Managing Information & Privacy

(Previously: Data Protection and Information Governance Policies)

This policy applies to all employees, Board Members and volunteers of Healthwatch Hertfordshire (HwH), as well as third parties responsible for processing of personal data on behalf of HwH.

Introduction & Purpose:

This policy outlines the expected behaviours of HwH employees, trustees, volunteers and third parties in relation to the collection, use, retention, transfer, disclosure and destruction of any **personal data** belonging to a HwH contact (i.e. the data subject).

HwH, as the Data Controller, is responsible for ensuring compliance with the data protection requirements outlined in this policy. Non-compliance may expose HwH to complaints, regulatory action, fines and/or reputational damage.

The purpose of this policy is to enable HwH to:

1. Comply with the law in respect of the data it holds about individuals
2. Follow good practice
3. Protect members of the public who contact HwH, staff, trustees, volunteers and other individuals
4. Protect the organisation from the consequences of a breach of its responsibilities

A brief introduction to the General Data Protection Regulation (GDPR)

The General Data Protection Regulation introduced a single data privacy law for the European Union (including the United Kingdom (UK). It aims to provide more transparency and provides individuals with more control and rights to the data held on them. Furthermore it provides a framework to ensure that personal information is handled properly by data controllers and data processors.

The UK GDPR is the retained EU law version of the General Data Protection Regulation EU as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419).

It is defined in section 3(10) of the Data Protection Act 2018 (DPA 2018), supplemented by section 205(4).

It includes the provisions of what was previously the applied GDPR, unless the context otherwise requires.

With effect from 1 January 2021, organisations need to bear in mind that there are two legal texts to consider, where relevant: the UK GDPR as well as the DPA 2018.

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

1. Processed **lawfully**, **fairly** and in a **transparent** manner
2. Processed for **limited purpose**
3. **Adequate**, **relevant** and limited to what is necessary in relation to the purposes of which they are processed.
4. **Accurate** and **up to date**
5. Not kept for longer than is necessary
6. **Secure**

The regulation outlines a seventh principle focused on **accountability.** This principle puts onus on the data controller to be responsible for and demonstrate compliance. As a public body, HwH additionally holds itself to the Caldicott Principles in the manner in which it processes personal information. See Appendix 1 for a full list of the Principles.

The second area covered by the regulation provides individuals with eight important rights:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

Policy statement

HwH will:

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

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

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

Secondly, the regulation aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account. HwH will seek to give individuals as much choice as is possible and reasonable over what data is held and how it is used, and is fully committed to upholding all data subject rights under the GDPR, as well as processing all personal data in accordance with the data protection principles.

HwH is committed to continued and effective implementation of this policy, and requires all HwH employees, trustees, volunteers and third parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action for staff, termination of a volunteer's involvement with HwH as a volunteer, or termination of contract for third parties.

Confidentiality

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

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

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

On occasions, it may be that HwH 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 HwH 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 a senior manager or the Data Protection Officer.

Data collection, processing and quality

Data Subject Notification

HwH will provide data subjects with information as to the purpose of processing their personal data. Where applicable, the data subject will be informed at the point of first contact that they have the right to object, at any stage, to having their data processed for such purposes.

When the data subject is asked to give consent to the processing of personal data and when any personal data is collected from the data subject, all appropriate disclosures will be made. This is unless one or both of the following applies:

- The data subject already has the information;
- A legal exemption applies to the requirements for disclosure and/or consent.

The disclosures may be given verbally, electronically or in writing. If given verbally, the person making the disclosures should use a suitable script pro forma approved in advance. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

Where it has been determined that notification to a data subject is required, notification should occur promptly, and no later than:

- One calendar month from the first collection or recording of the personal data
- At the time of first communication if used for communication with the data subject

Data collection

Personal data should be collected only from the data subject unless the collection must be carried out under emergency circumstances in order to protect the vital interests of the data subject or to prevent serious loss or injury to another person e.g. safeguarding purposes.

If personal data is collected from someone other than the data subject, the data subject must be informed of the collection. This is unless one or more of the following applies:

- The data subject has received the required information by other means
- The information must remain confidential due to a professional secrecy obligation
- A national law expressly provides for the collection, processing or transfer of the personal data

Data processing

HwH uses the personal data of its contacts for the following broad purposes:

- To deliver services and activities as outlined under part 5 of the Health and Social Care act 2012
- The general running and business administration of the organisation (including charitable and limited company aspects)
- The ongoing administration and management of services to customers

HwH will not process personal data unless at least one of the following requirements is met:

- The data subject has given consent to the processing of their personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject).

