

Confidentiality Policy

Introduction

Healthwatch Worcestershire (HWW) provides an independent voice for people who use publicly funded health & social care services; Our role is to ensure that people's views are listened to and fed back to service providers and commissioners to improve services. We use personal data to do this.

Definition

Confidentiality is defined as protecting information from unauthorised disclosure.

Scope

This policy and related policies set out the principles and requirements that must be observed by all directors, staff and volunteers carrying out activities on behalf of Healthwatch Worcestershire.

This Policy applies to all personally identifiable and confidential information held in any format (digital, written or recorded) and means that all such information must be kept strictly confidential.

It includes:

- personal data
- special category data
- commercially sensitive information
- HR records
- financial information
- information obtained in confidence from partners

This policy also applies to employees after they leave Healthwatch Worcestershire. Former employees must continue to protect any personal, confidential, commercially sensitive or otherwise restricted information obtained during their employment and must not disclose or use such information without proper authority.

Statement of Intent

All directors, staff and volunteers have legal and ethical responsibilities for protecting personal information they come into contact with during the course of their work and preserving information security. This is not just an obligation under their contracts of employment but also under relevant UK legislation.

It should also be noted that, all confidential or sensitive information, whether personal data or not, should be handled appropriately according to its sensitivity.

All information created during employment or volunteering belongs to HWW.

Please refer to the Data Retention Policy and Appendix 1 Deletion Schedule for details for specific data categories.

The Chief Officers have overall responsibility for ensuring that this policy is implemented by all directors, staff and volunteers and that this and associated policies comply with legal and statutory requirements including:

- UK GDPR
- Data Protection Act 2018
- Common Law Duty of Confidentiality
- Human Rights Act 1998 (Article 8)
- Caldicott Principles (where handling health and care information)

If a Breach of this policy occurs, you must inform your Line Manager, or the DPO (DB) immediately, they will decide what if any further action needs to be taken.

Intentional / negligent breaches of this policy may result in disciplinary action.

The principles of confidentiality are enshrined in our day-to-day operations, further details of the specific procedures are contained in the following policies:

- Privacy Statement
- IT Security Policy
- Data Protection Policy
- Email and Internet Policy
- Social Media Policy
- Password Policy
- Retention and Disposal Policy
- Homeworking Policy / Addendum
- Safeguarding Policies - Adults / Children

Please also refer to the Exit Plan for closure / transition specific data issues.

Document Details & Version Control

Version	Comments /Reason for Amendments	Lead Director	Author / Editor	Date	Review by
0.1	Draft	DB	PH	13/6/24	
1.0	Approved at CBM	DB	PH	20/6/24	6/26
1.1	Amended MD to CO's	DB	PH	09/07/26	
1.2	Amendments made as suggested by JN (email 3.8.26)	DB	PH	06/08/26	
2.0	Amendments agreed in principle at CBM 4.8.26 (DB not present) – final approval delegated to DB/PH. Approved by DB 18.8.26.	DB	PH	18/08/26	1/27