HW Kingston Information Security and Governance Policy and Procedures

1. Scope

This policy applies to

Employees	x
Contractors	
Volunteers	x
Partners	
Suppliers	
Consultants	

Unless otherwise stated, this policy and procedure is non-contractual, does not form part of any contract of employment, and may be adapted or amended at any time by the Board of Trustees.

2. 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.

3. Importance of information governance

Healthwatch Kingston 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 Kingston. 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.

4. Information Governance Framework and key roles

Healthwatch Kingston is a company limited by guarantee and registered charity. The Data Controller for the purposes of Healthwatch Kingston is the London Borough of Kingston upon Thames. The Data Controller will appoint a Data Protection Officer.

Healthwatch Kingston is the Data Controller for the purposes of Healthwatch Kingston, and they have appointed a Data Protection Officer.

The Royal Borough of Kingston upon Thames contract Healthwatch Kingston to deliver service. As the Data Controller, Healthwatch Kingston will consult the Royal Borough of Kingston 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 2018, and other relevant legislation. RBK has created a variation of contracts with Healthwatch Kingston, to include GDPR compliance and Data Processing agreement to ensure all cloud data back-up is UK compliant.

5. Confidentiality

Importance of confidentiality
Some information held by Healthwatch Kingston 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 section 15 'Using personal data and confidential personal information.

If there is a Data Breach this must be reported to the Chief Executive Officer and the DPO immediately. If the Data Breach is classified as serious by the

DPO or Chief Executive Officer then it must be reported to the ICO with 72 hours.

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 Kingston 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.

6. Legal requirements

In some cases, Healthwatch Kingston will be covered by legal requirements of confidentiality. Our legal responsibility to protect information about people is covered in section 15 'Using personal data and confidential personal information

In If there is a Data Breach this must be reported to the Chief Executive Officer and the DPO immediately. If the Data Breach is classified as serious by the DPO or Chief Executive Officer then it must be reported to the ICO with 72 hours.

7. Using personal data and confidential personal information (Section 16 of this policy)

Where Healthwatch Kingston 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, *"24. Information* Sharing*"*, section 25 of this policy.

8. 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 Kingston meets legislative and regulatory requirements. Healthwatch Kingston via Healthwatch England has access to training and guidance to ensure staff understand their legal responsibilities and can apply best practice in managing records. The key benefits for supporting Healthwatch Kingston in this are that records are:

The key benefits for supporting Healthwatch Kingston 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 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

9. Storage of records

Our policies and guidance support record storage and maintenance by:

- Protecting sensitive or confidential information.
- Sharing records.
- Version control.
- Storing and maintaining paper.
- Managing records within shared systems.

10. 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.

11. Record Keeping and retention

The Data Protection Act 2018 states that you shouldn't keep personal data longer than necessary. This means that you must have a lawful basis for keeping information, and once you no longer need it, you should securely erase and destroy it.

Whether held on computer systems or paper, any data should be subject to a strict retention schedule. All records used, received or created by Healthwatch Kingston have a retention period assigned that meets legislative and business requirements (see Healthwatch Kingston Retention Schedule and Lawful basis)

12. Information retention policy statement

We keep accurate, proportionate records to:

- Provide a high-quality service to patients and the public.

- Provide feedback to health and social care services
- Ensure good support and supervision to volunteers
- Comply with all employment, charity and company legal requirements
- Publicise our activities
- Comply with quality assurance systems.

All records are made and held in accordance with the principles of the UK GDPR and Data Protection Act 2018. Healthwatch Kingston responsibility is to ensure that our activities, whether solely or as part of another organisation, are covered by our registration with the Information Commissioner's Office.

We keep records for the period specified in the procedure below.

This policy was adopted on 01/09/2022 and will be reviewed annually

Name of Chair: Liz Meerabeau

Signature of Chair:

Retention schedule and Lawful Basis

Retention of records in Healthwatch Kingston **Employment Staff and volunteer records should be retained for six years after the end of employment but need only to contain sufficient information to provide a reference (e.g. training and disciplinary records).** **Copies of any reference should be retained for six years after the reference request. Director's files should be kept for six years.**	
Application form	Duration of employment, destroy when employment ends
References received	Duration of employment, destroy when employment ends
Sickness and maternity records	Six years from the end of employment
Annual leave records	Six years from the end of employment