There are some circumstances in which personal data may be further processed for purposes that go beyond the original purpose for which the personal data was collected. When making a determination as to the compatibility of the new reason for processing, guidance and approval must be obtained from the Data Protection Officer before any such processing may commence.

In any circumstance where consent has not been gained for the specific processing in question, HwH will address the following additional conditions to determine the fairness and transparency of any processing beyond the original purpose for which the personal data was collected:

- Any link between the purpose for which the personal data was collected and the reasons for intended further processing.
- The nature of the personal data, in particular whether special categories of data are being processed, or whether personal data related to criminal convictions and offences are being processed.
- The possible consequences of the intended further processing for the data subject.
- The existence of appropriate safeguards pertaining to further processing, which may include encryption, anonymisation or pseudonymisation.
- The context in which the personal data has been collected, in particular regarding the relationship between data subject and the Data Controller.

HwH may need to share personal or sensitive data with third parties for the following purposes:

- Gathering the views and experiences of patients, service users and the public and making these views known
- Making reports and recommendations about the improvement of services
- Promoting and supporting the involvement of people in the commissioning, provision and scrutiny of local services
- Recommending investigation and special review of services
- Signposting and information to enable people to make informed choices
- Making the views and experiences of people known to Healthwatch England and other bodies.
- Legal requirements

Special Categories of Data

HwH will only process special categories of data (also known as sensitive data) where the data subject expressly consents to such processing or where one of the following conditions apply:

- The processing relates to personal data which has already been made public by the data subject.
- The processing is necessary for the establishment, exercise or defence of legal claims.
- The processing is specifically authorised or required by law.
- The processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent.
- Further conditions, including limitations, based upon national law related to the processing of genetic data, biometric data or data concerning health.

Where special categories of data are being processed, HwH will adopt additional protection measures. In any situation where special categories of data are to be processed, the basis for the processing must be clearly recorded with the personal data in question.

Children's Data

Children under the age of 13 are unable to consent to the processing of personal data; in such cases consent must be sought from the person who holds parental responsibility over the child. However, it should be noted that where processing is lawful under other grounds, consent need not be obtained from the child or the holder of parental responsibility.

Consent

HwH will obtain personal data only by lawful and fair means and, where appropriate with the knowledge and consent of the individual concerned. Where a need exists to request and receive the consent of an individual prior to the collection, use or disclosure of their personal data, HwH is committed to seeking such 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 HwH (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 HwH will only be made public with their consent. See HwH's Confidentiality Policy for further details.

'Sensitive' data about members of the public who contact HwH (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.

Profiling & Automated Decision Making

HwH does not currently engage in profiling and automated decision-making of personal data.

If HwH were to engage in profiling and automated decision-making, it would only do so where it is necessary to enter into, or to perform, a contract with the data subject, or where it is authorised by law. Where HwH utilises profiling and automated decision-making, this will be disclosed to the relevant data subjects. In such cases the data subject will be given the opportunity to:

- Express their point of view.
- Obtain an explanation for the automated decision.
- Review the logic used by the automated system.
- Supplement the automated system with additional data.
- Have a human carry out a review of the automated decision.
- Contest the automated decision.
- Object to the automated decision-making being carried out. HwH will also ensure that all profiling and automated decision-making relating to a data subject is based on accurate data.

Data Transfers

HwH may transfer personal data to internal or third party recipients located in another country where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant data subjects. Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. third countries), they must be made in compliance with an approved transfer mechanism. HwH will only transfer personal data where one of the transfer scenarios list below applies:

- The data subject has given Consent to the proposed transfer.
- The transfer is necessary for the performance of a contract with the data subject
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the data subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded with a third party in the interest of the data subject.

- The transfer is legally required on important public interest grounds.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the data subject

Data Retention

To ensure fair processing, personal data will not be retained by HwH for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed. The length of time for which HwH will need to retain personal data is set out in HWH '*Data Retention schedule'*. This takes into account the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule.

All personal data will be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

Data 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.

