**Policy Title:** Data Protection

**Date:** May 2024

# Version Control

| Version Number | Date | Revisions | By |
|---|---|---|---|
| 5 | Jan 26 | Policy reviewed, Branding updated | Maxine Taffetani |
| 4 | May 2024 | Policy reviewed, minor edits made to punctuation and formatting. | HR Initiatives |
| 3 | 09.08.2021 | Reformatted document | HR Initiatives |
| 2 | 20.06.2019 | Review and typos corrected | Maxine Taffetani |
| 1 | 06.12.2018 | Full review | Maxine Taffetani |

# Contents

Policy Statement ..... 4
Compliance ..... 4
Definitions and Responsibilities ..... 5
Data Protection Principles ..... 6
Application of the Policy ..... 7
Data Security ..... 10
Paper records ..... 10
Electronically stored personal data ..... 10
Data Subject Access Requests ..... 11
Data Security ..... 11
1. Paper records ..... 12
2. Electronically stored personal data ..... 12
Third parties and data processors ..... 12
Data breaches ..... 13
Groups of Data Subjects ..... 14
Employees ..... 14
Children ..... 14
Adults in need of care and support ..... 15
Registration ..... 15
Audit and Review ..... 15
Data Protection Impact Assessments ..... 15
Data breaches ..... 16
Individual responsibilities ..... 16
Training ..... 17

## Policy Statement

Engage-Share-Inspire MK CIO, also trading as 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 Engage-Share-Inspire MK CIO manages and uses personal data. They also accord stronger rights for individuals to understand and control that use. As data controllers and processors, we ensure full compliance with GDPR/DPA 2018 and proactively design data protection systems that protect the rights and freedoms of data subjects.

To comply with the GDPR/DPA 2018 Engage-Share-Inspire MK CIO 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 Engage-Share-Inspire MK CIO. 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. Engage-Share-Inspire MK CIO is 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 any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

**"Special categories of personal data"** means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data.

**"Criminal records data"** means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

**"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.

Engage-Share-Inspire MK CIO 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". Engage-Share-Inspire MK CIO is also the processor of the data. In some cases, Engage-Share-Inspire MK CIO 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.

Engage-Share-Inspire MK CIO has a Data Protection Officer to monitor internal compliance, inform and advise Engage-Share-Inspire MK CIO 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

Engage-Share-Inspire MK CIO processes HR-related personal data in accordance with the following data protection principles:

- The organisation processes personal data lawfully, fairly and in a transparent manner.
- The organisation collects personal data only for specified, explicit and legitimate purposes.
- The organisation processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The organisation keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The organisation keeps personal data only for the period necessary for processing.
- The organisation adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

Engage-Share-Inspire MK CIO shall tell individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons. If the organisation wants to start processing HR-related data for other reasons, individuals will be informed of this before any processing begins.

HR-related data will not be shared with third parties, except as set out in privacy notices. Where the organisation relies on its legitimate interests as the basis for processing data, it will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

Where the organisation processes special categories of personal data or criminal records data to perform obligations, to exercise rights in

employment law, or for reasons of substantial public interest, this is done in accordance with a policy on processing special categories of data and criminal records data.

The organisation will update HR-related personal data promptly if an individual advises that their information has changed or is inaccurate.

Personal data gathered during the employment, worker, contractor or volunteer relationship, or apprenticeship or internship is held in the individual's personnel file (in hard copy or electronic format, or both), and on the BreatheHR system. The periods for which the organisation holds HR-related personal data are contained in its privacy notices to individuals.

The organisation keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the UK General Data Protection Regulation (UK GDPR).

## 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 – Healthwatch Milton Keynes. 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.

Engage-Share-Inspire MK CIO 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 Engage-Share-Inspire MK CIO 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 CEO 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 CEO.

   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. Engage-Share-Inspire MK CIO 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 Engage-Share-Inspire MK CIO 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 to pass them to another service provider.

   Engage-Share-Inspire MK CIO 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, Engage-Share-Inspire MK CIO must halt processing until it has investigated and demonstrated its legitimate grounds for processing.

Engage-Share-Inspire MK CIO 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 Engage-Share-Inspire MK CIO will ensure decisions are not made solely by automated means.

   Engage-Share-Inspire MK CIO 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

Engage-Share-Inspire MK CIO 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 Engage-Share-Inspire MK CIO, 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 Engage-Share-Inspire MK CIO 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.

## Data Subject Access Requests

To make a subject access request, the individual should send the request to Maxine.taffetani@healthwatchmiltonkeynes.co.uk. In some cases, Healthwatch Milton Keynes may need to ask for proof of identification before the request can be processed. We will inform the individual if we need to verify the identity and the documents required.

We will normally respond to a request within a period of 28 days from the date it is received. In some cases, such as where the request is complex, we may respond within three months of the date the request is received. The Chief Executive will write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, the organisation is not obliged to comply with it. Alternatively, the organisation can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded if it is made with the intention of harassing the organisation or causing disruption, or excessive where it repeats a request to which the organisation has already responded. If an individual submits a request that is unfounded or excessive, the organisation will notify them that this is the case and whether or not it will respond to it.

## Data Security

Engage-Share-Inspire MK CIO takes the security of HR-related personal data seriously. The organisation has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Engage-Share-Inspire MK CIO 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.

### 1. Paper records

All hard copy personal data is kept in locked cabinets in the Engage-Share-Inspire MK CIO 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.

No papers should be left in a car overnight and the car must be locked at all times when the car is unattended.

### 2. Electronically stored personal data

Data retained on laptops, smartphones and any other electronic equipment that is removed from Engage-Share-Inspire MK CIO 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

Where Engage-Share-Inspire MK CIO engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

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 Engage-Share-Inspire MK CIO.
- 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, Engage-Share-Inspire MK CIO 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 Engage-Share-Inspire MK CIO 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, Engage-Share-Inspire MK CIO 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

Engage-Share-Inspire MK CIO 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 Engage-Share-Inspire MK CIO, 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. Engage-Share-Inspire MK CIO may also process information relating to employees' 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 Engage-Share-Inspire MK CIO may ask employees to review and update the personal information that is held about them.

### Children

Wherever possible, Engage-Share-Inspire MK CIO 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 Engage-

Share-Inspire MK CIO will share information as per their Safeguarding Policy.

### Adults in need of care and support

In some cases, information will be shared with Engage-Share-Inspire MK CIO about a person's care by their carer or family member. In these cases, Engage-Share-Inspire MK CIO will only hold personal data with the explicit consent of the person who the information is about. A carer's 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, Engage-Share-Inspire MK CIO will ensure any information is fully anonymised. The only exception is that Engage-Share-Inspire MK CIO will share information as per the Safeguarding Policy.

### Registration

Engage-Share-Inspire MK CIO is 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. Engage-Share-Inspire MK CIO 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.

## Data breaches

If Engage-Share-Inspire MK CIO discovers that there has been a breach of HR-related 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.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it 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.

## Individual responsibilities

Individuals are responsible for helping the organisation keep their personal data up to date. Individuals should let the organisation know if data provided to the organisation changes, for example if an individual moves house or changes bank details.

Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment, contract, volunteer period, internship, or apprenticeship. Where this is the case, the

organisation relies on individuals to help meet its data protection obligations to staff and to customers and clients.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- not to store personal data on local drives or on personal devices that are used for work purposes; and
- to report data breaches of which they become aware to the data protection officer immediately.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the organisation's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

## Training

Engage-Share-Inspire MK CIO will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

## Reviews of this Policy

This policy will be reviewed every three years, or when changes are required.