Data Protection Policy

CONTENTS

1 PURPOSE

This policy establishes an effective, accountable and transparent framework for ensuring compliance with the requirements of the Data Protection Act 2018 (DPA 2018), the UK General Data Protection Regulation (UK GDPR), the Digital Economy Act 2017, the Human Rights Act 1998 and the provisions of PECR, Safeguarding and any other relevant legislation.
The Chief Executive and Board will act within the frameworks advised by the Information Commissioner's Office, Department for Health and Healthwatch England.

2 SCOPE

This policy applies to all Healthwatch Rochdale employees and all third parties responsible for the processing of personal data on behalf of Healthwatch Rochdale services/entities. It applies to all personal data, regardless of whether it is in paper or electronic format and irrespective of who the data subject is (be they employees, clients or others). The information and guidelines in this policy apply to the whole community including staff, volunteers and board members.

3 POLICY STATEMENT

Healthwatch Rochdale is committed to conducting its business in accordance with all applicable data protection laws and regulations and in line with the highest standards of ethical conduct.

This policy sets forth the expected behaviours of Healthwatch Rochdale employees and third parties in relation to the collection, use, retention, transfer, disclosure and destruction of any personal data belonging to a Healthwatch Rochdale contact (i.e., the data subject). Personal data is any information (including opinions and intentions) which relates to an identified or identifiable natural person. Personal data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process personal data. An organisation that handles personal data and makes decisions about its use is known as a Data Controller. Healthwatch Rochdale is both a "data controller" and "data processor" under the data protection regulations. This is because we determine the purpose and the means of processing of personal data as well as carrying out the processing itself on the personal data relating to clients, staff, volunteers, board members, visitors and others. We also have a number of "sub-processors" (organisations who process data on our behalf) these include Clinical Commissioning Group, NHS England, Local Authority, Payroll, NHS Complaints, IT Provider, HR, Mail Chimp. We are responsible for the actions of these "sub-processors". A complete list of our sub-processors can be obtained from the DPO.

We are registered with the ICO both as a data controller and renew our registration annually or as otherwise legally required. A copy of our registration is displayed in the Office. The UK GDPR and DPA 2018 aim to give control to individuals over their personal data and to put the rights and freedoms of individuals at the heart of data processing. As a processor of personal data, we will:

- Clearly disclose when data is collected.
- Declare the lawful basis and purpose for data processing.
- State how long data is being retained, if it is being shared (and who with), and how/when it will be disposed of.

Healthwatch Rochdale holds and processes information (personal data) about its employees, clients and other individuals (data subjects) for a variety of purposes such as, the effective provision of and services, to record activities, to operate the payroll, and to enable correspondence and communications. We have a Legal Basis for processing each category of information and these are clearly articulated in our Privacy Policies and Notices.

Healthwatch Rochdale's leadership is fully committed to ensuring continued and effective implementation of this policy and expects all Healthwatch Rochdale employees and third parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

3.1. Governance

This policy meets the requirements of the UK GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO), the Information and Records Management Society (IRMS), Department for Health and Healthwatch England and follows the ICO's code of practice for subject access requests.

The Chief Executive and Board are committed to providing and maintaining a data environment that is safe. The management of data risks is established by allocating specific duties to key staff and by producing additional policies and arrangements as detailed in this document. This will include the production of:

- Privacy Notices.
- Acceptable use of IT policy.
- Data Breach Procedure
- Subject Access Procedure.
- Records Management and Retention Policies.
- A Record of Processing Activities.
- Other Information Security Policies as required.

This Policy sets out our obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by our staff, agents, contractors, or other parties working on our behalf. All those involved in processing data are responsible for assisting us in the achievement of our aims and objectives and will play a positive role in promoting a secure data processing environment where the rights and freedoms of the individual are protected

Roles and Responsibilities
This policy applies to all staff employed by Healthwatch Rochdale, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action. The Board recognises its overall responsibility for ensuring that Healthwatch Rochdale complies with its legal obligations.
Specific data protection responsibilities are given to the following staff:

Area of Responsibility	Name	Role
Overall Responsibility for Data and Data Protection	Kate Jones	CEO
Data Protection Board Member	Margaret Parker	Chair
Data Protection Officer	Sam	DPO
Data Input	Claire Birch	Information & Comms Coordinator
IT Support	Steve Billing	Hands On IT
Staff with Safeguarding Responsibilities	All Staff	CEO, Engagement & volunteer Manager Information & Comms Coordinator Community engagement project worker Operations Coordinator

*Supported by our external consultant Sam Alford of PPP Management LTD.

