Healthwatch North Tyneside policies and procedures

Data Protection

November 2025

1. Policy

Healthwatch North Tyneside (HWNT) collects and uses personal data to carry out its business and provide services. This Data Protection Policy sets out how HWNT will protect individuals' rights in relation to the storage, access, use and disclosure of their personal data, and defines standards to achieve compliance with current legislation.

The Data Protection Act 2018 and United Kingdom General Data Protection Regulation (UK GDPR) detail requirements that must be complied with to ensure that the rights and freedoms of living individuals are not compromised, and that all personal data is processed in a secure and appropriate manner. The legislation also stipulates that those who record and use personal information must be open about how the information is used and must follow good handling practices. This applies to the whole lifecycle of information, including the collection, use, disclosure, retention and destruction of data. HWNT is committed to fulfilling its obligations under this data protection legislation and has produced this policy to both assist staff, trustees and volunteers and to provide assurance to its customers.

2. Purpose

The purpose of this policy is to enable HWNT to:

- Comply with all legislation in respect of the personal data it holds about individuals.

- Protect HWNT clients, service users, staff and other individuals for whom HWNT deals with in order to conduct its business or provide services.

- Follow good practice.

3. Scope

This policy applies to all the personal data held by HWNT and includes manual/paper records, and personal data that is electronically processed by a computer or any other means. This policy applies to anyone accessing or using HWNT personal data held by HWNT in any form. It applies to HWNT, Partners, contractual third parties and agents including:

- Current, past and prospective employees
- Volunteers
- Trustees
- Contractors
- Suppliers
- Others with whom HWNT communicates

4. Applying the Policy

4.1 What is Personal Data

Under the UK GDPR personal data refers to any information relating to an identified or identifiable natural person (data subject) who can be identified, directly or indirectly, in particular by reference to an identifier such as:

- A name
- An identification number
- Location data
- Online identifier (IP address)
- Physical details
- Physiological details

- Genetic details
- Mental health
- Economic factors
- Cultural or social identity of natural persons

4.2 Special Category Data (Previously known as Sensitive Personal Data)

The following categories of personal data relate to more private matters of a data subject's life:

- Racial or Ethnic origin
- Political opinions
- Religious beliefs
- Trade Union membership
- Physical or mental health
- Sexual orientation or sex life
- Genetic data
- Biometric data

Information relating to criminal proceedings or convictions is also categorised in a similar fashion.

4.3 Data Protection Principles

There are seven key obligations in the UK GDPR. These principles do not provide hard and fast rules but embody the spirit of the general data protection regime. Compliance with these principles is fundamental to embedding good data protection and is key to HWNT compliance with the provisions of the UK GDPR.

General Data Protection Regulation Principles

Principle	Description
Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
Data minimisation	Personal Data shall be adequate, relevant, and limited only to what is necessary in relation to the purposes for which it is processed
Accuracy	Personal Data shall be accurate and where necessary kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified.
Storage limitation	Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary. Personal data may be stored for longer periods in so far as the said personal data will be processed only for • archiving purposes • in the public interest • scientific or historical research purposes

Integrity and confidentiality (security)	Personal data shall be processed in a manner that ensures appropriate security, including protection against accidental loss, destruction or damage.
Accountability Principle	Where HWNT is the data controller it shall be responsible for and be able to demonstrate compliance with all the above principles

Based upon the UK GDPR principles, HWNT will:

- Observe fully, conditions regarding the fair collection and use of personal information.
- Meet its obligations to specify the purpose for which information is used.
- Collect and process appropriate information, to the extent for which it is needed, to fulfil operational needs, or to comply with any legal requirements.
- Apply checks to determine the length of time that information is held.
- Take all appropriate security measures to safeguard personal information.
- Uphold the rights of data subjects and support them fully if they wish to exercise any of these rights.
- Ensure that all staff and volunteers handling personal information understand their responsibilities.
- Ensure that all staff and volunteers managing and handling personal information are appropriately trained.
- Ensure that all staff and volunteers managing and handling personal information are appropriately supervised.
- Ensure that methods of handling personal information are regularly reviewed and evaluated.
- Ensure that personal information is not transferred abroad without the appropriate safeguards.

