Healthwatch Richmond

Information Security & Governance Policy

Version: 1

Mike Derry May 2018

# Introduction

## What is information governance?

Information Governance is the system of controls (policies, processes, systems etc.) by which an organisation ensures that it meets its legal, policy and moral obligations in relation to the processing of information.

## Importance of information governance

Healthwatch Richmond holds and has access to sensitive information including the experiences of people who use services, correspondence with providers of care and their commissioners and regulators; commercially sensitive information, information from strategic partners about regulatory activity and other actions to protect people from harm and improve the quality of services.

Loss, misuse or mishandling of this information creates a direct risk to the privacy, dignity, rights and welfare of people who use services and may significantly damage the effectiveness of Healthwatch Richmond. It is particularly important to maintain public trust in the confidentiality and security of their personal information within the wider health and social care system. Loss of this trust may significantly impact upon the effectiveness of the health and social care sectors.

## Information Governance Framework and key roles

Healthwatch Richmond is part of Richmond Health Voices, a company limited by guarantee and registered charity. The Data Controller for the purposes of Healthwatch Richmond is the London Borough of Richmond upon Thames. The data Controller will appoint a data Protection Officer

As the Data Controller, Healthwatch Richmond will consult London Borough or Richmond upon Thames where there are significant variations in our practices that require decision making on matters of information management, information security, information risk management, legal compliance with information law, information sharing and the organisation’s statutory responsibilities under the Freedom of Information Act 2000, the Data Protection Act 1998, and other relevant legislation.

# Confidentiality

## Importance of confidentiality.

Some information held by Healthwatch Richmond carries the risk of adverse or damaging effects if disclosed. Most obviously, private information about individual people carries the risk of affecting their privacy, dignity, safety or welfare if disclosed. The handling of this type of information is covered in *“Using personal data and confidential personal information”*, page 6 of this policy.

However, it is important to remember that other types of information may be confidential in nature too:

* Releasing information about a care provider may have a significant commercial impact upon their business.
* Information about planned or ongoing regulatory activity could prejudice the effectiveness of that activity.
* Information about local or national policy development or the management of Healthwatch Richmond or its stakeholders may pre-empt official announcements with damaging effect.

Whenever handling information, you should be mindful of whether the information is confidential in nature. Where appropriate, confidential information should be marked as such, and should always be handled with care.

We are still able to collect, use and share confidential information, but we should only do so with appropriate consideration, and where we are satisfied that our actions are lawful and in the public interest.

## Legal requirements

In some cases, Healthwatch Richmond will be covered by legal requirements of confidentiality. Our legal responsibility to protect information about people is covered in *“Using personal data and confidential personal information”*, page 6. Where Healthwatch Richmond has received information of a confidential nature (i.e. where disclosure has the potential to cause some damage or harm) in circumstances where it is reasonable to expect that we would protect that confidentiality (whether or not this has been explicitly agreed), we will be subject to the common law duty of confidentiality.

Whether there is a specific prohibition on disclosure or where the general common law duty of confidentiality applies, we may still have a legal basis to disclose information – but we must still exercise care in protecting the information and making these decisions.

This is covered further in, *“Information Sharing”*, page 9 of this policy.

# Knowledge and Information Management

## Importance of records management

Records provide vital evidence of business decisions, activities and transactions. They are also essential in ensuring that Healthwatch Richmond meets legislative and regulatory requirements.

The key benefits for supporting Healthwatch Richmond in this are that records are:

* Captured and stored in the right place.
* Authentic so are confident that records are accurate.
* Accessible in a timely way, by those who need or have a right to see them.
* Protected from unauthorised deletion, changes or access.
* Disposed of appropriately once they are no longer required.

Primary records should be:

* Held in electronic format on our secure drive (or in the appropriate a paper filing systems for HR and financial records)
* Permissions to view and edit should be given to appropriate personnel (i.e. those who may have a legitimate need to access them in your absence), or restricted from those who should not have access to them
* Named and filed in a logical and consistent manner

## E-mail

Each member of staff is assigned an email account. This is not to be used as the primary storage location for records.

All records required for business purposes must be held in on the shared drive to ensure that they remain accessible.

## Retention of records

All records used, received or created by Healthwatch Richmond have a retention period assigned that meets legislative and business requirements.

Once this period ends, records must be either transferred for permanent storage or destroyed in a way appropriate to their content and storage format. This applies to all records whether electronic or physical (such as paper records).

|  |
| --- |
| **Retention of Records in Healthwatch Richmond** |
| **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. | 1 year (This is in case there is a query regarding an entry on the database) |
| 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.  |
| Record of Concern Forms (ROCA) |
| All ROCAs and related information should be kept for 10 years. If the record relates to children and young people the record must be kept till they are 21 years old before destroying. |
| **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 |
| Membership records  | 20 years from commencement of membership 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. |

## Accessing records

For access to restricted areas staff must obtain authorisation from the Asset Owner.

