DATA PROTECTION and CONFIDENTIALITY POLICY

1. INTRODUCTION

Healthwatch Oxfordshire (HWO) is committed to a policy of protecting the rights and privacy of individuals, including staff, volunteers, trustees, and suppliers in accordance with the General Data Protection Regulation (GDPR) May 2018 and the Data Protection Act 2018 (DPA 2018).

The GDPR/DPA 2018 demand higher transparency and accountability in how HWO manages and uses personal data. They also accord new and stronger rights for individuals to understand and control that use. As data controllers and processors, we need to ensure that we fully comply with GDPR/DPA 2018 and that we proactively design data protection systems that protect the rights and freedoms of data subjects.

To comply with the GDPR/DPA 2018 HWO must ensure that all information about individuals is collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

2. COMPLIANCE

This policy applies to all staff, volunteers, and trustees of HWO and guidelines can be found at appendix 1. Any breach of this policy or of the law will be considered an offence and HWO’s disciplinary procedures will be invoked. All staff, volunteers and trustees should proactively raise any queries or concerns about data protection through appropriate channels as soon as these arise. HWO will be responsible for making training, support and resources available to staff, volunteers and trustees to enable them to fulfil their data protection obligations.

This policy will be updated as necessary to reflect best practice in data management, security, and control and to ensure compliance with any changes or amendments to legislation.

3. DEFINITIONS AND RESPONSIBILITIES

A ‘data subject’ is the person whose personal data is being held and used. HWO’s data subjects include employees, volunteers, job applicants and members of the public.

‘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.

'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.

“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.

HWO will be the ‘data controller’ under the terms of the legislation, this is described by the Information Commissioners Office as someone who “determines the purposes and means of processing personal data”. HWO is also the processor of the data. In some cases, HWO may be a data processor for other another controller (e.g. when carrying out research for a health provider), or they may pass personal data to another party for processing (e.g. a payroll company).

All staff, volunteers and trustees are responsible for compliance with this policy. The trustees are responsible for monitoring delivery of this policy. The Executive Director (ED) is responsible for managing data subject access requests.

HWO has a Data Protection Officer to monitor internal compliance, inform and advise HWO on its data protection obligations and provide advice regarding Data Protection Impact Assessments (DPIAs). The DPO is independent, an expert in data protection, adequately resourced, and reports to the highest management level at HWO and to the Governance and Finance Group, a sub group of the board of trustees’ which has oversight of the organisation.

4. DATA PROTECTION PRINCIPLES

The legislation places a responsibility on every data controller to process any personal data in accordance with the eight principles below. More detailed guidance on these principles can be found in this link to the ICO’s website.

To comply with the law, the information we obtain will be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To meet these requirements, Healthwatch Oxfordshire staff, staff, volunteers and trustees must follow the Data Protection Principles set out in the GDPR/DPA 2018 which are summarised below:

I. We will process data lawfully, fairly and transparently
II. We will only collect data for explicit and lawful purposes. A list of lawful reasons is given in Appendix 3
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. APPLICATION OF THE POLICY

We retain and use personal data to help us to carry out our role as the local watchdog for people who use health and social care services. We collect information about our staff, volunteers and people who share their experiences of using health and social care services through our website, by post and telephone and through our outreach events.

Healthwatch Oxfordshire staff, volunteers and trustees who collect, store or use any personal information in the course of their duties must follow this policy at all times. This is a legal requirement and any failure to comply may result in disciplinary proceedings. We will proactively and by design protect the rights and freedoms of data subjects. How we do this is set out below:

i) The right to fair processing: That data subjects have the right to information about the processing of their data and about their rights

We will tell data subjects about the way we handle data and their rights in clear language that they can understand. We will do this when we collect the data. Our privacy statement sets out the data processing practices carried out by Healthwatch Oxfordshire and tells them what their rights are.

ii) 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 lawfulness of the processing

