obtained and recorded of any marketing activity conducted by the company in pursuit of its normal business.

Staff Responsibilities

Access to personal data shall only be granted to staff and contractors who require such access in order to fulfil their role or a necessary business function.

Data shall only be shared in accordance with Healthwatch Worcestershire's Information Security Policy

Staff and contractors are responsible for ensuring that they protect personal data by acting in accordance with Healthwatch Worcestershire's Information Security Policy and Acceptable Usage Policy and their working procedures.

The MD is the first point of contact for any queries relating to personal data and data security. If staff or contractors are in any doubt about their responsibilities, they must contact the MD for advice.

Where staff feel there may have been a breach in data handling process or are informed by any partner company that there has been a breach of data, they are required to inform the MD without delay

Data Use

Personal data shall only be processed in relation to the specific purposes listed in Healthwatch Worcestershire's registration with the Information Commissioners

Office (ICO) (which can be found in Healthwatch Worcestershire's Privacy Statement (which can be found at https://www.healthwatchworcestershire.co.uk/privacy-statement/)

Personal data shall not be transferred outside the EEA unless the organisation storing the data is subject to an adequacy agreement that is supported by the Information Commissioner's Office.

Data Accuracy

The law requires Healthwatch Worcestershire to take reasonable steps to ensure data is kept accurate and up to date.

The MD shall regularly review Healthwatch Worcestershire's approach to storing and handling personal data and ensure that processes are in place to maintain the accuracy of all personal data.

Staff and contractors shall alert the MD to any inaccurate information, in order that it can be corrected. The MD is responsible for correcting such inaccuracies.

In order to assist with maintaining accuracy, data must be held in as few places as necessary. Staff must not create unnecessary duplicates of data sets.

Disclosing Data

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcing agencies without the consent of the data subject.

If a request is received to disclose data in this manner, the Data Protection Officer and the board will review the request for disclosure and shall confirm that the request is genuine, taking legal advice as necessary.

Data subjects have a right to access the data held by Healthwatch Worcestershire about them. This is called a subject access request. Requests would usually be received by post from data subjects but may be received by email. All staff shall forward such requests to the DPO immediately.

Healthwatch Worcestershire will fulfil all data access requests without delay. It is the DPO's responsibility to lead this process.