DATA PROTECTION AND CONFIDENTIALITY POLICY

1. General Policy Statement

1.1 Healthwatch Central Bedfordshire is fully committed to compliance with the requirements of the Data Protection Act 2018 and GDPR. The organisation will therefore follow procedures that aim to ensure that all employees, volunteers and directors; along with contractors, agents, consultants, partners or others acting on its behalf; who have access to any personal data held by or on behalf of the organisation, are fully aware of and abide by their duties and responsibilities under the Act.

1.2 In order to operate efficiently, Healthwatch Central Bedfordshire has to collect and use information about people with whom it works. These may include members of the public; service users; current, past and prospective employees, volunteers and directors; and suppliers. This personal information must be handled and dealt with properly, however it is collected, recorded and used; whether it is on paper, in computer records or recorded by any other means; in accordance with the safeguards set out within this policy and the Act.

1.3 Employees, volunteers and directors may also have access to confidential information about the organisations with which Healthwatch Central Bedfordshire works and the internal business affairs of Healthwatch Central Bedfordshire, including contracts and tenders, and other information considered ‘commercially sensitive’. Access to such information is on a ‘need to know’ and properly authorised basis. It must only be used for the purpose(s) for which it has been authorised.

1.4 Healthwatch Central Bedfordshire regards the lawful and correct treatment of personal and/or confidential information as very important to its successful operation and to maintaining confidence between the organisation and those with whom it works. Healthwatch Central Bedfordshire will also ensure that it treats personal and confidential information lawfully and correctly.

2. Purpose

2.1 The purpose of this policy is to set out the organisation’s commitment and procedures for protecting personal data and dealing with confidential information held by the organisation.

2.2 The objectives of this policy are to:

- put in place effective controls and ensure appropriate records are kept;
- meet its legal obligations under the Data Protection Act 2018 and GDPR and other appropriate legislation;
- prevent inappropriate use of data held and harm to individuals whose data is held;
- meet its contractual obligations and the requirements of funders;
- demonstrate good data protection management, respect for confidentiality and meet relevant quality assurance systems.

3. Scope

3.1 This policy applies to all employees, volunteers and directors of Healthwatch Central Bedfordshire. It also applies to all contractors, agents, consultants, partners or others acting on its behalf; who have access to any personal data or confidential information held by or on behalf of the organisation.

3.2 Healthwatch Central Bedfordshire has a range of policies and procedures, which deal with good practice standards and information processing; these include:

- Equality and Diversity
- Governance
- Financial Controls
- Recruitment
- Safeguarding
- Whistle Blowing

This policy needs to be read in conjunction with these other policies. Employees, volunteers and directors are encouraged to use the provisions of these policies and procedures when appropriate.

4 Definitions

4.1 A 'data subject' is the person whose personal data is being held and used. Healthwatch Central Bedfordshire's data subjects include employees, volunteers, job applicants and members of the public.

4.2 'Personal data' is defined as data relating to a living individual who can be identified from that data; or from that data and other information which is in the possession of or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

4.3 'Sensitive personal data' is defined as personal data consisting of information regarding an individual's racial or ethnic origin; political opinion; religious or other beliefs; trade union membership; physical or mental health or condition; sexual life; or criminal proceedings or convictions.

4.4 'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, transmission, dissemination or adaption of the data.

5. General Principles

5.1 Healthwatch Central Bedfordshire recognises that its employees, volunteers and directors gain information about individuals and organisations during the course of their work. This may involve dealing with information such as names/addresses/telephone numbers and, in certain areas of work, information on the health of service users; as well as being told or overhearing other sensitive information about the work of Healthwatch Central Bedfordshire.

