Managing Personal 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.

Contents

1. 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 (see glossary at end of document for full definitions), 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

1.1 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 documents to consider, where relevant: the UK GDPR as well as the DPA 2018.

These laws work in two ways. Firstly, they state 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 I 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[1]

1.2 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

[1] Please see here for an explainer on each of the rights.

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.

1.3 Confidentiality

Because confidentiality applies to a much wider range of information than Data Protection, 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 here.

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.

2. Data collection, processing and quality

2.1 Data Subject Notification

HwH will provide data subjects with information as to the purpose of processing their personal data (please see glossary at the end of this document for relevant definitions). 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 (examples have been included at the end of this document in appendix II). The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure. Please find pro forma scripts/templates used by HwH staff members included in the mentioned appendix at the end of this document.

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

2.2 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

2.3 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 (see glossary) of the data subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest.
- 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 (see glossary for definition) with third parties for the following purposes:

- Legal requirements
- Protecting the vital interests of the data subject or another natural person (such as in a safeguarding concern)

2.4 Special Categories of Data or Sensitive 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.

2.5 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.

2.6 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.

2.7 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.

2.8 Data Transfers outside the UK

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 listed 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

2.9 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'*, see appendix III. 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, or after 30 days have passed since last contact. Most short-term contact data will be deleted within 30 days of the last contact if no further action is needed.

2.10 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, (see glossary) 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 (see appendix IV) 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.

2.11 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

2.12 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' (Appendix V) and the 'Data protection impact assessment template' (Appendix VI) for more detail.

3. Access to Data and Data Subject Requests (Subject Access 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 their line manager or volunteer lead without delay. The responsible person must allocate a staff member to manage the request. This may be the Data Protection Officer (DPO) or a staff member, and the data subject may be offered, where possible, the choice.

Subject access requests must be in writing. Where the individual making a subject access request is not personally known 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 responded to within 1 month from the day the request is received (with possible extension up to two months for complex cases).

Detailed guidance for dealing with requests from data subjects can be found in HwH's 'Data Subject Access Request Procedure' document (see Appendix VII).

4. Breach Reporting and Complaints Handling

4.1 Breach Reporting

Any individual who suspects that a personal data breach has occurred must **immediately** notify the Data Protection Officer providing a description of what occurred.

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

When a personal data breach has occurred, the likelihood of the risk to people's rights and freedoms will be established. If a risk is likely, the ICO will be notified within 72 hours of the discovery of the breach. If a risk is unlikely, justification for this decision will be documented and it does not have to be reported to the ICO.

More detail on the process can be found in the HwH 'Data Breach Procedure' (see Appendix VIII).

4.2 Complaints Handling

Data subjects with a complaint about the processing of their personal data, should put forward the matter in writing to any staff member or the Data Protection Officer. Staff should pass the complaint to the DPO 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.

4.3 Responsibilities

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

4.4 Board

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

4.5 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.

4.6 Data Protection Officer (Moreau & Co)

Our Data Protection Officer is an external organisation named Moreau & Co. The Data Protection Officer operates with independence and is supported by suitably skilled individuals granted all necessary authority. The Data Protection Officer reports to HwH's CEO. The Data Protection Officer's duties include:

- To provide on-going ad-hoc advice to Healthwatch Hertfordshire staff on GDPR issues via telephone and/or e-mail, up to 1 hour per month;
- To offer support to the completion of an annual audit and improvement plan of DP practice at Healthwatch Hertfordshire, liaising with key staff and the Senior Information Risk Owner, including review meetings every 6 months;
- To maintain own knowledge of data protection regulations and best practice in order to offer advice aligned with recognised professional industry standards and the expert knowledge requirements of the UK GDPR.
- To hold responsibility for a dedicated DPO@ e-mail address, and responding to enquiries from the public to this e-mail address;
- To be prepared to respond to data breaches, data subject access requests and support Data Protection Impact Assessments as required (terms and conditions to be agreed in each event).

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).

5. 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 (or sensitive) 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.

Vital interest: in the context of data protection, this is a lawful basis for processing personal data, meaning it can be done if necessary to protect someone's life.