Whether restricted or not, you must only access Healthwatch Richmond’s records as authorised and required for the exercise of your role.

# Information Security

Records stored on the Drive are protected by encryption and 2 sign in security with passwords having to exceed a minimum level of security.

Passwords protect the other systems that we use and these should always have comparative levels of security where possible.

The loss of any device that has been used to access this system or used for 2-step sign in must be reported immediately to the Chief Officer so that the system can be secured.

Logs of activity are made on all systems where possible and any unusual or unexpected activity must be reported to the Chief Officer who will secure the systems by resetting the passwords.

In the absence of the Chief Officer you must make every attempt to reset passwords of accounts that may have been compromised.

Our IT contractors can be contacted to provide assistance if required.

# Using personal data and confidential personal information

## What is personal data

Personal data is defined under section 1 of the Data Protection Act 1998, it is information that relates to and identifies a living person, either on its own or when combined with other information we hold (or which is likely to come into our possession). Some personal data - such as information about a person’s ethnicity, religion, sexuality or sexual life, trade union membership, physical or mental health, or about alleged offences or prosecution – is defined as ‘sensitive personal data’ and is subject to greater legal protection.

## What is confidential personal information

Confidential personal information is defined under section 76 of the Health and Social Care Act 2008. It is personal data that has been obtained by Healthwatch Richmond in circumstances requiring it to be held in confidence. This could mean that there was an explicit agreement of confidentiality when information was provided to Healthwatch, or that a reasonable person would have considered that a duty of confidentiality was implied.

# Legal requirements and obligations

The Data Protection Act provides a set of Principles that must be followed when ‘processing’ (holding, obtaining, handling, using, sharing, altering, disposing of) personal data. The Health and Social Care Act 2008 creates a specific offence of disclosing confidential personal information except in defined circumstances.

## Fair processing

The most fundamental requirement of Data Protection compliance is ‘fair processing’. A key element of fair processing is a ‘no surprises’ approach where people are informed of who has their personal data, how they will use it and why. Processing someone’s personal data in a way that would be a surprise to a reasonable person is unlikely to be fair, and would therefore be unlawful. This creates an obligation to tell people, at the point where you collect their information, how and why you will use it. If there are elements of your intended use that are optional, the person should be told this and given an easy way to exercise choice. Where personal data is being collected via a third party, reasonable steps should be taken to communicate this information back to the ‘data subject’.

## Lawful processing

Processing of personal data must also be ‘lawful’. This requires that all of the Data Protection Principles must be met, the rights of individuals under the Act (e.g. the right to see what information we hold about them, to correct inaccurate information, and the right to object to the processing of information in ways which are damaging to them) must be complied with, and we must process personal data in accordance with other laws (such as the Human Rights Act 1998, which requires that any intrusion upon personal privacy must be justified and proportionate).

## Conditions for processing personal data

Personal data may only be processed where a condition under schedule 2 of the DPA is met. Sensitive personal data (information about a person’s racial or ethnic origin, political opinions, religious (or similar) beliefs, trade union membership, physical or mental health, sexual life, or relating to offences, alleged offences or prosecution) may only be processed where a condition under schedule 3 of the DPA is also met.

Our [Data Asset Register](https://www.healthwatchrichmond.co.uk/information-asset-register) sets out the lawful basis for our processing of data.

## Necessity Test

The necessity test is the decision making process designed to assist in reaching lawful decisions on obtaining, using and sharing confidential personal information/data.

The person considering the disclosure should understand what ‘legitimate purpose’ they are seeking to achieve by the proposed disclosure.

They should satisfy themselves that the intended action will be fair and meet a schedule 2 (and, for sensitive personal data, also a schedule 3) condition.

Then they should consider the two-step test:

STEP 1: Is the disclosure a necessary step in achieving this outcome?

If the outcome could reasonably be achieved, in an efficient and effective manner and within the available resources, by other means, then personal data should not be shared. For example, could anonymised or aggregated data be used instead? This step should include consideration of whether the minimum personal data required to achieve the purpose is being shared. We should not share more personal data than necessary.

STEP 2: Is the proposed disclosure proportionate?

Consideration should be given here to the likely impact upon the privacy and interests of the data subject (including any objections they have raised) and these should be balanced against the anticipated public interest to be served by disclosure.

In short, having considered the necessity test, the person should be satisfied that they would be able to explain and justify their actions if challenged.