HwH will adopt physical, technical, and organisational measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment. A summary of the personal data related security measures is provided below:

- Prevent unauthorised persons from gaining access to data processing systems in which personal data are processed.
- Prevent persons entitled to use a data processing system from accessing personal data beyond their needs and authorisations.
- Ensure that personal data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation (see below discussing contracts with third parties).
- Ensure that access logs are in place to establish whether, and by whom, the personal data was entered into, modified on or removed from a data processing system.
- Ensure that in the case where processing is carried out by a Data Processor, the data can be processed only in accordance with the instructions of the Data Controller.
- Ensure that personal data is protected against undesired destruction or loss.
- Ensure that personal data collected for different purposes can and is processed separately.
- Ensure that personal data is not kept longer than necessary

HwH also has a 'Standard Data Processing Agreement' document that is used as a baseline template for creating UK GDPR compliant information sharing protocols with third parties. When HwH is

outsourcing services to a third party (including cloud computing services), they will identify whether the third party will process personal data on its behalf and whether the outsourcing will entail any third country transfers of personal data. In either case, it will make sure to include, in cooperation with the HwH Data Protection Officer, adequate provisions in the outsourcing agreement for such processing and third country transfers.

Data Quality

HwH will adopt all necessary measures to ensure that the personal data it collects and processes is complete and accurate in the first instance, and is updated to reflect the current situation of the data subject. The measures adopted by HwH to ensure data quality include:

- Correcting personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the data subject does not request rectification.
- Keeping personal data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
- The removal of personal data if in violation of any of the data protection principles or if the personal data is no longer required.
- Restriction, rather than deletion of personal data if:
    - a law prohibits erasure
    - erasure would impair legitimate interests of the data subject
    - the data subject disputes that their personal data is correct and it cannot be clearly ascertained whether their information is correct or incorrect

Data Protection by Design

To ensure that all data protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them will go through an approval process before continuing.

See the 'Data Protection impact assessment procedure' and the 'Data protection impact assessment template' for more detail.

Access to Data and Data subject Requests

All staff, trustees, volunteers and members of the public who contact HwH have the right to request access to all information stored about them.

All staff, trustees and volunteers are required to pass on anything which might be a subject access request to the Data Protection Officer without delay.

Subject access requests must be in writing. 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. 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.

HwH will consider each such request in accordance with all applicable data protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

It should be noted that situations may arise where providing the information requested by a data subject would disclose personal data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights. Any subject access requests will be handled by the Data Protection Officer within 40 days from the day the request is received.

Detailed guidance for dealing with requests from data subjects can be found in HwH's 'Data Subject Access Rights Procedure' document.

Breach Reporting and Complaints Handling and Breach Reporting

Breach Reporting

Any individual who suspects that a personal data breach has occurred due to the theft or exposure of personal data must immediately notify the Data Protection Officer providing a description of what occurred.

The Data Protection Officer will investigate all reported incidents to confirm whether or not a personal data breach has occurred. If a personal data breach is confirmed, the Data Protection Officer will follow the relevant authorised procedure based on the criticality and quantity of the personal data involved.

More detail on the process can be found in the HwH 'Data Breach Procedure'.

Complaints Handling

Data subjects with a complaint about the processing of their personal data, should put forward the matter in writing to the Data Protection Officer. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Data Protection Officer will inform the data subject of the progress and the outcome of the complaint within timeframes outlined in the 'HwH Complaints Policy'. If the issue cannot be resolved through consultation between the data subject and the Data Protection Officer, then the data subject may seek redress via a complaint to Information Commissioner's Office.

Responsibilities

All staff, Board Members, and volunteers should reference Appendix II of this document for more detailed explanations of how/when to share data.

Board

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

Staff and Volunteers

HwH will make sure all third parties engaged to process personal data on their behalf (i.e. their data processors) are aware of and comply with the contents of this policy. Assurance of such compliance will be obtained from all third parties, whether companies or individuals, prior to granting them access to personal data controlled by Healthwatch Hertfordshire.

All staff and volunteers 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 Managing Information and Privacy Policy, Confidentiality policy and the operational procedures for handling personal data.

All staff and volunteers are required to read, understand and adhere to any policies and procedures that relates to the personal data that they may handle in the course of their role, as well as ensure that good Data Protection practice is established and followed.

HwH will provide opportunities for staff and volunteers to explore Data Protection issues through training and supervisions as a minimum.

