

## **Healthwatch Hertfordshire Confidentiality Policy**

This policy applies to all staff, trustees, and volunteers of Healthwatch Hertfordshire (HWH). The data covered by the confidentiality policy includes:

- Information about the organisation, for example, its plans or finances
- Information about other organisations
- Information about individuals, for example, members of the public, volunteers, trustees, and staff whether recorded electronically or in paper form

All staff, volunteers, trustees and others who contribute to the work of HWH must respect the need for confidentiality of information held about anyone who comes into contact with HWH and about any HWH business. This is expected to continue even when contact has ceased with this person.

This policy should be read in conjunction with HWH's Managing Information and Privacy Policy.

### **Principles of confidentiality**

- We will collect only information that is needed to fulfil HWH's remit and to safeguard staff, volunteers, trustees, and clients.
- All personal information will be kept electronically, only accessible to those with authorised access.
- Personal information will only be kept on mobile devices, i.e. laptops, phones, tablets, or external drives, with appropriate security/encryption.
- All electronic information will be kept in designated folders and protected by passwords and firewalls, as appropriate.
- Information will be factual.
- Permissions will be sought from individuals regarding the use of their data and that data will only ever be used for that specified purpose.
- We will not keep personal information any longer than stated in the HWH retention schedule/required by law.
- Information that is no longer needed will be shredded or permanently deleted.
- It is everyone's responsibility to ensure that confidentiality is maintained both inside and outside work.
- Where it is necessary to transmit personal information electronically only secure communications methods will be used.

## **Information about individuals**

HwH is committed to ensuring confidential services to all individuals. The confidentiality is between the individual and the organisation, not the members of staff delivering a particular service. Where confidential information needs to be shared internally (in order to deliver a service), GDPR principles and best practice will be followed.

Confidential information will not be sought from a member of the public unless expressly in the interests of that person, i.e. to help in signposting appropriately or enable a better service delivery.

Confidential or personal information will only be passed to another agency or to other individuals outside of HwH (including Healthwatch England) with the consent of the member of the public, where possible this will be with written consent. For example, if a member of staff or volunteer intends to share information about a member of the public with another agency in order to refer them to that agency.

No personal information about staff, volunteers or members of the public will be given to any third party including a member of their family, without consent.

Information will be treated in confidence and will not be divulged to anyone outside the organisation without the individual's permission, except where extenuating circumstances exist (see below). However, in order that we can provide the best possible help it may be necessary to share information with a manager or colleagues within HwH.

In no circumstances will details of a member of the public/client be discussed with anyone outside of the organisation, or in a public area in such a manner that it is possible to identify that person.

Staff, trustees and volunteers should take due care and attention when speaking to members of the public and using the telephone. No member of the public should be able to hear a conversation or personal details of another service user.

## **Email**

### **Sending personal information via email**

The following practice must be followed when sending information about members of the public via email outside of the organisation:

- Personal information should not be included in the body of the email e.g. address, photos or details of a condition or case.
- Where personal information is required to be shared via email, it should be attached as a document which is password protected. The password must then be sent in a separate email.
- If the information is especially extensive or sensitive it is advisable to post by recorded delivery and request acknowledgement of receipt from the recipient.
- If in doubt about the most secure way to share information, discuss with the Deputy Chief Executive, Governance and Operations. It may also be helpful to discuss with the intended recipient to find out their own organisation's policy.

### **Receiving personal information via email**

Personal information should not be stored in the email accounts of Staff for more than 20 working days. Staff must ensure such information is moved to the HwH shared drive and deleted from their email account.

### **Use of information for publicity, reporting or training purposes**

HwH does need to be able to give information where appropriate about the quality of the health and social care services in Hertfordshire.

If confidentially shared information from a member of the public would provide useful material for publicity, reporting or training purposes, then permission of that person will always be sought at the point of providing that information before the story is told to anyone else. This will include all experiences, stories and comments provided by members of the public to HwH. Permission will be gained (through the use of a model release form) before photographic images of individuals other than HwH staff are used in HwH publicity or promotional materials. Where the subject is under 16 the permission of a parent or guardian will be sought. If permission cannot be obtained then any details that would enable identification of that person will not be used.

### **Limits to client confidentiality**

If you tell us something which leads us to believe you or someone else may be at risk of serious harm or abuse, or assisting a serious criminal offence, HwH reserves the right to break confidentiality should this be deemed necessary. These circumstances include:

- If a member of staff, trustee or volunteer believes that a member of the public could cause danger to themselves or to others.
- If a member of staff, trustee or volunteer suspects abuse or has knowledge of abuse

- If the member of the public gives information which indicates that a crime has been committed
- If disclosure is required by law, for example, by the police
- If a person is felt to lack the mental capacity to make a decision. In such cases staff or volunteers will discuss with a manager and they will only act in the person's best interest.
- If the caller gives information which indicates a possible terrorist threat.

Staff, trustees or volunteers must report the alert immediately to someone who is in a position to take responsibility. The decision on whether to break confidentiality will be decided on a case by case basis and always in conjunction with a senior manager and/or the data protection officer.

### **Access to data**

Apart from HwH staff and volunteers, no-one will have access to personal information unless it is relevant to the work of HwH. Staff should never give out phone numbers or email addresses of individuals. If there is a request for information, it is important to find out why this information is required. In such situations, details should be taken and passed on to the individual concerned.

All members of the public, staff, trustees and volunteers have the right to request access to all information stored about them, and have a right to see a copy of this confidentiality policy on request.

If any party concerned has a disability or impairment which affects their ability to understand this, efforts should be made to ensure that all aspects of this policy and exchanges between parties are understood.

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

### **Attending meetings where confidential information is discussed**

HwH Board Members, volunteers and staff may attend meetings where confidential information is discussed. Anyone working for HwH, whether in a paid or unpaid capacity, will respect the bounds of confidentiality of that meeting, whether this be regarding individuals, commissioning or services.

### **Evaluation and Monitoring**

All staff, trustees and volunteers will be given a copy of the policy when they join HwH and will sign the confidentiality statement that they will abide by this policy. HwH will ensure that all staff and volunteers are trained in the application of this policy.

The policy will be reviewed at least annually by the Policy Lead, Deputy Chief Executive, Governance and Operations and approved by the Board. It will also be reviewed in response to changes in relevant legislation, contractual arrangements, good practice or in response to an identified failing in its effectiveness.

**Declaration:**

I can confirm I have read and understood and will follow the Healthwatch Hertfordshire Confidentiality Policy.

.....

Print name:

**Reviewed and signed off at with minimal changes on: 15<sup>th</sup> January 2025**

**Nuray Ercan**

**Signed by Nuray Ercan, as Company Secretary**

**Responsible Officer**

Ivana Chalmers, Chief Executive