4.4 Specific data use by HWNT

HWNT's work is based on gathering the views and experiences of people who live in the borough and ensuring that those views are taken into account by providers and commissioners of services. To do this HWNT will be party to, and record information which could be considered confidential and sensitive. HWNT will make every effort to store information from residents anonymously in keeping with its confidentiality policy. HWNT also keeps information relating to trustees, employees and volunteers which are also covered by data protection legislation.

HWNT uses personal data of its contacts for the following:

- Delivery of services and activities as outlined under part 5 of the Health & Social Care Act 2012.
- The general running and business of the charity.
- The ongoing management and delivery of services to individuals.
- Compliances with the law.
- Compliances with contractual obligations.

- Managing the employment of its staff and volunteers

Personal data must only be used for the purposes stated.

Children under the age of 13 are generally considered unable to give their consent to the processing of personal data. Consent must be sought from the person holding parental or guardianship responsibility over the child. However, in the event that a parent or guardian makes a subject access request, it is usually appropriate to respond to the child. In the event that this happens HWNT's Subject Access Guidance will be followed.

HWNT adopts 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 is processed by maintaining high IT security and ensuring personal information is maintained in locked cabinets.
- Prevent persons entitled to use a data processing system from accessing personal data beyond their needs and authorisations by restricting access.
- Ensure that personal data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation by transferring information securely.
- Ensure that personal data is protected against undesired destruction or loss.
- Ensure that personal data collected for different purposes is processed separately.
- Ensure that personal data is not kept longer than necessary

HWNT will maintain a register of the personal data HWNT holds, where it comes from, who we share it with and how long it will be kept.

4.5 Working with Third-Party Data Processors and Other data Controllers

We frequently work with third party data processors to collect, analyse, store and otherwise handle personal data for us. Third party data processors include contractors, consultants and suppliers. We work with third party providers for a variety of purposes, including but not limited to obtaining a service.

In all cases, we must ensure that the third party data processor is ready and able to collect, use and store the data in accordance with UK data protection standards and principles.

For these reasons, HWNT will only allow personal data to be processed on our behalf by a third-party data processor where:

- we have a valid business reason for the processing.
- the planning and design of the processing has been reviewed and approved in according with our Data Protection Impact Assessments.
- we have a written, signed contract with appropriate data protection clauses.
- we are satisfied that the third-party data processor has suitable staff, processes and systems to protect the data.

Where we collaborate on a research or evaluation project or wish to share personal data with another data controller, so they can use it for a common purpose or their own purpose, we will ensure that a data sharing agreement is in place.

Data sharing agreements can only be signed by data controllers and no partner is responsible for ensuring that the others are compliant with data protection legislation, however the agreement must contain a declaration by each party that they are compliant and have all appropriate policies and procedures in place.

Personal information sharing between partners must comply with the data protection principle of 'Purpose' stating that personal data shall be obtained only for one or more specified and lawful purposes and shall not be processed in a manner incompatible with that purpose. The lawful basis to be used to legitimise the sharing will be declared in the sharing agreement as well as the process by which information will be shared.

4.6 Data Privacy Impact Assessments (DPIA)

DPIAs are now mandatory in certain circumstances under the UK GDPR. A DPIA must be carried out for processing that is likely to result in a high risk to individuals. It is also good practice to carry out a DPIA for any major project that requires the processing of personal data. A DPIA must:

- Describe the nature, scope, context and purpose of the processing
- Assess necessity
- Identify and assess risks to individuals
- Identify additional measures to mitigate risks

The results of DPIAs should be reported either to the Director or the Board where any high risks are identified.

Should either the Director or the Board be uncertain about whether the high risks are outweighed by the benefits to the data subject, they will submit the DPIA to the Information Commissioner's Office. The decision made by the ICO will be final.

4.7 Consent

The UK GDPR sets a high standard for consent as a lawful basis for processing personal or special category data. Where processing is based on consent, HWNT is required to demonstrate that the data subject has consented to the processing of their personal data. Consent therefore requires either a positive opt-in process or a clearly written declaration, pre-ticked boxes or any other method of default approval cannot be used. The data subject has the right to withdraw their consent at any time where consent is the basis for processing personal data.

4.8 Data Subjects' Rights including Subject Access Requests (SARs)

Data subjects whose data is held by HWNT have the following rights over their personal data and have the right to access that data and any supplementary information about how their data is being processed, by making a subject access request (SAR).