5.2 Healthwatch Central Bedfordshire endorse and adhere to the principles of the Data Protection Act 2018 and GDPR. The way we will do this is summarised below.

i. We will process data lawfully, fairly and transparently
ii. We will only collect data for explicit and lawful purposes
iii. Data must be relevant and necessary for the purpose its being collected
iv. We will keep data up to date and accurate
v. We will keep data only if required and for no longer than necessary
vi. We will keep data secure
vii. We will process data in such a way as to protect the rights and freedoms of data subjects
viii. Personal data will be transferred outside of the EU only in certain specific circumstances and ways

5.3 Employees, volunteers and directors must assume that information is confidential unless they know that it is intended to be made public by Healthwatch Central Bedfordshire; this includes passing information to another organisation.

5.4 Employees, volunteers and directors should avoid exchanging personal or confidential information or comments (gossip) about individuals and/or organisations with whom they have a professional relationship and should avoid talking about organisations or individuals in social settings.

5.5 Employees, volunteers and directors will not disclose to anyone, other than to colleagues, their line manager and/or Chief Executive Officer, any information considered sensitive, personal, financial or private without the knowledge or consent of the individual, or an officer, in the case of an organisation.

5.6 Employees and volunteers are able to share information with their line manager/supervisor and/or Chief Executive Officer in order to share information, discuss issues and seek advice.

5.7 Employees, volunteers and directors must not compromise or work to evade security measures designed to protect personal and/or confidential information.

5.8 Where there is a legal duty on Healthwatch Central Bedfordshire to disclose information, the person to whom the confidentiality is owed will be informed that disclosure has or will be made wherever possible.

5.9 Employees', volunteers' and directors' obligations to use and respect personal and confidential information continue to apply after they have stopped working or volunteering for Healthwatch Central Bedfordshire.

6. The rights of data subjects, and how we meet them

The table below sets out the rights of data subjects as defined in the DPA 2018 and GDPR. In the table is a description of how Healthwatch Central Bedfordshire protects these rights and minimises the risk that these rights are infringed.

The DS rights	What this means	What we do
The right to fair processing	That data subjects have the right to information about the processing of their data and about their rights	Data subjects will be informed at the point at which information is collected: ▪ What data is being collected and for what purpose; ▪ How long the data is held for; ▪ Their rights in relation to that data; ▪ Anyone else who will have access to the data why, and how they will use the data we will either name the third party or describe groups of third parties; ▪ Any data that is crossing an EU border, where to, and how it is protected. This information will be clearly presented in a privacy notice on the Healthwatch Central Bedfordshire website. Short versions will be on forms and signing in registers. Staff will be given information in their terms and conditions and volunteers in volunteer welcome packs.
The right of access	That data subjects have the right to receive a copy of their data, including any data being processed by third parties. This allows them to be aware of, and verify, the	Ensure that all individuals who have personal data held and used by Healthwatch Central Bedfordshire can easily: ▪ Ask what personal data Healthwatch Central Bedfordshire holds about them, with a description of the data; ▪ Ask why Healthwatch Central Bedfordshire holds this data; ▪ Ask how long data is held for, and why; ▪ Ask for a copy of the personal data; ▪ Ask about anyone else who has access to this data and why, including anyone outside the EU, and how this data was transferred legally and safely. Asking about personal data is called a “subject access request”. To enable data subjects to do this Healthwatch Central Bedfordshire will: ▪ Train all directors, staff and volunteers to recognise a subject access request (including one from a person who does not know the correct term, or what their rights are);