The GDPR details rights of individuals (data subject) to access both manual data (which is recorded in a relevant filing system) and electronic data for the data subject. This is known as a Data Subject Access Request (DSAR). Under the GDPR, organisations are required to respond to subject access requests within one month. Failure to do so is a breach of the GDPR and could lead to a complaint being made to the Data Protection Regulator. Staff, volunteers and trustees should be alert to DSAR’s, and proactively help data subjects to make these requests. Requests should be made in writing and include the full name, date of birth and address of the person seeking access to their information. When a subject access request is received, it should immediately be reported to the Executive Director to log and track each request. No fee can be charged for initial DSAR for all types of records, whether manual or electronic format. Information relating to the individual must only be disclosed to them or someone with their written consent to receive it.
Any individual wishing to exercise this right should apply in writing to the Executive Director using the form at appendix 2. Any member of staff receiving a DSAR should forward this to the Executive Director

Anyone who believes that this policy has not been followed with regard to personal data about him/her should raise the matter with the person responsible for that data. If the matter is not satisfactorily resolved, it should be raised as a formal complaint.

iii) The Right to Rectification: The data subject has the right to correct any inaccuracies in the data.

We will work to maintain accurate data by regularly reviewing the data we have and making it clear to data subjects that they can correct any data that is wrong. This will be clear in our privacy statement.

iv) The right to be forgotten: That the data subject can have their personal data removed or erased at any time without delay. We will only store data for as long as is needed. The periods that data is retained are kept in an Information Asset Register which gives further clarity on how we manage and keep secure data that is shared with us. HWO will erase data in line with this register, and additionally consider any requests to erase data in line with GDPR/DPA 2018

v) The right to restriction of processing: That a data subject is allowed, in specific circumstances, to prevent HWO from conducting specific processing tasks. The Information Asset register and the privacy statement taken together give a clear description of the processing that is taking place. Any data subject who wants HWO to stop some processing activity can make this request. Processing will be halted pending a decision, which may include the DPO acting as mediator, and will involve HWO clearly evidencing the lawful grounds for the processing. The default position will be to comply with the request.

vi) 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

HWO will make personal data available to data subjects in a useful format, most commonly electronic.

vii) The right to object: That if a data subject objects to how their data is being controlled or processed, HWO must halt processing until it has investigated and demonstrated its legitimate grounds for processing

HWO will respond proactively to concerns of or complaints by data subjects and will involve the DPO in mediation where necessary. The information asset register clearly describes the lawful grounds for controlling and processing each kind of data.

viii) The right to appropriate decision-making: That HWO will ensure decisions are not made solely by automated means.
HWO puts data protection at the heart of our work by design and by default and gives people in the organisation explicit roles to manage the personal data we collect. These roles are set out above.

6. DATA SECURITY: HWO

HWO 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);

**Paper records**

All hard copy personal data is kept in locked cabinets in the HWO office, a secure building. Data collected at events outside of the office will be kept with the member of the team collecting the information, stored in the boot of their car and placed in a locked cabinet upon their return to the office.

**Electronically stored personal data**

Data retained on laptops, smartphones and any other electronic equipment that is removed from HWO offices is protected by the use of passwords. Access to information on the main database is controlled by a password and only those needing access are given the password.

All staff, volunteers and trustees 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.

7. DATA SECURITY; Third parties and data processors

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 have to confirm their conformance to the requirements of the GDPR/DPA 2018.

Specifically:

- The data subject will be informed about any third parties who are in receipt of their data from HWO;
- Any disclosure of personal data will be in compliance with approved procedure;
- Data stored electronically (e.g. in databases, survey providers etc.) will be kept to at minimum industry standards. This includes access controls.
(password protection), physical security, the use of anti-virus software and ensuring staff are trained in information governance and controls.

By law, HWO 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.

**Data breaches**

If HWO 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 immediately.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, HWO 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.

**8. PARTICULAR GROUPS OF DATA SUBJECTS**

**Employees;**

- HWO hold personal information about all employees as part of general employee records. This includes address and contact details, educational background, employment application, employment history with HWO, 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;

- 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;

- HWO 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;

- From time to time HWO may ask employees to review and update the personal information that is held about them.
Children

- Wherever possible, HWO 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 organisation's data protection policy;
- 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;
- The only exception is that HWO will share information as per their Safeguarding Policy.