Additional rights are:

- The right to be informed about how and why their personal data is processed
- The right to rectify their data
- The right to be forgotten – erasure of their data
- The right to restrict processing of their data
- The right to data portability
- The right to object to processing of their data
- The right to object to profiling, or automated decision making

These requests must be handled and responded to in a timely manner in line with the requirements of the UK GDPR. which determines that all requests to exercise rights should be dealt with within 30 days.

A SAR must be:

- Provided free of charge
- Answered without delay and within 30 days unless it is very complicated in which case the response time can be extended by up to two months.

All SARs will be managed and tracked by the Director.

HWNT has a procedure for complying with a SAR.

4.9 Training

Data protection training will be made available for all HWNT employees. Training will be mandatory for all staff and volunteers who process personal data. The training provided is aimed to ensure that all individuals understand their responsibilities for managing data in line with all legislation. Training materials must be kept up to date with all relevant UK data protection legislation and should be made available to staff, volunteers and trustees.

Initial training should take place within three months of joining HWNT and refresher training will be given at not greater than two yearly intervals.

5. Roles and Responsibilities

5.1 Senior Information Risk Owner (SIRO)

The SIRO has overall responsibility and accountability in all aspects of Data Protection. They are required to provide assurance that all risks are effectively managed and mitigated.

This role will be discharged by the Director.

5.2 Data Protection Officer (DPO) The DPOs role is:

- To inform and advise HWNT and its employees about the HWNT's obligations to comply with the UK GDPR and other data protection laws
- To monitor compliance with the UK GDPR and other data protection laws, along with HWNT's policies in relation to the protection of personal data, including the assignment of responsibilities, awareness training and training of staff involved in processing operations and conducting related audits
- Provide advice and monitor data impact assessments (DPIA)
- Co-operate with the Supervisory Authority – The ICO

- To be the first point of contact for the supervisory authorities and for individuals on issues relating to processing, including prior consultation where appropriate
- Perform their duties in an independent manner with due regard to the risk associated with processing of operations, considering the nature, scope, context and purposes of all data processing
- Escalate where appropriate to the CMB.

5.3 This role can be discharged by an employee of HWNT or an external practitioner. Our current DPO is Catherine Hunt of GDPR Charity Solutions. Information Asset Owners (IAOs, all staff) IAOs take responsibility for:

5.4 Ensuring the correct protection and handling arrangements for the information assets that they own.
Ensuring that the Data Protection Policy is communicated and implemented within their respective areas of responsibility, and for ensuring that any issues regarding resourcing, training, and compliance are escalated to the DPO and or the IGG

5.5 Information Asset Administrator (IAA)

This role is discharged by the Operations Coordinator.
The IAA takes responsibility for:

- Keeping the Asset Registers up to date
- Ensuring information handling procedures are managed
- Ensuring that personal information is not unlawfully exploited
- Acting as first port of call for any staff seeking advice related to data protection

5.6 Individuals supporting HWNT

All persons whether permanent, temporary, or voluntary are required to:

- Read and understand and accept any policies and procedures that relate to personal data that they may handle as part of their role
- Take responsibility for data protection and adhere to this policy and related procedures
- Attend training related to data protection
- Understand the main concepts of data protection related legislation
- Identify and report any risks that they identify in relations to the security of personal data to the Director.
- Assist their customers to understand their rights and HWNT's responsibilities regarding data protection
- Identify any SARs and follow the correct reporting procedure and escalation

6. Governance

6.1 The HWNT Board (the Board)

The Board should

- maintain oversight of the Information Governance Group (IGG)
- ensure that HWNT's approach is effective in terms of resources, commitment and execution of all matters related to Information Governance
- review and provide final approval for all Information Governance related policies

The Information Governance Group (IGG)

The IGG comprises the Director, Trustees (as agreed by the board) and usually the Operations Coordinator. The group will meet no less than twice each year. It is the role of the IGG to:

- Decide and/or recommend operational matters around all aspects of Information Governance
- Establish a Framework to embed best practice in all aspects of Information Governance
- Define the organisational policies in respect of data protection considering any legal and local authority requirements
- Provide regular reporting to the Board which should include any key risks relating to the HWNT's ability to demonstrate compliance to regulation/policies
- Provide an update on reported incidents of Personal Data Breaches, SARs, IGG actions, audit points and any other key points as agreed by the IGG members

6.2 Monitoring Compliance

Compliance with this policy and related standards will be monitored by the IGG. Ongoing monitoring and an action plan for improvements will be formulated by the IGG and communicated accordingly. Any disregard for this policy may be treated as misconduct and a serious breach may be treated as gross misconduct and will be subject to HWNT's disciplinary procedure. If you do not understand the implications of this policy or how it may apply to you, seek advice from the Director.