The DS rights	What this means	What we do
	lawfulness of the processing	▪ Make a subject access request form available. In some cases, Healthwatch Central Bedfordshire may need to ask for proof of identification before the request can be processed. We will inform the individual if we need to verify the individual's identity and the documents required. ▪ Ask the data subject which data they want in what format; ▪ Allocate a staff member to manage the request. This may be the DPO or a staff member, and the data subject may be offered, where possible, the choice; ▪ Remove any third-party information from the record; ▪ In most cases within 30 days, provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise. It will only be provided to the data subject. Healthwatch Central Bedfordshire will also provide information about where the data has or will be disclosed, how long it will be stored for and the criteria used to determine that period of time; ▪ In some cases, such as where Healthwatch Central Bedfordshire processes large amounts of a data subject's data, it may respond within three months of the date the request is received. We will write to the individual within one month of receiving the original request to tell them if this is the case. ▪ If a subject access request is manifestly unfounded or excessive, Healthwatch Central Bedfordshire is not obliged to comply with it. Alternatively, Healthwatch Central Bedfordshire can agree to respond but will charge a fee, which will be transparently based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the organisation has already responded. If an individual submits a request that is unfounded or excessive, Healthwatch Central Bedfordshire will notify the data subject that this is the case and whether or not it will respond to it.
The Right to Rectification	The data subject has the	Healthwatch Central Bedfordshire will make every effort to ensure the quality and accuracy of data it collects. Healthwatch Central Bedfordshire will enable data subjects to rectify their data by:

The DS rights	What this means	What we do
	right to correct any inaccuracies in the data.	▪ Regularly reviewing and updating personal information in their systems. Telling data subjects that it is their right to rectify their data, and make it easy to do so; ▪ In the case of a data subject request, tell the data subject about his/her rights to rectification or erasure of data, or to restrict or object to processing;
The right to be forgotten	That the data subject can have their personal data removed or erased at any time without delay	Healthwatch Central Bedfordshire will enable this by; ▪ Telling data subjects that it is their right to ask for their data to be erased, and make it easy to do so; ▪ Collecting and processing personal information only to the extent that it is needed to fulfil operational needs or legal Requirements; ▪ Not keeping information for longer than required, operationally or legally; ▪ Having a clear process by which data is erased in a timely way; ▪ Making it clear what the exceptions are: where personal data is held to protect the right to freedom of expression or information, to comply with legal obligations, to perform a task in the wider public interest or exercise of official authority, for public health reasons, for archiving, scientific or historical research, or for the establishment or defence of a legal claim; ▪ Giving a clear explanation of any erasure decision in writing to the data subject.
The right to restriction of processing	That a data subject is allowed, in specific circumstances, to prevent Healthwatch Central	This may be because they feel the data is inaccurate, is being processed unlawfully, is no longer needed or they object on some other grounds. Healthwatch Central Bedfordshire will enable this by; ▪ Telling data subjects that it is their right to restrict processing, and make it easy to do so; ▪ Clearly describing the processing activities that are being done so that data subjects can make informed choices; ▪ Holding the data securely while a request to restrict processing is considered (and halting all processing);

The DS rights	What this means	What we do
	Bedfordshire from conducting specific processing tasks.	▪ Involving the DPO in managing and documenting a process to consider the request, comparing their grounds with the legal grounds that Healthwatch Central Bedfordshire have for the processing. ▪ Giving a clear explanation of any restriction in writing to the data subject.
The right to data portability	That the data subject can request copies of their data in a useful format in order to pass them to another service provider	Healthwatch Central Bedfordshire will enable this by; ▪ Telling data subjects that it is their right to data portability; ▪ Providing data in an easy read, electronic format (see data subject access requests, above).
The right to object	That if a data subject objects to how their data is being controlled or processed, Healthwatch Central Bedfordshire must halt processing until it has	Healthwatch Central Bedfordshire will enable this by; ▪ Telling data subjects that it is their right to object to processing, and make it easy to do so; ▪ Telling the data subject about their right to complain to the Information Commissioner if they think Healthwatch Central Bedfordshire has failed to comply with their data protection rights; ▪ Involving the DPO to mediate where appropriate in any request to halt processing.