6. Policy review and Declaration

The policy will be reviewed at least once every two years by the GDPR Lead 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 Managing Personal Information & Privacy Policy:

Signature.....

Job title.....

Date.....

Reviewed and signed off by Board with minimal changes on 21st October 2025:

Nuray Ercan

Signed by Nuray Ercan, as Company Secretary

Responsible Officer
Ivana Chalmers, 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 – Data Subject Notification Scripts and Consent Statements

Signposting and Feedback:
In cases where individuals have copied us into a complaint they've written directly to the service provider or commissioner, where individuals have fed back to us directly by email (not via the website):

"Please note we record the public's experiences of services they share with us anonymously (we do not store contact details or identifiable information), and share any trends we identify with providers and commissioners to improve services for everyone. For more information about this, please read our privacy policy.

Given that you have shared your experience with us, we will take this as an indication that you give your permission for this to be anonymously recorded on our database. If you have any questions or do not wish for us to do this, please let me know."

When wrapping up a phone call, we gather the caller's permission to record their experiences by reading the below script:

"Thank you for sharing your experience with us, and I hope we have been able to help. So that we can help others, are you happy for us to record your experience anonymously on our database (so, not using any identifiable information)? We will never pass on anything identifiable to a third party without your agreement, but we do share broad themes collected from the feedback we get – your experience would feed into this. Does that sound okay? You can find more information on all of this in our privacy statement via our website."

Research Projects, including focus groups and 1-1 interviews:

HwH talk before Engagement

Introduction

Thank you for sparing your time and agreeing to take part in this [insert engagement method]. Before we begin, I'll provide a short introduction to Healthwatch Hertfordshire, the work we are doing, and what we will do with the information you share today.

[Insert introduction about Healthwatch Hertfordshire and information about the study]

Do you have any questions before I move on to how we handle the information you provide today?

I will now read out how we handle data we collect.

- Any information you share today will be anonymised and treated in like with UK GDPR guidelines.
- In no circumstances will details be discussed with anyone in such a manner that it is possible to identify you.
- Anonymised data we collect with be collated to identify key themes. Key themes will be shared with the [insert relevant service] to [insert reasons here]

- I plan to record the information you provide today, solely for the purpose of analysing the information. The recording will not be shared with anyone and will be deleted as soon as it has been analysed. **Are you happy for me to record this conversation today?**
- You have the right to withdraw your data at anytime. This also means if you wish to leave the conversation at any point, you are able to do so.
- If there are any questions you don't feel comfortable answering, please say and we will move on.
- If you need any more information on how we collect and use data and your right to withdraw, you can look at the privacy statement on our website, or we can email this to you.

Is there anything else regarding your data that you would like to ask before we begin?

Can I please confirm that you are happy with the data protection discussed and that you are happy to proceed?

Appendix III – Data Retention Rules/Schedule

Employment	
In general the staff records (including those of volunteers) should be retained for **6 years after the end of employment**, but need only contain sufficient information in order to provide a reference (e.g. training and disciplinary records). Copies of any reference given should be retained for 6 years after the reference request. Director's files should be retained for 6 years.	
Application form	Duration of employment, destroy when employment ends
References received	Duration of employment, destroy when employment ends
Sickness and maternity records	6 years from end of employment
Annual leave records	6 years from end of employment
Unpaid leave/special leave records	6 years from end of employment
Records relating to an injury or accident at work	12 years
References given/information to enable a reference to be provided	6 years from end of employment
Recruitment and selection material (unsuccessful candidates)	2 years after recruitment is finalised
Disciplinary records	6 years after employment has ended
Statutory Maternity Pay records, calculations and certificates	Retain while employed and for seven years after employment has ended
Redundancy details, calculation of payments and refunds	Seven years from date of redundancy
Note: if an allegation has been made about the member of staff, volunteer or trustee the staff record should be retained until they reach the normal retirement age or for 10 years, if that is longer. E.g. around Safeguarding.	
Record of Comments and other evidence, e.g. observations, interviews, enter and view notes.	
Comments recorded on internal databases	Retain in line with local policy
Any paper based comments recorded on the database.	Destroyed once recorded electronically
Comments and or other evidence that have not been recorded on the database.	Retain in line with local policy