## Anonymisation and pseudonymisation

Wherever possible, anonymised or pseudonomised data should be used instead of personal data / confidential personal information. Data of this type can be more freely used or shared, and its use minimises the risk to the privacy and dignity of individuals.

Anonymised data is information from which it is not possible to identify individuals – for example, aggregated data showing statistical information about large numbers of people.

Pseudonymised data is information where the identities of individuals are concealed, but where re-identification is possible – for example, narrative information about a person’s care where their name is replaced with a pseudonym such as ‘patient A’.

Care should be taken as simply removing names, addresses etc. does not always guarantee that individuals cannot be identified.

Advice should be sought if in doubt.

## Authorisation to use PD/CPI and PIA

When considering new ways of using information – for example, planning the introduction of new systems, processes or policies – consideration should be given as to whether the proposed changes will involve changes to the way in which personal data or other confidential information will be obtained, used, stored or shared.

Where this is likely to be the case, appropriate authorisation must be sought from the Chief Officer in the first instance and if necessary from the DPO appointed by London Borough if Richmond upon Thames.

Privacy impact assessments are a structured way to assess the likely risks to personal privacy arising from changes, and for putting appropriate measures in place to mitigate those risks.

# Information Sharing

## Why we share information

The appropriate and effective sharing of information can play a vital role in protecting people from harm, improving services and in facilitating the exercise of strategic partners such as Richmond CCG, Richmond Council, Healthwatch England and CQC.

## Legal requirements

Personal data must only be shared where it is fair and lawful to do so.

Consideration should be given to whether data subjects would reasonably have expected their personal data to be shared by Healthwatch Richmond. In making this assessment, consideration should be given to any information previously provided to the data subject, any discussions with them, any indication they have given about how they wish or expect their data to be used, and publicly available information materials about uses of information.

Consideration may also be given to what information the data subject themselves has put into the public domain. Where they have made their own information public, then it is more likely to be fair to share that information – however, care should be taken in differentiating between information that the person has made public and information that they may reasonably expect to be maintained in confidence.

Where it is considered that the data subject would not reasonably expect their information to be shared, they should be contacted and their consent sought for the disclosure.

Where it is not appropriate or possible to do this, consideration should be given to whether there is another lawful basis which would permit a disclosure which would otherwise be unfair. The only exemptions which are likely to apply are:

* Where the disclosure is necessary for the prevention or detection of crime, or the prosecution of offenders. This may apply where the disclosure is considered to be necessary for regulators to investigate allegations of serious breaches of regulations or offences relating to registered activities.
* Disclosures which are necessary in connection with legal proceedings, proposed legal proceedings, or for the purpose of obtaining legal advice.

In other cases, exceptional circumstances may permit the sharing of information. Most notably, a disclosure that is considered necessary to protect a person from significant risk of serious harm would be permissible.

## Making decisions to share information

Decisions on sharing personal data should be made using the ‘necessity test’ (see above).

Confidential medical information about identifiable people should only be shared without consent where there is a very high public interest in doing so.

Decisions on sharing other kinds of information should take into account the potential impact of disclosure and the possible prejudice or damage that may be caused.

## Authorisation

You should only share information if you are authorised to do so as part of your role, or where you have authorisation to do so from the Chief officer or DPO.

# Access to Information

Into to FOIA, EIR and DPA SARs

Healthwatch Richmond as a Data Processor to the London Borough of Richmond upon Thames must comply with the terms of its contract with the London Borough of Richmond upon Thames with regard to requests for data under the Freedom of Information Act, or Data Protection Act.

## What to do if you receive a request

If you receive a request for information whether written or otherwise it should be passed immediately to the appointed person at the London Borough of Richmond upon Thames.

## What to do if asked to support a request

London Borough of Richmond upon Thames may request your help in handling a request for information. You may be asked to locate and extract requested information, or to provide advice on the background of the information or potential impact of disclosure (to help consider possible exemptions).

It is important to provide the requested assistance in a timely manner to help ensure compliance with these statutory requirements.

## Sign-off and decision making

All responses to requests for information regarding Healthwatch Richmond are signed off by the London Borough of Richmond upon Thames and will be disclosed by them via their internal processes.

## Disclosure of information about you

You should be aware that information about your role, professional decisions and actions may be disclosed in response to requests. Generally speaking, information of a personal nature will not be disclosed.

The more senior and public facing your role, the more likely it is that information about you may have to be disclosed. Where potentially sensitive or confidential information about you is being considered for disclosure, you will be consulted.

# Support and guidance

In the first instance approach the Chief Officer. In his/her absence contact an Officer of the Board (Chair, Healthwatch Committee Chair, Audit Committee Chair or Treasurer).

The DPO at London Borough of Richmond upon Thames can be approached for support with the authorisation of the above.