The DS rights	What this means	What we do
	investigated and demonstrated its legitimate grounds for processing	
The right to appropriate decision-making	That Healthwatch Central Bedfordshire will ensure decisions are **not** made solely by automated means.	Healthwatch Central Bedfordshire will ensure this happens by ensuring the following roles are clearly in place and that the people in those roles are trained and equipped. All **employees, volunteers and directors**; along with contractors, agents, consultants, partners or others acting on behalf of Healthwatch Central Bedfordshire are to be made fully aware of this Policy and of their duties, responsibilities and contractual obligations under the Act. They will be required to sign a Confidentiality Statement before commencing work with Healthwatch Central Bedfordshire. The **Board of Directors** will act as the 'Data Controller' and is the 'person' legally responsible for complying with the Data Protection Act. The Board of Directors will determine the policy, taking into account legal requirements, and ensure that it is properly implemented and adequately resourced. The Board of Directors will designate lead responsibility for data protection in the organisation to the Communications Officer. The role of **'Data Protection Officer'** is commissioned by Healthwatch Central Bedfordshire and fulfilled as of 6th July 2018 by taproot (www.taproot.org.uk) The 'Data Protection Officer' will also have overall responsibility to: 1. Inform and advise Healthwatch Central Bedfordshire of their obligations in relation to data protection; 2. Monitor compliance with GDPR; 3. Provide advice where requested about Data Protection Impact Assessments;

The DS rights	What this means	What we do
		4. Cooperate with the Information Commissioner's Office; 5. Act as a contact point for the Information Commissioner's Office; The **Chief Executive Officer** will also exercise control over the following matters, in consultation and/or with the DPO: 1. handling subject access requests; 2. handling Freedom of Information Act requests; 3. approving requests for the transfer of data to other agencies (other than established procedures already approved); 4. approving unusual or controversial disclosures of personal information; 5. approving information sharing protocols and contracts with data processors;

7. Delivery of this policy

7.1 The delivery of this policy will be facilitated by:

- A Code of Conduct for staff and volunteers – Appendix 1;
- Training, support and resources appropriate to their role to all employees, volunteers and directors to enable them to abide by this policy in general, and the actions described above specifically;
- An information asset register will identify all the different data that Healthwatch Bedfordshire holds, the steps in place to keep it secure and periods of retention;
- A Privacy Notice made available to all data subjects in clear and accessible language at appropriate times
- Appropriate security measures (see 8. below)
- A system of monitoring and review (see 10. below)

8. Data security

8.1 Healthwatch Central Bedfordshire endeavour to safeguard personal information (i.e. keeping paper files and other records or documents containing personal/sensitive data in a secure environment; protecting personal data held on computers and computer systems by the use of secure passwords, which where possible, are changed periodically; and ensuring that individual passwords are not easily compromised).

All hard copy (paper) personal data is kept in locked cabinets in the Healthwatch Central Bedfordshire office. The key for the cabinets is held in a locked safe. The Healthwatch Central Bedfordshire office is located in a building that has a manned reception and a security pass access system in place.

Data retained on laptops, smartphones and any other electronic equipment that is removed from Healthwatch Central Bedfordshire offices is protected by the use of strong passwords and/or PIN numbers. Data that is held on the internal closed NAS drive is protected by use of strong passwords. All electronic data is backed up daily either on a third-party cloud application or on an external hard drive that is kept in a fireproof safe.

All directors, staff and volunteers are responsible for ensuring that any personal data that they hold is stored securely and that personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party. 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.

8.2 Any data passed to a third party, including to a processor, will be specified in a written agreement, setting out the scope and limits of the sharing. These parties are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data. They are required to confirm their conformance to the requirements of the DPA & GDPR.

Specifically:

- The data subject will be informed about any third parties who are in receipt of their data from Healthwatch Central Bedfordshire;
- Any disclosure of personal data will comply with approved procedure;

Data stored electronically (e.g. in databases, survey providers etc.) will be kept in compliance with the Government’s cyber essentials scheme, and we have the following safety features in place: Firewall in internet connection (personal or dedicated boundary), Securest settings on all devices, password protection on all relevant spaces, accounts set to right access levels, accounts set to right access levels, limited access to software, malware protection and device and system software is up to date.

