Policy Title: Data Protection Policy

Date: December 2018

Version Control

Version Number	Date	Revisions	By
1.1	06.12.2018	Full review	Maxine Taffetani

Contents

Policy Statement

Healthwatch Milton Keynes is committed to a policy of protecting the rights and privacy of individuals, including staff, volunteers, Trustees, and suppliers in accordance with the General Data Protection Regulation (GDPR) May 2018 and the Data Protection Act 2018 (DPA 2018).

The GDPR/DPA 2018 demand higher transparency and accountability in how Healthwatch Milton Keynes manages and uses personal data. They also accord new and stronger rights for individuals to understand and control that use. As data controllers and processors, we need to ensure that we fully comply with GDPR/DPA 2018 and that we proactively design data protection systems that protect the rights and freedoms of data subjects.

To comply with the GDPR/DPA 2018 Healthwatch Milton Keynes must ensure that all information about individuals is collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

Compliance

This policy applies to all staff, volunteers and Trustees of Healthwatch Milton Keynes. Breach of this policy, or of the law will be managed under Healthwatch Milton Keynes' disciplinary procedures. All staff, volunteers and trustees should proactively raise any queries or concerns about data protection through appropriate channels as soon as these arise. Healthwatch Milton Keynes will be responsible for making training, support and resources available to staff, volunteers and trustees to enable them to fulfil their data protection obligations.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to legislation.

Definitions and Responsibilities

A 'data subject' is the person whose personal data is being held and used. Healthwatch Milton Keynes' data subjects include employees, volunteers, job applicants and members of the public.

'Personal data' is defined as data relating to a living individual who can be identified from that data; or from that data and other information which is in the possession of or is likely to come into the possession of the data controller and includes an 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.

'Sensitive personal data' is defined as personal data consisting of information regarding an individual's racial or ethnic origin; political opinion; religious or other

beliefs; trade union membership; physical or mental health or condition; sexual life; or criminal proceedings or convictions.

“Processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, transmission, dissemination or adaption of the data.

Healthwatch Milton Keynes will be the ‘data controller’ under the terms of the legislation, this is described by the Information Commissioners Office as someone who “determines the purposes and means of processing personal data”. Healthwatch Milton Keynes is also the processor of the data. In some cases, Healthwatch Milton Keynes may be a data processor for other another controller (e.g. when carrying out research for a health provider), or they may pass personal data to another party for processing (e.g. a payroll company).

All staff, volunteers and trustees are responsible for compliance with this policy. The trustees are responsible for monitoring delivery of this policy. The Chief Executive Officer is responsible for managing data subject access requests.

Healthwatch Milton Keynes has a Data Protection Officer to monitor internal compliance, inform and advise Healthwatch Milton Keynes on its data protection obligations and provide advice regarding Data Protection Impact Assessments (DPIAs). The DPO is independent, an expert in data protection, adequately resourced, and reports to the Board of Trustees which has oversight of the organisation.

Data Protection Principles

The legislation places a responsibility on every data controller to process any personal data in accordance with the eight principles below. More detailed guidance on these principles can be found in this link to the ICO’s website.

To comply with the law, the information we obtain will be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To meet these requirements, Healthwatch Milton Keynes’ staff, staff, volunteers and trustees must follow the Data Protection Principles set out in the GDPR/DPA 2018 which are summarised below:

1. We will process data lawfully, fairly and transparently
2. We will only collect data for explicit and lawful purposes
3. Data must be relevant and necessary for the purpose its being collected
4. We will keep data up to date and accurate
5. We will keep data only if required and for no longer than necessary
6. We will keep data secure
7. We will process data in such a way as to protect the rights and freedoms of data subjects
8. Personal data will be transferred outside of the EU only in certain specific circumstances and ways

Application of the Policy

We retain and use personal data to help us to carry out our role as the local independent champion for people who use health and social care services. We collect information about our staff, volunteers and people who share their experiences of using health and social care services through our website, by email, post and telephone, and through our outreach events.

