Data Protection Policy

1. Purpose of this policy

Healthwatch Sutton recognises the role it has to protect the rights, freedoms and privacy of the people who share personal data with it. This policy applies to all staff, directors and volunteers of HWS. HWS collects and uses personal data, including sensitive personal data, which means it is responsible for complying with the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR).

HWS is an Information and Commissioning Office (ICO) registered organisation, and follows the ICO framework.

The aim of this policy is to assist and inform the staff, directors and volunteers of HWS to comply with the requirement of the Data Protection Act (DPA) 2018 and GDPR, to minimise any risks to HWS and its data subjects, and to provide clear good practice guidelines for all involved. It sets out what HWS will do, what is expected of staff, directors and volunteers. It must be fully understood and adopted by all staff, directors and volunteers.

2. Definitions

Data subject

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

Personal data

'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

'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

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 adaptation of the data.

3. Data controller

HWS is the Data Controller under the Act, which means that it determines what purposes personal information is held and will be used for. It is also responsible for notifying the

Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

4. Disclosure

HWS may share data with other agencies such as the local authority, funding bodies and other voluntary agencies. The individual/service user will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows HWS to disclose data (including sensitive data) without the data subject's consent. These are:

- Carrying out a legal duty or as authorised by the Secretary of State
- Protecting vital interests of an individual
- The individual has already made the information public
- Conducting any legal proceedings, obtaining legal advice or defending any legal rights
- Monitoring for equal opportunities purposes i.e. race, disability or religion
- Providing a confidential service where the individual's consent cannot be obtained or where it is reasonable to proceed without consent e.g. where we would wish to avoid forcing stressed or ill individuals/members to provide consent signatures.

5. Principles

HWS endorse and adhere to the principles of the Data Protection Act 2018. The way we do this is summarised below:

- We will process data lawfully, fairly and transparently;
- We will only collect data for explicit and lawful purposes;
- Data must be relevant and necessary for the purpose its being collected;
- We will keep data up to date and accurate;
- We will keep data only if required and for no longer than necessary (see the Information Asset Register);
- We will keep data secure;
- We will process data in such a way as to protect the rights and freedoms of data subjects; and
- Personal data will be transferred outside of the EU only in certain specific circumstances and ways.

These principles apply to obtaining, handling, processing, transporting and storage of personal data. Staff, directors and volunteers, as well as agents of HWS who obtain, handle, process, transport and store personal data, must adhere to these principles at all times. HWS will provide reasonable levels of training, support and resources to do so.

HWS will, through appropriate management and strict application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of information.
- Meet its legal obligations to specify the purposes for which information is used.
- Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements.
- Ensure the quality of information used.

- Take appropriate technical and organisational security measures to safeguard personal information.
- Ensure that personal information is not transferred abroad without suitable safeguards.
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.
- Set out clear procedures for responding with requests for information.

HWS will also ensure that the rights of people about whom information is held, can be fully exercised under the Act. These include:

- **The right to fair processing**

Data subjects have the right to information about the processing of their data and about their rights.

- **The right of access**

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 right to rectification**

The data subject has the right to correct any inaccuracies in the data.

- **The right to be forgotten**

The data subject can have their personal data removed or erased at any time without delay.

- **The right to restriction of processing**

A data subject is allowed, in specific circumstances, to prevent HWS from conducting specific processing tasks.

- **The right to data portability**

The data subject can request copies of their data in a useful format in order to pass them to another service provider.

- **The right to object**

If a data subject objects to how their data is being controlled or processed, HWS must halt processing until it has investigated and demonstrated its legitimate grounds for processing.

- **The right to appropriate decision making**

HWS will ensure decisions are not made solely by automated means.

6. Data collection

HWS will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form. Informed consent is when:

- An individual/member clearly understands why their information is needed and how it will be used, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data.

When collecting data, HWS will ensure that the individual/member:

- As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed
- Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress

7. Data storage

HWS 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 were possible, are changed periodically; and ensuring that individual passwords are not easily compromised);

7.1. Paper records

All hard copy personal data is kept in locked cabinets in the HWS office, a secure building.

7.2. Electronically stored personal data

Data stored electronically (e.g. in databases, survey providers etc.) will be kept to an appropriate standard and audited annually.

Data retained on laptops, smartphones and any other electronic equipment that is removed from HWS 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, directors and volunteers 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.

8. Data access and accuracy

All individuals/members have the right to access the information HWS holds about them. HWS will also take reasonable steps to ensure that this information regarding complaints is kept up to date by asking data subjects whether there have been any changes.

In addition, HWS will ensure that:

- It has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection.
- Everyone processing personal information understands that they are contractually responsible for following good data protection practice.
- Everyone processing personal information is appropriately trained to do so.
- Everyone processing personal information is appropriately supervised.

- Anybody wanting to make enquiries about handling personal information knows what to do.
- It deals promptly and courteously with any enquiries about handling personal information.
- It describes clearly how it handles personal information.
- It will regularly review and audit the ways it holds, manages and uses personal information.
- It regularly assesses and evaluates its methods and performance in relation to handling personal information.
- All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against him.

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 made to the Data Protection Act 1998 and General Data Protection Regulation (GDPR).

In case of any queries or questions in relation to this policy, please contact the Healthwatch Sutton Data Protection Officer: Pete Flavell, Chief Executive Officer, telephone: 020 8641 9540.

Approved by Healthwatch Sutton Board of Directors: 09/03/2020

To be reviewed: 09/03/2023

Responsible Officer: Chief Executive Officer of Healthwatch Sutton