Signed consent forms	Destroy in line with above
DBS checks	
Record disclosure reference no. and date of check and return to the volunteer or staff member.	
Financial Records	
Financial records	6 years (public funded Companies)
Income tax and NI returns, income tax records and correspondence with HMRC	Not less than 3 years after the end of the financial year to which they relate
Payroll records (also overtime, bonuses, expenses)	10 years
Pension contribution records	6 years
Pension Scheme Investment Policies	12 years from any benefit payable under the policy
Corporate	
Employers Liability Certificate	40 years
Insurance policies	Permanently
Certificate of Incorporation	Permanently
Minutes of Board of Trustees	Permanently
Memorandum of Association	Original to be kept permanently
Articles of Association	Original to be kept permanently
Variations to the Governing Documents	Original to be kept permanently
Statutory Registers	Permanently
Subscriber records	20 years from commencement of subscriber register
Rental or Hire Purchase Agreements	6 years after expiry
Others	
Deeds of Title	Permanently
Leases	12 years after lease has expired
Accident books	3 years from the date of the last entry (or, if the accident involves a child/ young adult, then until that person reaches the age of 21).
Health and Safety Policy Documents	Retain until superseded
Assessment of Risks under Health and Safety Legislation	Retain until superseded
Contact Details	

Paper forms	Upload to electronic system and destroy once it is confirmed that the contact details have been correctly uploaded (i.e. email sent and does not bounce).
Mailing lists	Retain until unsubscribed, notified of change or cleaned due to non-receipt of emails
Google Contacts (Day to day contact details)	Retain until we receive a request to delete or are notified of a change of contact details
Postal contacts	Retain until we receive a request to delete.

Processes for Deletion

All records are made and held in accordance with the principles of the General Data Protection Regulation. Records are retained for the period specified in the table above, and with the exception of items that must be stored permanently, are then safely destroyed.

Procedure:

1. Any paper based records, such as HR files are held securely in a locked filing cabinet.
2. Electronic files are kept securely, are password protected and regularly backed up. These include databases with personal information, payroll information and financial records.
3. Members of the public who choose to engage with Healthwatch Hertfordshire are asked for consent that their comments be stored on a secure database and informed that personal information will be kept confidential and will not be shared unless express consent has been given. When asking for consent to pass on personal details HwH will always confirm how the information will be used and passed on.
4. When DBS checks are requested, HwH will keep a record of the date the check was completed on the relevant volunteer or staff file, but do not keep a copy of the DBS check.
5. HwH complies with the requirements of company law and records are maintained and retained in accordance with the retention summary above. HwH also complies with the Statement of Recommended Practice (SORP) in relation to its financial record keeping and reporting; and all financial records are retained in accordance with the retention summary above.
6. HwH stores insurance policies and employer's liability insurance certificates and records relating to the ownership or leasehold of premises securely and in line with the retention summary above.
7. Confidential hard copy records that are waiting to be destroyed should be kept securely and shredded or disposed of using a reputable company.
8. Electronic records should be destroyed in line with the retention schedule above by a reputable company and a certificate of destruction provided.

Appendix IV – Data Processing Agreement Template

Data Processing Agreement

Template

AGREEMENT DATED [*insert date*]

BETWEEN:

(1) **Healthwatch Hertfordshire** ("HwH"); and

(2) [ ], having its registered office at [ ] (the "Processor").

BACKGROUND

(A) This Agreement is to ensure there is in place proper arrangements relating to personal data passed from HwH to the Processor.

(B) This Agreement is compliant with the requirements of Article 28 of the General Data Protection Regulation.

(C) The parties wish to record their commitments under this Agreement.

IT IS AGREED AS FOLLOWS:

1. DEFINITIONS AND INTERPRETATION

In this Agreement:

"Data Protection Laws" means the Data Protection Act 1998, together with successor legislation incorporating GDPR;

"Data" means personal data passed under this Agreement;

"GDPR" means the General Data Protection Regulation;

"Services" means [*describe the services provided by the Processor to HwH*].