Data Protection Officer

?? acts as our Data Protection Officer and is supported by our external consultant as required. He is the designated lead for all Data Protection and IT Matters and is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. The Chief Executive will provide an annual report of their activities directly to the board and, where relevant, report to the board to provide advice and recommendations on data protection issues.

The Chief Executive is also the first point of contact for individuals whose data we process, and for the ICO.

Full details of the Chief Executive's responsibilities are set out in their job description, and these include the following data protection responsibilities:

- Briefing the board on Data Protection issues.
- Reviewing Data Protection and related policies.
- Advising other staff on Data Protection issues.
- Ensuring that Data Protection induction and training takes place.
- Handling subject access requests.
- Approving unusual or controversial disclosures of personal data.
- Ensuring contracts with Data Processors have appropriate data protection clauses.
- Electronic security.
- Approving data protection-related statements on publicity materials and letters.

All Staff and Volunteers

Each member of staff and volunteer at Healthwatch Rochdale who handles personal data will comply with the organisation's operational procedures for handling personal data (including induction and training) to ensure that good Data Protection practice is established and followed.

All staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work.

Significant breaches of this policy will be handled under Healthwatch Rochdale's disciplinary procedures.

It is the responsibility of every member of staff and volunteer to maintain the quality of the data that Healthwatch Rochdale processes and to comply with UK GDPR and the DPA 2018. Anyone who collects data, enters, extracts or analyses data on our Information Systems should be aware of how their job contributes to the organisation's function and the need to ensure the safety and accuracy of the data that they process. Personal data processed by our employees shall:

- Be kept for no longer than it is required for the purpose for which it was originally collected and thereafter securely disposed of.
- Be kept up to date and accurate as far as is reasonable.
- Be processed only where there is a lawful purpose.
- Not be used for purposes other than that for which it was collected (unless consent is obtained).

Any questions or concerns about the interpretation or operation of this policy should be taken up with the DPO.

Staff are responsible for:

- Collecting, storing and processing all personal data in accordance with this policy.
- Ensuring that any personal data, which they hold or process, is kept securely, whether they are in the office or working from home.
- Irrespective of where they are. Ensuring that personal data is not disclosed orally or in writing or otherwise to any unauthorised third party, and that every reasonable effort is made to see that personal data is not disclosed accidentally.

- Informing the organisation of any changes to their own personal data, such as a change of address.
- Making sure that all third-party requests for access to personal data, including those from the police, are directed via the DPO.
- Contacting the Chief Executive in the following circumstances:
  - If there has been a data breach.
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way.
  - If they have any concerns that this policy is not being followed.
  - If they need help with any contracts or sharing personal data with third parties.
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK.
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.

Staff should be particularly aware of how a lapse on their part could adversely affect our reputation, incur financial penalties from the ICO or affect performance or service delivery. In extreme circumstances lapses can have a negative impact on the allocation of funding. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, access to facilities being withdrawn, or even to a criminal prosecution. Unauthorised disclosure is a disciplinary matter. If in any doubt consult the Chief Executive.

In addition to their responsibilities as data users, all staff have additional responsibilities regarding the operation of this policy, which are:

- To inform the board if they believe the Information Commissioner should be notified about any processing of personal data.
- Obtain specific informed consent from data subjects where appropriate to process personal data (e.g. consent for marketing photography).
- Provide any personal data required by the DPO in response to a subject access request in a timely manner.
- Maintain the security of, and access to, personal data within their scope.

3.1.2.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 must go through an approval process before continuing. Each Healthwatch Rochdale service/entity must ensure that a Data Protection Impact Assessment (DPIA) is conducted, in cooperation with the Data Protection Officer, for all new and/or revised systems or processes for which it has responsibility. The subsequent findings of the DPIA must then be submitted to the CO for review and approval. Where applicable, the Information Technology (IT) department (or outsourced IT provider), as part of its IT system and application design review process, will cooperate with the Data Protection Officer to assess the impact of any new technology uses on the security of personal data.

3.1.3.Compliance Monitoring

To confirm that an adequate level of compliance that is being achieved by all Healthwatch Rochdale services/entities in relation to this policy, the Data Protection Officer will carry out an annual data protection compliance audit for all such services/entities. Each audit will, as a minimum, assess:

- Compliance with policy in relation to the protection of personal data, including:

- The assignment of responsibilities.
  - ✓ Raising awareness.
  - ✓ Training of employees.
- The effectiveness of data protection related operational practices, including:
  - ✓ Data subject rights.
  - ✓ Personal data transfers.
  - ✓ Personal data incident management.
  - ✓ Personal data complaints handling.
  - ✓ The level of understanding of data protection policies and privacy notices.
  - ✓ The currency of data protection policies and privacy notices.
  - ✓ The accuracy of personal data being stored.
  - ✓ The conformity of data processor activities.
  - ✓ The adequacy of procedures for redressing poor compliance and personal data breaches. The Data Protection Officer, in cooperation with key business stakeholders from each Healthwatch Rochdale service/entity, will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame. Any major deficiencies and good practice identified will be reported to, monitored and shared by the Healthwatch Rochdale CO.