Unpaid leave/special leave records	Six years from the end of employment
Records relating to an injury or accident at work	12 years
References given/information to enable a reference to be provided	Six years from the end of employment
Recruitment and selection material (unsuccessful candidates)	Six months after recruitment is finalised
Disciplinary records	Six 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 the 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 ten years, if that is longer. E.g. around Safeguarding.	
Public experience, e.g. observations, interviews, enter and view notes, surveys, research/engagement project data.	
Comments recorded on internal databases	Retain in line with local policy
Any paper-based comments recorded on the database.	One 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 numbers. and date of the check and return to the volunteer or staff member.	
Safeguarding concern recording forms	
All safeguarding concern forms and related information should be kept for ten years. If the record relates to children and young people, it must be kept until they are 21 years old before destruction.	
Financial records	
Income tax and NI returns, income tax records and correspondence with HMRC	Six years (public-funded companies)
Payroll records (also overtime, bonuses, expenses)	Not less than six years after the end of the financial year to which they relate
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 held permanently
Variations to the governing documents	Original to be stored permanently
Statutory registers	Permanently
Membership records	20 years from the commencement of membership register
Rental or hire purchase agreements	Six years after expiry

Others	
Deeds of title	Permanently
Leases	12 years after the lease has expired
Accident Books	Three 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
Microsoft	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

Lawful Basis

Article 6 Section 1 - Processing shall be lawful only if and to the extent that at least on the of the following applies:	
Column M:	**Lawful Basis for Processing Personal Data (via CQC and HWE)**
(a)	the data subject has given consent to the processing of his or her personal data for one or more specific purposes
(b)	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
(c)	processing is necessary for compliance with a legal obligation to which the controller is subject
(d)	processing is necessary in order to protect the vital interests of the data subject or of another natural person
(e)	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 controller
(f)	processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child
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 ten years, if that is longer. E.g. around Safeguarding.	
Article 9 Section 1 and 2	

(1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning the person's sex life or sexual orientation shall be prohibited. **(2) This shall not apply if one of the following applies;**	
Column O:	**Lawful Basis for Processing Special Category Data (via CQC and HWE)**
(a)	the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject
(b)	processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
(c)	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
(d)	processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects

(e)	processing relates to personal data which are manifestly made public by the data subject;
(f)	processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
(g)	processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject
(h)	processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3
(j)	processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy

13. Accessing records

For access to restricted areas staff must obtain authorisation from the Asset Owner. Whether restricted or not, you must only access Healthwatch Kingston's records as authorised and required for the exercise of your role.

14. 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 Executive 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 Executive Officer who will secure the systems by contacting our IT support who can then reset any passwords.

In the absence of the Chief Executive Officer, contact IT support and employees 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.

If there is a Data Breach this must be reported to the Chief Executive Officer and the DPO immediately. If the Data Breach is classified as serious by the DPO or Chief Executive Officer then it must be reported to the ICO with 72 hours.

15. Using personal data and confidential personal information

What is personal data
Personal data is defined under section 1 of the Data Protection Act 2018, 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.

16. What is confidential personal information

Confidential personal information is defined under section 76 of the Health and Social Care Act 2012. It is personal data that has been obtained by Healthwatch Kingston 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.

17. Legal requirements and obligations

The Data Protection Act 2018 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 2012 creates a specific offence of disclosing confidential personal information except in defined circumstances.

18. 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'.

19. 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).

20. Conditions for processing personal data

Personal data may only be processed where a condition under schedule 2 of the Data Protection Act 2018 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 Healthwatch Kingston Data Asset Register sets out the lawful basis for our processing of data.

21. 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.

22. 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.

23. 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 Executive Officer in the first instance and if necessary from the appointed DPO Healthwatch Kingston

Data 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. Where the proposed changes will involve information about people who use care services, the privacy impact assessment will form part of the Caldicott Principles approval process. The Caldicott Principles ensure that uses of information about people who use services are lawful, fair and proportionate.

24. 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 Kingston CCG, Kingston Council, Healthwatch England and CQC.

25. 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 Kingston. 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.

26. Making decisions to share information

Decisions on sharing personal data should be made using the 'necessity test' (see section 22).
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.

27. 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 Executive Officer or DPO.

28. Access to Information
Into to FOIA, EIR and DPA SARs

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

Data Protection Act 2018 gives data subjects a right of access to information Healthwatch England holds about them. This is called a subject access request (SAR). Any SAR request will be handled by the appointed Healthwatch Kingston DPO.

The Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations (EIR) give a general public right of access to any information held by Healthwatch England – subject to some exemptions. SARs must be answered within 40 days. FOIA and EIR requests must be responded to within 20 working days

29. 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 (DPO).

30. What to do if asked to support a request

You may be asked by the DPO 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.

31. Sign-off and decision making

All responses to requests for information regarding Healthwatch Kingston are signed off by the Chief Executive Officer and the assigned DPO and will be disclosed by them via their internal processes.

32. 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.

33. Support and guidance

In the first instance approach the Chief Executive Officer. In his/her absence contact an Officer of the Board. The DPO at Healthwatch Kingston can be approached for support with the authorisation of the above.