2. DATA PROCESSING

HwH is the data controller for the Data and the Processor is the data processor for the Data. The Data Processor agrees to process the Data only in accordance with Data Protection Laws and in particular on the following conditions:

a. the Processor shall only process the Data (i) on the written instructions from HwH (ii) only process the Data for completing the Services and (iii) only process the Data in the UK with no transfer of the Data outside of the UK (Article 28, para 3(a) GDPR);

b. ensure that all employees and other representatives accessing the Data are (i) aware of the terms of this Agreement and (ii) have received comprehensive training on Data Protection Laws

and related good practice, and (iii) are bound by a commitment of confidentiality (Article 28, para 3(b) GDPR);

c. HwH and the Processor have agreed to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, complying with Article 32 of GDPR, details of those measures are set out under Part A of the Annex to this Agreement (Article 28, para 3(c) GDPR);

d. the Processor shall not involve any third party in the processing of the Data without the consent of HwH. If consent is given a further processing agreement will be required (Article 28, para 3(d) GDPR);

e. taking into account the nature of the processing, assist HwH by appropriate technical and organisational measures, in so far as this is possible, for the fulfilment of HwH's obligation to respond to requests from individuals exercising their rights laid down in Chapter III of GDPR – rights to erasure, rectification, access, restriction, portability, object and right not to be subject to automated decision making etc (Article 28, para 3(e) GDPR);

f. assist HwH in ensuring compliance with the obligations pursuant to Articles 32 to 36 of GDPR – security, notification of data breaches, communication of data breaches to individuals, data protection impact assessments and when necessary consultation with the ICO etc, taking into account the nature of processing and the information available to the Processor (Article 28, para 3(f) GDPR);

g. at HwH's choice safely delete or return the Data at any time. [It has been agreed that the Processor will in any event securely delete the Data at the end of the Services]. Where the Processor is to delete the Data, deletion shall include destruction of all existing copies unless otherwise a legal requirement to retain the Data. Where there is a legal requirement the Processor will prior to entering into this Agreement confirm such an obligation in writing to HwH. Upon request by HwH the Processor shall provide certification of destruction of all Data (Article 28, para 3(g) GDPR);

h. make immediately available to HwH all information necessary to demonstrate compliance with the obligations laid down under this Agreement and allow for and contribute to any audits, inspections or other verification exercises required by HwH from time to time (Article 28, para 3(h) GDPR);

i. arrangements relating to the secure transfer of the Data from HwH to the Processor and the safe keeping of the Data by the Processor are detailed under Part A of the Annex.

j. maintain the integrity of the Data, without alteration, ensuring that the Data can be separated from any other information created; and

k. immediately contact HwH if there is any personal data breach or incident where the Data may have been compromised.

3. <u>Termination</u>

The Processor may not terminate this Agreement without the written consent of HwH.

4. <u>General</u>

a. This Agreement may only be varied with the written consent of both parties.

b. For the purposes of this Agreement the representatives of each party are detailed under Part B of the Annex.

c. This Agreement represents the entire understanding of the parties relating to necessary legal protections arising out of their data controller/processor relationship under Data Protection Laws.

d. This Agreement is subject to English law and the exclusive jurisdiction of the English Courts.

For and on behalf of Healthwatch Hertfordshire

.....

For and on behalf of [ ]

.....

ANNEX

Part A

Compliance with Article 32, para 1 of GDPR

1. Consideration of anonymisation, pseudonymisation and encryption.

   Is the above possible? If not, please explain why. If possible please insert details.

2. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and related services.

   Please explain how the above will be delivered.

3. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

   Please confirm the above is possible and description of process in place to deliver the above.

4. A process for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures for ensuring the security of the processing.

   Please confirm the above process is in place and broadly what that process is.

Compliance with Article 32, para 2 of GDPR

5. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to data transmitted, stored or otherwise processed.

Please describe secure transfer process from HwH to the Processor and levels of security to be applied by the Processor when the Data is in their possession.