3.2. Data Protection Principles

Healthwatch Rochdale has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of personal data:

Principle 1: Lawfulness, Fairness and Transparency. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. This means, Healthwatch Rochdale must tell the data subject what processing will occur (transparency), the processing must match the description given to the data subject (fairness), and it must be for one of the purposes specified in the applicable data protection regulation (lawfulness).

Principle 2: 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. This means Healthwatch Rochdale must specify exactly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.

Principle 3: Data Minimisation. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means Healthwatch Rochdale must not store any personal data beyond what is strictly required.

Principle 4: Accuracy. Personal data shall be accurate and, kept up to date. This means Healthwatch Rochdale must have in place processes for identifying and addressing out-of-date, incorrect and redundant personal data.

Principle 5: Storage Limitation. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. This means Healthwatch Rochdale must, wherever possible, store personal data in a way that limits or prevents identification of the data subject.

Principle 6: Integrity & Confidentiality. Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful

processing, and against accidental loss, destruction or damage. Healthwatch Rochdale must use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times. Further reference the HWR Confidentiality Policy.

Principle 7: Accountability. The Data Controller shall be responsible for and be able to demonstrate compliance. This means Healthwatch Rochdale must demonstrate that the six data protection principles (outlined above) are met for all personal data for which it is responsible.

3.3. Data collection

Lawfulness, Fairness and Transparency

All processing of personal data which is undertaken by data users in the course of their employment must be in compliance with the principles above. Healthwatch Rochdale will process personal data under the following legal reasons:

- Consent: the individual has given clear consent for us to process their personal data for a specific purpose.
- Contract: the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.
- Legal obligation: the processing is necessary in order to comply with the law (not including contractual obligations).
- Vital interests: the processing is necessary to protect someone's life.
- Legitimate interests: we use this as our lawful basis where the processing is necessary for our legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Limitation, Minimisation and Accuracy
We only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer require the personal data that they hold, they must ensure it is deleted or anonymised. This will be done in accordance with our Data Retention Schedule and Record of Processing Activities.

3.3.1. Data Sources

Personal data should be collected only from the data subject unless one of the following apply:

- The nature of the business purpose necessitates collection of the personal data from other persons or bodies.
- 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.

If personal data is collected from someone other than the data subject, the data subject must be informed of the collection unless one of the following apply:

- 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.

Where it has been determined that notification to a data subject is required, notification should occur promptly, but in no case 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
- At the time of disclosure if disclosed to another recipient.

3.3.2. Data subject consent

Healthwatch Rochdale will obtain personal data only by lawful and fair means and, where appropriate with the knowledge and consent of the individual concerned. Where we rely on consent for processing this will be clearly articulated at the time of data collection. Consent will be requested on every occasion where we wish to use personal data for a reason other than that for which it was originally collected. Consent may be given in written or verbal forms and in all cases, it will be documented on the database that consent has been given.

Information about clients will only be made public with their consent. (This includes photographs). 'Sensitive' data about clients (including health information) will be held only with the knowledge and consent of the individual.

If we offer online services to a child, we will get parental consent where appropriate.

All Data Subjects will be given the opportunity to opt out of their data being used in particular ways, such as the right to opt out of direct marketing (see below).

Healthwatch Rochdale acknowledges that, once given, consent can be withdrawn.

Data subject Notification

Healthwatch Rochdale service/entity will, when required by applicable law, contract, or where it considers that it is reasonably appropriate to do so, provide data subjects with information as to the purpose of the processing of their personal data. 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, in a manner that draws attention to them, unless one of the following apply:

- The data subject already has the information.
- A legal exemption applies to the requirements for disclosure and/or consent. The disclosures may be given orally, electronically or in writing. If given orally, the person making the disclosures should use a suitable script or form approved in advance by the Data Protection Officer. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

3.3.3. External Privacy Notices

external website provided by Healthwatch Rochdale will include an online 'Privacy Notice' and an online 'Cookie Notice' fulfilling the requirements of applicable law.

3.4. Data Use

3.4.1. Data processing

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

- The general running and business administration of Healthwatch Rochdale
- To provide services to Healthwatch Rochdale's stakeholders.
- The ongoing administration and management of customer services.