7. Guidance

Guidance on implementation of the Data Protection Act, and key data

protection - related documents are available on the Internet on the Information Commissioner's Office website Home | ICO This site should also be used to report any data breach if appropriate.

8. National Data Opt-out

From September 2021 it has been the duty of HWNT, as an adult social care provider for the local authority and the NHS, to comply with the National data opt-out enabling clients to opt out from the use of their data for anything other than their individual care and treatment.

If current uses or disclosures should have national data opt-outs applied, HWNT needs to:

- implement the technical solution as laid down by the NHS to enable us to check lists of NHS numbers against those with national data opt-outs registered
- have a process in place, when we get the results back, to ensure that we only use or disclose information for the returned list of NHS numbers, as any with national data opt-outs registered will have been removed

If we have no uses or disclosures which need to have national data opt-outs applied, we must still put procedures in place to assess future uses or disclosures against the national data opt-out operational policy guidance, and can choose to either:

- implement the technical solution in readiness, or
- be ready to implement it if needed for future data uses or disclosures

National data opt-outs apply to a disclosure when an organisation, for example a research body, confirms they have approval from the Confidentiality Advisory Group (CAG) for the disclosure of confidential patient information held by another organisation responsible for the data (the data controller) such as an NHS Trust, or in this case HWNT.

The CAG approval is also known as a section 251 approval and refers to section 251 of the National Health Service Act 2006 and its current Regulations, the Health Service (Control of Patient Information) Regulations 2002. The NHS Act 2006 and the Regulations enable the common law duty of confidentiality to be temporarily lifted so that confidential patient information can be disclosed without the data controller being in breach of the common law duty of confidentiality.

In practice, this means that the organisation responsible for the information (the data controller) can, if they wish, disclose the information to the data applicant, for example a research body, without being in breach of the common law duty of confidentiality.

It is only in these cases where opt-outs apply.

Following careful scrutiny of the disclosures of relevant personal data which are made by HWNT, it has been determined that that the organisation does not currently have data disclosures which require opt-outs to be applied.

HWNT has chosen to be ready to implement the technical solution if needed for future data uses or disclosures.

Compliance still requires that HWNT:

a. Ensures that there are procedures in place to apply the National data opt-out if at any time in the future this is required (only required if HWNT decides to be ready to implement)
b. Communicates the responsibilities of HWNT to employees, clients and partner organisations
c. Includes a statement on compliance with the National data opt-out on its website and in relevant privacy notices
d. Ensures that relevant printed materials on 'Your NHS Data Matters' are available in our public/communal spaces

e. Sets an official date for declaring compliance after ensuring that a., b., c. and d. are undertaken
f. Officially declares compliance

The official declaration of compliance was 31 July 2022.

Having due regard to ensuring that this is detailed in HWNT's relevant policies and procedures and that all employees are made aware of the requirement to comply and how this must be done, this means that HWNT is compliant with Information Standard DCB3058 – Compliance with national data opt-outs.

9. Publication of documents

HWNT, as a public authority under the Freedom of Information Act 2000 has a legal obligation to provide information through an approved publication scheme and in response to requests.

Under this scheme, this policy and privacy notices for clients will be on our website and where appropriate will be made publicly available upon request and within the organisation.

10. Policy Review

This policy will be reviewed as it is deemed appropriate, but in line with any new or changed legislation, regulations or business practices but no less frequently than every two years. Policy review will be undertaken by the Information Governance Group and presented to the Board for approval.

Document classification	Public	Document Reference	
Document category	Governance	Policy introduced	May 2016
Updated by	C Hunt, T Hindmarch, P Jones	Date last updated	November 2025
Approved by	HWNT Board	Date approved	December 2025
		Review date	December 2027