Compliance with Article 32, para 3 of GDPR

6. Adherence to an approved code of conduct referred to in Article 40 (GDPR) or an approved certification mechanism as referred to in Article 42 (GDPR) may be used as an element by which to demonstrate compliance with the requirements set out in para 1 of GDPR – see above.

   Please describe any relevant code of practice relied upon.

Compliance with Article 32, para 4 of GDPR

7. The Processor to ensure that anyone acting on their behalf does not process any of the Data unless following instructions from HwH unless they are required to do so under English law.

ANNEX

Part B

Healthwatch Hertfordshire's Representative shall be [*insert details*] or such other person as shall be notified by HwH [*insert details*].

The Processor Representative shall be [*insert details*] or such other person as shall be notified by the Processor [*insert details*].

Appendix V – Data Protection Impact Assessment (DPIA) Procedure

Purpose

A Data Protection Impact **Assessment** is a tool used to identify and reduce the privacy risks of entities by analysing the personal data that is processed and the policies in place to protect the data.

Data Protection Impact Assessments (DPIA) are used to identify and mitigate against any data protection related risks arising from a new project, service, product, or process, which may affect the organisation (Data Controller) or the individuals (Data Subjects).

This procedure applies to all Healthwatch Hertfordshire employees, including part-time, temporary, or contract employees, that handle personal data as part of working for Healthwatch Hertfordshire.

This procedure should be read in conjunction with the HWH Data Protection Policy, HWH Confidentiality Policy and the HWH Information Governance Policy.

When is DPIA necessary

DPIA is necessary:

- Before the implementation of new technologies, processes, systems or projects, or before the modification of existing technologies or processes;
- Data processing is likely to result in a high risk to the rights and freedoms of individuals.

Processing that is likely to result in a high risk includes (but is not limited to):

- Systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals;
- Large scale processing of special categories of data or personal data relation to criminal convictions or offences;
- Large scale, systematic monitoring of public areas e.g. CCTV

Please see the Data Protection Impact Assessment Template 'Section One' for more detail.

Should the Regulator (Information Commissioners Office) be consulted on completion of the DPIA

If, during the DPIA process, Healthwatch Hertfordshire has identified and taken measures to mitigate any risks to personal data, it is not necessary to consult with the ICO before proceeding with the changes.

If the DPIA suggests that any identified risks cannot be managed and the residual risk remains high, you must consult with the Regulator before moving forward with the project.

Regardless of whether or not consultation with the Regulator is required, all HwH employees have an obligation to retain a record of the DPIA and update the DPIA in due course.

Even if consultation is not required, the DPIA may be reviewed by the ICO at a later date in the event of an audit or investigation arising from your use of personal data.

Procedure

Steps for conducting DPIA

1.1 **Describe the purpose and the lawful basis**. *Populate Section Two of the Data Protection Impact Assessment (DPIA) Form.*

1.2 **Describe data flows.** Identify how personal information will be collected, stored, used and deleted as part of the new (or modified) system or process. Identify what kinds of data will be used as part of the new (or modified) system or process and who will have access to the data. *Populate Section Three of the Data Protection Impact Assessment (DPIA) Form.*

1.3 **Identify data protection and related risks.** List the relevant people and organisations that been engaged to understand the potential privacy risks that may result as part of your planned work activity. *Populate Section Four of the Data Protection Impact Assessment (DPIA) Form.* Identify all risks to Data Subjects or to the organisation (Data Controller) that are related to personal data protection. *Populate Section Five of the Data Protection Impact Assessment (DPIA) Form.*

1.4 **Assign risk mitigation measures.** For each risk assign risk mitigation measures. Focus on mitigating measures for risks with High and Medium impact category. *Populate Section Five of the Data Protection Impact Assessment (DPIA) Form.*

1.5 Explain why you consider that it is **necessary and proportionate to proceed with the proposal**. *Populate Section Six of the Data Protection Impact Assessment (DPIA) Form.*

1.6 **Further actions.** Consider if the Regulator should be consulted for the DPIA. Plan regular DPIA reviews and updates of required.

1.7 **DPO** Recommendation and Sign off.