The use of a contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within a contact's expectations that their details will be used by Healthwatch Rochdale to respond to a contact request for information about the products and services on offer. However, it will not be within their reasonable expectations that Healthwatch Rochdale would then provide their details to third parties for marketing purposes.

Healthwatch Rochdale will process personal data in accordance with all applicable laws and applicable contractual obligations. More specifically, Healthwatch Rochdale will not process personal data unless at least one of the following requirements are 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 or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, in particular where the data subject is a child).

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, Healthwatch Rochdale 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 context in which the personal data has been collected, in particular regarding the relationship between data subject and the Data Controller.
- 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.

3.4.2.Special Categories of Data

We may from time-to-time process sensitive personal data particularly medical data, ethnicity, religion and sex in relation to our clients and employees. This data will only be processed where we have a Legal basis and a separate condition for processing this special category data (e.g. vital interests). This will only be processed 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 natural 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.

In any situation where special categories of data are to be processed, prior approval must be obtained from the Data Protection Officer, and the basis for the processing clearly recorded with the personal data in question. Where special categories of data are being processed, Healthwatch Rochdale will adopt additional protection measures.

3.4.3.Children's Data

Children under the age of 14 are unable to consent to the processing of personal data for information society services (any service normally provided for payment, by electronic means and at the individual request of a recipient of services). 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.

3.4.4.Data Quality

Healthwatch Rochdale 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 Healthwatch Rochdale 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, insofar as:
    - ✓ 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.

3.4.5.Profiling & Automated Decision Making

Healthwatch Rochdale will only engage in profiling and automated decision-making where it is necessary to enter into, or to perform, a contract with the data subject or where it is authorised by law. Where Healthwatch Rochdale service/entity 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. Each Healthwatch Rochdale must also ensure that all profiling and automated decision-making relating to a data subject is based on accurate data.

3.4.6. Digital Marketing

As a general rule Healthwatch Rochdale will not send promotional or direct marketing material to an Healthwatch Rochdale Contact through digital channels such as mobile phones, email and the Internet, without first obtaining their consent. Any Healthwatch Rochdale wishing to carry out a digital marketing campaign without obtaining prior Consent from the data subject must first have it approved by the Data Protection Officer. Where personal data processing is approved for digital marketing purposes, the data subject must 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. If the data subject puts forward an objection, digital marketing related processing of their personal data must cease immediately, and their details should be kept on a suppression list with a record of their opt-out decision, rather than being completely deleted. It should be noted that where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain an indication of Consent to carry out digital marketing to individuals provided that they are given the opportunity to opt-out.

3.5. Data Retention

To ensure fair processing, personal data will not be retained by 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 Healthwatch Rochdale need to retain personal data is set out in Healthwatch Rochdale '*Data Retention Policy*'. 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 should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

3.6. Security of Personal Data

Healthwatch Rochdale 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.
- 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

Any recorded information on clients, volunteers and staff will be:

Kept in locked cabinets

Protected by the use of passwords if kept on computer

Destroyed confidentially if it is no longer needed

Access to information on the main database is controlled by a password and only those needing access are given the password. Staff and volunteers should be careful about information that is displayed on their computer screen and make efforts to ensure that no unauthorised person can view the data when it is on display.

Notes regarding personal data of clients should be shredded or destroyed.

In Addition:

Encryption software will be used to protect portable devices and removable media.

Papers containing confidential personal data must not be left out in the office pinned to notice/display boards, or left anywhere else where there is general access.

Complex Passwords (e.g. 3 random words) should be at least 8 characters long containing letters and numbers.

Where this is permitted any use of personal devices should follow the same security procedures as for Healthwatch Rochdale-owned equipment.

Where personal information needs to be taken off site, staff must sign it in and out from the office.

Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

3.7. Data subject Requests

An individual who wishes to make a "Subject Access Request" (SAR) to obtain a copy of the personal data that we process about them may make their request to any member of staff in any format. If possible individuals should be requested to complete our "Subject Access Request Form" and send it to the Chief Executive.

Subject access requests should include the name, contact details, address (email and correspondence) of the individual making the request together with details of the information requested. If the request is made verbally then the staff member to whom the request is made should take sufficient notes to answer the request. A log of all subject access requests should be kept.

On receipt of a Subject Access Request Healthwatch Rochdale is required to respond within 30 days. Therefore staff who receive a subject access request must immediately forward the matter to the Chief Executive.

The information that will be provide under a subject access request will include an explanation of any internal codes contained within it. The data supplied will, in principle, be all that is held at the time that the request is made, although the law permits routine amendments and deletions of data to continue between the time of the request and the time of the reply. We will not make a charge for such information.