Data Protection Officer

The Data Protection Officer operates with independence and is supported by suitability skilled individuals granted all necessary authority. The Data Protection Officer reports to HwH's CEO. The Data Protection Officer's duties include:

- Informing and advising HwH and its employees who carry out processing pursuant to data protection regulations, national law or European Union based data protection provisions;
- Ensuring the alignment of this policy with data protection regulations, national law or European Union based data protection provisions;
- Providing guidance with regards to carrying out Data Protection Impact Assessments (DPIAs);
- Acting as a point of contact for and cooperating with Data Protection Authorities (DPAs);
- Determining the need for notifications to one or more DPAs as a result of HwH's current or intended personal data processing activities;
- Making and keeping current notifications to one or more DPAs as a result of HwH's current or intended personal data processing activities;

- The establishment and operation of a system providing prompt and appropriate responses to data subject requests;
- Informing HwH senior managers, officers, and Trustees of any potential corporate, civil and criminal penalties which may be levied against HwH and/or its employees for violation of applicable data protection laws.

Ensuring establishment of procedures and standard contractual provisions for obtaining compliance with this Policy by any third party who:

- provides personal data to HwH
- receives personal data from HwH
- has access to personal data collected or processed by HwH

Support, Advice and Communication

For advice and support in relation to this policy, please contact the Data Protection Officer via email DPO@healthwatchhertfordshire.co.uk.

Glossary of terms:

General Data Protection Regulation (GDPR): the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It is embodied in UK Law. The version applying to the UK also addresses the export of personal data outside the UK.

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 demonstrating compliance with the regulation.

Data Processor – is the legal 'person' that processes data on behalf of the Data Controller

Data Protection Impact Assessment: a tool used to identify and reduce the privacy risks of legal 'persons' by analysing the personal data that are processed and the policies in place to protect the data

Data Protection Officer (DPO) - is the name given to the person who is the central point of contact for all data compliance issues. They are an expert on data privacy and work independently to ensure that the organisation is adhering to the policies and procedures set out in the GDPR.

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union.

Information Commissioner's Office (ICO): The ICO is the UK's independent body set up to uphold information rights

Personal Data is any information (including opinions and intentions) which relates to a natural person or 'data subject' that can be used to directly or indirectly identify the person. Personal data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process personal data.

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

- Employees – current and past
- Volunteers
- Job applicants
- Users
- Suppliers

Processing is any operation performed on personal data, whether or not by automated means, including:

- Obtaining and retrieving
- Holding and storing
- Making available within or outside the organisation
- Printing, sorting, matching, comparing, destroying

Profiling: any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour.

Regulation: a binding legislative act that must be applied in its entirety across the Union.

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them.

Policy review

The policy will be reviewed at least once every two years by the 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.

I confirm that I have read, understood and will follow the HwH Data Protection Policy:

Signature.....

Job title.....

Date**.....**

Reviewed and signed off with minimal changes on 21st April 2023:

Nuray Ercan

Signed by Nuray Ercan, as Company Secretary

Responsible Officer
Geoff Brown, Chief Executive

Appendix I – Caldicott Principles

HwH will apply the Six Caldicott Principles as detailed in the Caldicott Report 1997 to its information governance. Caldicott is the name given to a set of six principles, which resulted from a Government investigation, by Dame Fiona Caldicott into confidentiality and security of personal information within the NHS. These principles and new arrangements were first introduced into the Health Service but have, with effect from 2002, been introduced by the Government for Family Services records.

The updated Caldicott Principles are:

- Justify the purpose
- Do not use personal data unless it is absolutely necessary
- Use the minimum necessary personal data
- Access to personal data should be on a strict need to know basis
- Everyone with access to personal data should be aware of their responsibilities
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality.

Appendix II - Principles guiding the sharing of information

HwH will apply the following key principles to the sharing of information between any parties:

- HwH acknowledge their 'Duty of Confidentiality' to individuals. In requesting release and disclosure of information from other organisations, and/or agencies, staff will respect this responsibility and not seek to override the procedures, which the organisation has in place to ensure that information is not disclosed illegally or inappropriately.
- As a minimum, individuals will be informed at the point at which information is collected, if information is to be shared, the circumstances in which this could happen and who the information may be shared with. HwH will ensure written or verbal consent of the individuals is sought and provided before sharing information
- An individual's personal information will only be disclosed where the purpose for which it has been agreed to share clearly requires that this is necessary in accordance with Data Protection principles and the 'need to know' principle. For all other purposes information should be anonymous.
- Where it is agreed to be necessary for information to be shared, only the information needed will be shared and that would only be on a "need to know" basis.