1.8 Send the completed DPIA form to the relevant HwH Senior Manager for storing. Senior Manager to save in DPIA folder on t-drive. Liaise with Senior Manger to make any changes required throughout the project lifecycle.

Responsibilities

The overall responsibility for ensuring compliance with the requirements of the related legislation in relation to performing data protection impact assessment activities at Healthwatch Hertfordshire rests with the Data Protection Officer.

All HwH staff that deal with personal data are responsible for processing this data in full compliance with the relevant Healthwatch Hertfordshire policies and procedures.

Record management

HwH employees to maintain and pass on all relevant documentation relating to this procedure to the appropriate Senior Manager (and/or the DPO when required).

Records will be kept for at least 5 years by the DPO and Senior Manager.

Appendix VI – Data Protection Impact Assessment (DPIA) Template

Project Title	
Organisation	
Date	
Author	
Authorising Officer	

Section One: In order to assess the need for a Data Protection Impact Assessment please answer the following questions:	
Are you collecting any new or personal data from people?	Yes/No
Will people have to give you their personal data as part of the planned activities?	Yes/No
Will you be sharing personal data with any organisations who haven't received it before?	Yes/No
Are you using personal data in a new way?	Yes/No
Will you be using new technology that may be regarded as being intrusive?	Yes/No
Will you be taking action against people as a result of your project?	Yes/No
Will any privacy concerns be raised such as cold calling?	Yes/No
Section Two: If you have answered yes to any of the questions above please describe the purpose of the proposed change, service or project, the lawful basis for processing the data under Article 6 of the GDPR and (where relevant) the lawful basis for processing special category personal data under Article 9.	

Section Three: Please describe what personal data will be collected, stored, used deleted and/or affected. Where this personal data will be obtained from. Who will have access, and whether recipients to whom personal data will be disclosed.
Section Four: Please list the relevant people and organisations that have been engaged to understand the potential privacy risks that may result as part of your planned work activity.
Section Five: Please list all identified privacy risks and the mitigation you are putting in place to minimise or resolve them.

Privacy risk	Privacy solution (mitigation measures)

Section Six: Please explain why you consider that it is necessary and proportionate to proceed with the proposal.	
Recommendation of the Data Protection Officer	
Sign Off:	
Accountable Officer: Approved: YES/NO Date:	

Appendix VII – Data Subject Access Request (DSAR) Procedure

Purpose

The General Data Protection Regulation (GDPR) details rights of access to 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.

This procedure applies to all Healthwatch Hertfordshire employees, including part-time, temporary, or contract employees, as well as volunteers that handle personal data.

Procedure

This procedure informs staff and volunteers of the process for supplying individuals with the right of access to personal data, and the right of access to staff and volunteer information under the GDPR specifically:

- All staff and volunteers need to be aware of their responsibilities to provide information when a data subject access request is received. A subject access request can be made to anyone within the organisation, and does not have to include the phrase 'subject access request' or Article 15 on the GDPR, as long as it is clear that the individual is asking for their own personal data.
- When a subject access request is received, it should immediately be reported to the Data Protection Officer to log and track each request via dpo@healthwatchhertfordshire.co.uk
- Requests can be initiated verbally but must ultimately be made in writing (using template form provided is desirable, but not mandatory)
- The statutory response time is one month.
- Requests should include the full name, date of birth and address of the person seeking access to their information. To comply with the GDPR, information relating to the individual must only be disclosed to them or someone with their written consent to receive it.
- No fee can be charged for initial DSAR for all types of records, whether manual or electronic format.

How should DSARs be processed after receiving

When a subject access request is received from a data subject, it should immediately be reported to the Data Protection Officer who will log and track each request.

If asked for information, The Data Protection will need to consider the following before deciding how to respond:

Under GDPR Articles 7(3), 12, 13, 15-22 data subjects have the following rights:

- to be informed;
- to access their own data;

- to rectification;
- to erasure (Right to be Forgotten);
- to restriction of processing;
- to be notified;
- to data portability;
- to object;
- to object to automated decision making.

The type of access provided and the possible fee charged is dependent on how the records are held.