The information that data subjects will receive includes:

Confirmation that their personal data is being processed.

A copy of the data (routinely provided as a hard copy).

The purpose for which the data is processed (contained in our Privacy Documents).

The categories of the personal data concerned (contained in our Privacy Documents).

Who the data has been, or will be, shared with (contained in our Privacy Documents).

How long the data will be stored for, or the criteria used to determine this period.

The source of the data, if it was not the individual making the request.

Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Our Subject Access Request Flow Chart is attached to this Policy and displayed on the wall of the office.

If the data subject has reason to believe that we have not dealt correctly with their access request, the matter should be taken up in the first instance with the DPO. If the data subject is unsatisfied after discussion with the Data Protection Officer, they should contact the Information Commissioner who is officially appointed to consider such complaints. The address is: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Alternatively they may fill in the online form at https://ico.org.uk/make-a-complaint/.

Children and Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or to have given their consent. Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request.

Responding To Subject Access Requests

Prior to responding to requests, we:

May ask the individual to provide 2 forms of identification (or identify themselves from information we hold about them).

May contact the individual via phone to confirm the details of the request.

Healthwatch Rochdale will:

Provide the information free of charge.

Respond without delay and within 1 month of receipt of the request.

We may tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

We will not disclose information if it:

Is contained in adoption or parental order records.

Is given to a court in proceedings concerning the child.

Might cause serious harm to the physical or mental health of the client or another individual.

Would reveal that the individual is at risk of abuse, where the disclosure of that information would not be in the client's best interests.

Refusing Subject Access Requests

In accordance with the regulations Healthwatch Rochdale reserves the right to reject repeated or vexatious requests where a reasonable period has not elapsed between requests and may charge for large volumes of documents. A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

3.8. Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that personal data be shared without the knowledge or consent of a data subject. This is the case where the disclosure of the personal data is necessary for any of the following purposes:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of a tax or duty.
- By the order of a court or by any rule of law.

If Healthwatch Rochdale processes personal data for one of these purposes, then it may apply an exception to the processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question. Healthwatch Rochdale receives a request from a court or any regulatory or law enforcement authority for information relating to an Healthwatch Rochdale contact, you must immediately notify the Data Protection Officer who will provide comprehensive guidance and assistance.

3.9. Data Protection Training

All Healthwatch Rochdale employees and volunteers that have access to personal data will have their responsibilities under this policy outlined to them as part of their staff or volunteer induction training. In addition, Healthwatch Rochdale will facilitate regular Data Protection training and procedural guidance for their staff and volunteers.

3.10. Data Transfers

Where we transfer personal data to a country or territory outside the UK, we will do so in accordance with data protection law.

Disclosure Outside The UK

We do not routinely transfer personal data outside the UK.

3.11. 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 a reasonable period. If the issue cannot be resolved through consultation between the data subject and the Data Protection Officer, then the data subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Data Protection Authority within the applicable jurisdiction.

3.12. 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. Notification of the incident can be made via e-mail, by calling, or by using the independent whistleblowing line 0303 123 1113 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. For severe personal data breaches, Healthwatch Rochdale will initiate an emergency response team to coordinate and manage the personal data breach response.

4 ROLES AND RESPONSIBILITIES

4.1 Implementation

The CEO must ensure that all Healthwatch Rochdale employees responsible for the processing of personal data are aware of and comply with the contents of this policy. In addition, Healthwatch Rochdale 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 must be obtained from all third parties, whether companies or individuals, prior to granting them access to personal data controlled by Healthwatch Rochdale.

4.2 Support, Advice and Communication

For advice and support in relation to this policy, please contact the Data Protection Officer on 01706 249 575 or send emails for the attention of the DPO to info@healthwatchrochdale.org.uk

5 REVIEW

This policy will be reviewed by the Data Protection Officer every three years unless there are any changes to regulations or legislation that would enable a review earlier.

6 RECORDS MANAGEMENT

Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognised Healthwatch Rochdale recordkeeping system.

All records relevant to administering this policy and procedure will be maintained for a period of 5 years.

7 TERMS AND DEFINITIONS

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 also addresses the export of personal data outside the EU.

Data Controller: the entity that determines the purposes, conditions and means of the processing of personal data.

Data Processor: the entity that processes data on behalf of the Data Controller.

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.

Data Protection Officer (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR.

Data subject: a natural person whose personal data is processed by a controller or processor.

personal data: any information related to a natural person or 'data subject', that can be used to directly or indirectly identify the person.

Privacy Impact Assessment: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data.

Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

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.