Healthwatch Milton Keynes staff, volunteers and trustees who collect, store or use any personal information in the course of their duties must follow this policy at all times. This is a legal requirement and any failure to comply may result in disciplinary proceedings. We will proactively and by design protect the rights and freedoms of data subjects. How we do this is set out below:

1. **The right to fair processing:** That data subjects have the right to information about the processing of their data and about their rights

We will tell data subjects about the way we handle data and their rights in clear language that they can understand. We will do this when we collect the data. Our Privacy Statement sets out the data processing practices carried out by Healthwatch Milton Keynes' and tells them what their rights are.

2. **The right of access:** That data subjects have the right to receive a copy of their data, including any data being processed by third parties. This allows them to be aware of, and verify, the lawfulness of the processing

The GDPR details rights of individuals (data subject) to access both manual data (which is recorded in a relevant filing system) and electronic data for the data subject. This is known as a Data Subject Access Request (DSAR). Under the GDPR, organisations are required to respond to subject access requests within one month. Failure to do so is a breach of the GDPR and could lead to a complaint being made to the Data Protection Regulator. Staff, volunteers and trustees should be alert to DSAR's, and proactively help data subjects to make these requests. Requests should be made in writing and include the full name, date of birth and address of the person seeking access to their information. When a subject access request is received, it should immediately be reported to the Executive Director to log and track each request. No fee can be charged for initial DSAR for all types of records, whether manual or electronic format. Information relating to the individual must only be disclosed to them or someone with their written consent to receive it.

Any individual wishing to exercise this right should apply in writing to the Chief Executive and the process for this should be available on the Healthwatch Milton Keynes website. Any member of staff receiving a DSAR should forward this to the Chief Executive.

Anyone who believes that this policy has not been followed with regard to personal data about him/her should raise the matter with the person responsible for that data. If the matter is not satisfactorily resolved, it should be raised as a formal complaint.

3. **The Right to Rectification:** The data subject has the right to correct any inaccuracies in the data.

We will work to maintain accurate data by regularly reviewing the data we have and making it clear to data subjects that they can correct any data that is wrong. This will be clear in our privacy statement.

4. **The right to be forgotten:** That the data subject can have their personal data removed or erased at any time without delay.

We will only store data for as long as is needed. The periods that data is retained are kept in an Information Asset Register which gives further clarity on how we manage and keep secure data that is shared with us. Healthwatch Milton Keynes will erase data in line with this register, and additionally consider any requests to erase data in line with GDPR/DPA 2018.

5. **The right to restriction of processing:** That a data subject is allowed, in specific circumstances, to prevent Healthwatch Milton Keynes' from conducting specific processing tasks.

The Information Asset register and the privacy statement taken together give a clear description of the processing that is taking place. Any data subject who wants Healthwatch Milton Keynes to stop some processing activity can make this request. Processing will be halted pending a decision, which may include the DPO acting as mediator, and will involve Healthwatch Milton Keynes clearly evidencing the lawful grounds for the processing. The default position will be to comply with the request.

6. **The right to data portability:** That the data subject can request copies of their data in a useful format in order to pass them to another service provider.

Healthwatch Milton Keynes will make personal data available to data subjects in a useful format, most commonly electronic.

7. **The right to object:** That if a data subject objects to how their data is being controlled or processed, HEALTHWATCH OXFORDSHIRE must halt processing until it has investigated and demonstrated its legitimate grounds for processing.

Healthwatch Milton Keynes will respond proactively to concerns of or complaints by data subjects and will involve the DPO in where required. The information asset register clearly describes the lawful grounds for controlling and processing each kind of data.

8. **The right to appropriate decision-making:** That Healthwatch Milton Keynes will ensure decisions are not made solely by automated means.

Healthwatch Milton Keynes puts data protection at the heart of our work by design and by default and gives people in the organisation explicit roles to manage the personal data we collect.

Data Security

Healthwatch Milton Keynes endeavours to safeguard personal information (i.e. keeping paper files and other records or documents containing personal/sensitive data in a secure environment; protecting personal data held on computers and computer systems by the use of secure passwords, which where possible, are changed periodically; and ensuring that individual passwords are not easily compromised);

Paper records

All hard copy personal data is kept in locked cabinets in the Healthwatch Milton Keynes' office, a secure building. Data collected at events outside of the office will be kept with the member of the team collecting the information, stored in the boot of their car and placed in a locked cabinet upon their return to the office.

Electronically stored personal data

Data retained on laptops, smartphones and any other electronic equipment that is removed from Healthwatch Milton Keynes' offices is protected by the use of passwords. Access to information on the main database is controlled by a password and only those needing access are given the password.