- By law, Healthwatch Central Bedfordshire is required to provide employee liability information to any organisation that our employees are transferring to, in line with the Transfer of Undertakings Regulations (TUPE);
- References that disclose personal information will not be provided to any third party without the data subject's prior authority (unless this is required or permitted by law such as by the police, HMRC, Contributions Agency or similar body.

9. Particular groups of data subjects

Employees and volunteers

9.1 Healthwatch Central Bedfordshire hold personal information about all employees as part of general employee records. This includes address and contact details, marital status, educational background, employment application, employment history with Healthwatch Central Bedfordshire, areas of expertise, details of salary and benefits, bank details, performance appraisals and salary reviews, records relating to holiday, sickness and other leave, working time records and other management records;

9.2 This information is used for a variety of administration and management purposes, including payroll administration, benefits administration, facilitating the management of work and employees, performance and salary reviews, complying with record keeping and other legal obligations;

9.3 Healthwatch Central Bedfordshire may also process information relating to employee's health which may amount to sensitive personal data. This includes pre-employment health questionnaires, records of sickness absence and medical certificates (including self-certification of absence forms), VDU assessments, noise assessments and any other medical reports. This information is used to administer contractual and Statutory Sick Pay, monitor and manage sickness absence and comply with our obligations under health and safety legislation and the Working Time Regulations;

9.4 From time to time Healthwatch Central Bedfordshire may ask employees to review and update the personal information that is held about them.

Children

9.5 Wherever possible, Healthwatch Central Bedfordshire will avoid holding personal data about people under the age of 16. Where it is working with children, it will seek to work with a third party who controls the data in line with that organisations data protection policy;

9.6 If personal data is held about a child, then the consent of that child's legal parent or guardian will be sought and appropriately stored;

9.7 The only exception is that Healthwatch Central Bedfordshire will share information as per their Safeguarding children policy.

Adults in need of care and support

9.8 In some cases, information will be shared with Healthwatch Central Bedfordshire about a person's care by their carer or family member;

9.9 In these cases, Healthwatch Central Bedfordshire will only hold personal data with the explicit consent of the person who the information is about;

9.10 A carers experiences of caring may be gathered and shared. If the information identifies the person they care for, it will only be processed with the informed consent of the cared for person. If the person receiving care does not consent, Healthwatch Central Bedfordshire will ensure any information is fully anonymised;

9.11 The only exception is that Healthwatch Central Bedfordshire will share information as per their Safeguarding Adults in need of care and support policy.

10. Monitoring data protection and assessing risk

10.1 Healthwatch Central Bedfordshire will maintain an information asset register. The information asset register is a list of personal and non-personal information assets that Healthwatch Central Bedfordshire controls and processes.

10.2 Healthwatch Central Bedfordshire will undertake an annual audit of its compliance with this policy and with best practice. This will be overseen by the Data Protection Officer.

10.3 Data Protection Impact Assessments (DPIAs) are used to identify specific risks to personal data as a result of processing activities. Their role is to maintain security and prevent processing infringements of GDPR. Healthwatch Central Bedfordshire will use them when required to evaluate the risks inherent in our work. A DPIA must contain:

- a description of processing and purposes;
- legitimate interests pursued by the controller;
- an assessment of the necessity and proportionality of the processing;
- an assessment of the risks to the rights and freedoms of data subjects;
- the measures envisaged to address the risks;
- timeframes if processing for retention and erasure of data;
- recipients of data;

- any evidence of compliance;
- details of consultation with and consent of data subjects.

This information is held within the information asset register. The register identifies which personal data processing presents any particular risk, and how this is managed, including the decision to use a DPIA.

10.4 Healthwatch Central Bedfordshire will add to the information risk register in advance of any new project where a new category of personal data is collected, or when existing processing activities are changed.

11.Data breaches

11.1 If Healthwatch Central Bedfordshire discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The organisation will record all data breaches regardless of their effect. The DPO will be informed.