If a request has already been complied with and an identical or similar request is received from the same individual a fee may be charged for the second request unless a reasonable interval has elapsed.

Requests

- Requests should include the full name, date of birth and address of the person seeking access to their information. To comply with the GDPR, information relating to the individual must only be disclosed to them or someone with their written consent to receive it.
- Before processing a request, the requestor's identity will be verified. Examples of suitable documentation include:
    - Valid Passport
    - Valid Identity Card
    - Valid Driving Licence
    - Birth Certificate along with some other proof of address e.g. a named utility bill (no longer than 3 months old)

Fees

No fee will be charged for providing information in response to a data subject access request, unless the request is 'manifestly unfounded or excessive', in particular because it is repetitive.
If Healthwatch Hertfordshire receives a request that is manifestly unfounded or excessive, it will charge a reasonable fee taking into account the administrative costs of responding to the request. Alternatively, Healthwatch Hertfordshire will be able to refuse to act on the request.

Subject access requests made by a representative or third party

Anyone with full mental capacity can authorise a representative/third party to help them make a data subject access request. Before disclosing any information, Healthwatch Hertfordshire must be satisfied that the third party has the authority to make the request on behalf of the requestor and that the appropriate authorisation to act on their behalf is included (see *Data Request Form*).

Complaints

If an individual is dissatisfied with the way Healthwatch Hertfordshire has dealt with their subject access request, they should be advised to invoke the Healthwatch Hertfordshire complaints

process. If they are still dissatisfied, they can complain to the Information Commissioners Office (IO) as the Data Protection Regulator in the UK.

Responsibilities

The overall responsibility for ensuring compliance with the requirements of the related legislation in relation to performing subject access rights at Healthwatch Hertfordshire rests with the Data Protection Officer.

All staff and volunteers that deal with personal data are responsible for processing this data in full compliance with the relevant Healthwatch Hertfordshire policies and procedures.

Records management

Staff and volunteers are required to maintain all records relevant to administering this procedure and pass this on to the Data Protection Officer.

Appendix VIII – Data Breach Notification Procedure

Purpose

This document outlines the procedure for handling a **Data Breach.** A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

The procedure applies to all employees, including part-time, temporary, or contract employees, volunteers as well as contractors that handle personal data across as part of working for Healthwatch Hertfordshire, and should be read in conjunction with the HWH Data Protection Policy, HWH Confidentiality Policy and the HWH Information Governance Policy.

Notification Procedure

Any staff member who suspects that a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data might have occurred, must **immediately** notify HWH's Data Protection Officer and provide a description of the circumstances. Notification of the incident should be be made via e-mail, however can be made by telephone, or in person. If notifying the DPO verbally, this should be followed up via email within 24 hours. The Operational Manager must also be informed, either at the same time by copying them into the email sent to the DPO, or with a follow up email if notifying the DPO verbally. The email to the Operational Manager should provide a description of the circumstances as well as the date you notified the DPO.

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 data breach notification procedure based on the criticality and quantity of the personal data involved. For severe personal data breaches, Healthwatch Hertfordshire's CEO will initiate and chair an emergency response team to coordinate and manage the personal data breach response.

If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Data Protection Regulator is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Art 3.2) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

Data breach notifications shall include the following information:

- The categories and approximate number of data subjects concerned;
- The categories and approximate number of personal data records concerned;

- The name and contact details of Healthwatch Hertfordshire's Data Protection Officer;
- The likely consequences of the breach;
- Details of the measures taken, or proposed to be taken, by Healthwatch Hertfordshire to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

Responsibilities

The overall responsibility for ensuring compliance with the requirements of the related legislation in relation to performing Healthwatch Hertfordshire activities at Healthwatch Hertfordshire rests with the Data Protection Officer.

All staff and volunteers that deal with personal data are responsible for processing this data in full compliance with the relevant Healthwatch Hertfordshire policies and procedures.

Records management

Staff must maintain suitable records and pass this on to the DPO and Operational Manager. All records relevant to administering this procedure will be maintained for a period of 5 years by the DPO and Operational Manager.

Appendix IX - 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.