All staff, volunteers and trustees are responsible for ensuring that any personal data that they hold is stored securely and that personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party. 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.

Third parties and data processors

Any data passed to a third party, including to a processor, will be specified in a written agreement, setting out the scope and limits of the sharing. These parties are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data. They have to confirm their conformance to the requirements of the GDPR/DPA 2018.

Specifically:

- The data subject will be informed about any third parties who are in receipt of their data from Healthwatch Milton Keynes
- Any disclosure of personal data will be in compliance with approved procedure
- Data stored electronically (e.g. in databases, survey providers etc.) will be kept at minimum industry standards. This includes access controls (password

protection), physical security, the use of anti-virus software and ensuring staff are trained in information governance and controls.

By law, Healthwatch Milton Keynes is required to provide employee liability information to any organisation that our employees are transferring to, in line with the Transfer of Undertakings Regulations (TUPE);

References that disclose personal information will not be provided to any third party without the data subject's prior authority (unless this is required or permitted by law such as by the police, HMRC, Contributions Agency or similar body.

Data breaches

If Healthwatch Milton Keynes discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The organisation will record all data breaches regardless of their effect. The DPO will be informed immediately.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, Healthwatch Milton Keynes will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

Groups of Data Subjects

Employees

Healthwatch Milton Keynes holds personal information about all employees as part of general employee records. This includes address and contact details, educational background, employment application, employment history with Healthwatch Milton Keynes, areas of expertise, details of salary and benefits, bank details, performance appraisals and salary reviews, records relating to holiday, sickness and other leave, working time records and other management records

This information is used for a variety of administration and management purposes, including payroll administration, benefits administration, facilitating the management of work and employees, performance and salary reviews, complying with record keeping and other legal obligations;

Healthwatch Milton Keynes may also process information relating to employee's health which may amount to sensitive personal data. This includes pre-employment health questionnaires, records of sickness absence and medical certificates (including self-certification of absence forms), VDU assessments, noise assessments and any other medical reports. This information is used to administer contractual and Statutory Sick Pay, monitor and manage sickness absence and comply with our obligations under health and safety legislation and the Working Time Regulations;

From time to time Healthwatch Milton Keynes may ask employees to review and update the personal information that is held about them.

Children

Wherever possible, Healthwatch Milton Keynes will avoid holding personal data about people under the age of 16. Where it is working with children, it will seek to work with a third party who controls the data in line with that organisations data protection policy. If personal data is held about a child, then the consent of that child's legal parent or guardian will be sought and appropriately stored. The only exception is that Healthwatch Milton Keynes will share information as per their Safeguarding Policy.

Adults in need of care and support

In some cases, information will be shared with Healthwatch Milton Keynes about a person's care by their carer or family member. In these cases, Healthwatch Milton Keynes will only hold personal data with the explicit consent of the person who the information is about. A carers experiences of caring may be gathered and shared. If the information identifies the person they care for, it will only be processed with the informed consent of the cared for person. If the person receiving care does not consent, Healthwatch Milton Keynes' will ensure any information is fully anonymised. The only exception is that Healthwatch Milton Keynes will share information as per their Safeguarding Policy.

Registration

Healthwatch Milton Keynes registered in the Information Commissioner's public register of data controllers. Reference: ZA262574.

Audit and Review

This policy will be updated as necessary to reflect best practice or future amendments made to the law.

We are committed to having a proactive and systematic review process in place and as such we will conduct an annual audit.

Data Protection Impact Assessments

DPIAs are used to identify specific risks to personal data as a result of processing activities. Their role is to maintain security and prevent processing infringements of GDPR. Healthwatch Milton Keynes will use them when required to evaluate the risks inherent in our work. A DPIA must contain:

- a description of processing and purposes;
- legitimate interests pursued by the controller;
- an assessment of the necessity and proportionality of the processing;
- an assessment of the risks to the rights and freedoms of data subjects;

- the measures envisaged to address the risks;
- timeframes if processing for retention and erasure of data;
- recipients of data;
- any evidence of compliance;
- details of consultation with and consent of data subjects.

This information is held within the information asset register. The register identifies which personal data processing presents any particular risk, and how this is managed, including the decision to use a DPIA.