11.2 If the breach is likely to result in a high risk to the rights and freedoms of individuals, Healthwatch Central Bedfordshire will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

12. Lawful basis for controlling and processing data

Healthwatch Central Bedfordshire will only hold or use data for which it has a lawful basis for doing so. The 6 lawful bases are:

12.1 Consent; the data subject gives consent based on real choice and control. The consent must be freely given with a full understanding of what it means. This means a positive opt-in to sharing the data. Consent should be kept separate from any other terms and conditions. Consent for different kinds of data will be separately sought. Records of consent will be kept;

12.2 Contract; the processing is necessary for a contract Healthwatch Central Bedfordshire has with the data subject, or because they have asked Healthwatch Central Bedfordshire to take specific steps before entering into a contract (e.g. employee contract);

12.3 Legal obligation; the processing is necessary for Healthwatch Central Bedfordshire to comply with the law (not including contractual obligations) (e.g. prevention of fraud);

12.4 Vital interests: the processing is necessary to protect someone’s life (e.g. child protection disclosures);

12.5 Public task: the processing is necessary for Healthwatch Central Bedfordshire to perform a task in the public interest and for their official functions, and the task or function has a clear basis in law. While Healthwatch Central Bedfordshire provides a public function, the public has a right to refuse to take part in Healthwatch activities, and it will seek consent to process data in most cases;

12.6 Legitimate interests: the processing is necessary for Healthwatch's 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. This basis does not apply to public authorities and so Healthwatch Central Bedfordshire cannot use this as a legal ground.

Registration

Healthwatch Central Bedfordshire registered in the Information Commissioner's public register of data controllers. Reference: ZA095413

Code of Conduct (Appendix 1)

DO:

- Read and understand the data protection and confidentiality policy and refer to it when you are unsure of your responsibilities.
- **At all times** treat personal and operational information as confidential except when it is necessary to share it as per the policy.
- When you collect personal information from someone, including during informal conversation (e.g. at events), explain why Healthwatch Central Bedfordshire collects information, how it is stored and used, and what their rights are.
- Ensure you obtain consent and record that this has been done each time you collect personal data
- When someone tells you information about a third party (e.g. a carer tells you about their cared for person), only collect anonymised information (be careful that the person cannot be identified by the nature of the information). If the carer wants personal information to be collected, you **must** seek the informed consent of the person the information is about.
- Keep all personal information securely and locked away as soon as is practicable. Use password protection as agreed with your line manager on electronic files.
- Share information with your line manager/supervisor and/or Chief Executive Officer in order to share information, discuss issues and seek advice.
- Where possible, tell people if you are sharing information about them with anyone outside of Healthwatch Central Bedfordshire because of a legal duty.
- If you think there has been a breach the data protection policy, inform your line manager or another member of staff immediately.
- Adhere to this policy after you have left Healthwatch Central Bedfordshire.

> How to tell the general public about their personal data:
>
> "Our aim is to improve health and social care services in Central Bedfordshire. To do this we collect feedback about health and social care services. Any personal information you tell us is confidential within Healthwatch unless you agree that you want us to share it with someone else. The only rare exceptions are if we are aware of a crime or are worried that you or someone else is at serious risk, in which case we may tell someone such as social care services or the police.
>
> You don't have to tell us any personal or identifiable information if you don't want to. We will still try and help you if you don't. If you **do** give us personal information we will keep it secure for only as long as we need it. You have the right to see the information, update or correct it, ask us to delete it or to use it differently. There is more information about how we use data on our website, or someone in the office can send you more details."

DON'T

- Disclose to anyone, other than to colleagues, their line manager and/or Chief Executive Officer, any information considered sensitive, personal, financial or private without the knowledge or consent of the individual, or an officer, in the case of an organisation.
- Talk in personal or operational (i.e. about the business dealings) detail about their Healthwatch work in social settings.
- Compromise or work to evade security measures designed to protect personal and/or confidential information.
- Collect personal information for children under the age of 16, unless you have the clear consent of their parent or guardian to do so.