Adults in need of care and support

- In some cases, information will be shared with HWO about a person’s care by their carer or family member;
- In these cases, HWO will only hold personal data with the explicit consent of the person who the information is about;
- A carer’s 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, HWO will ensure any information is fully anonymised;
- The only exception is that HWO will share information as per their Safeguarding Policy.

9. REGISTRATION

HWO registered in the Information Commissioner's public register of data controllers. Reference: ZA099136

10. AUDIT AND REVIEW

This policy will be updated as necessary to reflect best practice or future amendments made to the law.

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. HWCP 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.

Audit

We are committed to having a proactive and systematic review process in place and as such we will conduct an annual audit.

CONFIDENTIALITY POLICY

1. INTRODUCTION

This policy applies to all trustees, staff and volunteers of Healthwatch Oxfordshire (HWO). The policy covers information handled on behalf of HWO in a variety of forms recorded either on paper or electronically, and information received verbally.

How personal data is kept in line with the law is covered in the Data Protection Policy above. As well as personal data, which is covered by the data protection policy, HWO also holds and uses data about the business of HWO (for example its strategic plans or budgets) and information about the business of other organisations. This data whether it is held on paper, on computer or other media will be subject to appropriate safeguards.

All staff, volunteers and others who work for HWO will respect the need for confidentiality of information held about anyone who comes into contact with HWO, and about any organisational business. This is expected to continue even when contact has ceased with this person, and when the volunteer or staff member no longer works for HWO. All staff, volunteers and trustees’ will be expected to sign a confidentiality agreement (appendix 4).

The decision on whether to breach confidentiality will be decided on a case by case basis in consultation with the Executive Director (or in his/her absence a member of the Board).

5. GENERAL STATEMENT

This policy is authorised by the Board and any breach will be taken seriously and may result in formal action. Any Board member, employee, volunteer or other party who considers that the policy has not been followed should raise the matter with the Executive Director in the first instance.

<table>
<thead>
<tr>
<th>Policy approved by the Board on:</th>
<th>20.11.18</th>
</tr>
</thead>
<tbody>
<tr>
<td>Person responsible for implementation of the Policy:</td>
<td>CIO Communications</td>
</tr>
<tr>
<td>Review Interval</td>
<td>Annual</td>
</tr>
<tr>
<td>Last Reviewed</td>
<td>06.09.19</td>
</tr>
</tbody>
</table>
Appendix 1

Guidelines for Trustees, Employees and Volunteers

During the course of your work for Healthwatch Oxfordshire, (HWO) you may handle information such as names, addresses, phone numbers and email addresses of Healthwatch Oxfordshire members, clients or volunteers. You may also be told or overhear sensitive information. The GDPR/ DPA 2018 gives specific guidance on how such information should be dealt with by organisations like Healthwatch Oxfordshire. In brief, personal information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. Also, data subjects must be told explicitly and up front how and why we are collecting and using their personal data.

The following guidelines are intended to help you to comply with the terms of the GDPR/DPA 2018 while working for HWO. Please read them carefully and ask the Communications Officer if you are in any doubt about any of them.

1. Sharing members’ or clients’ personal information

‘Personal information’ includes details such as addresses/phone numbers and health details supplied by members/clients. Be mindful that even without a name attached, information could be personal if someone could reasonably guess the identity of the person from the information. So some “anonymous” information about health needs might in fact be personal data if the health issue identifies the person.

Such information may be shared between employees and volunteers at HWO for work reasons but should not be given to anyone outside HWO without explicit consent from the individual concerned. If such a situation arises, please ask your line manager for advice.

2. New members/clients

Before collecting any personal information, the person giving the information must be made aware of the reason for collecting the information, and how and where it will be stored. They should, at minimum, be made aware of the fact that they have rights and how to find out about these (they are available on the website).

All requests from new members/clients for any service offered by HWO should be referred to the appropriate member of staff. If the appropriate member of staff is not available, please take a name and contact number only and pass on the message. This is particularly important when dealing with a third party (e.g. if a relative or friend phones on behalf of a client), as HWO should not (in most cases) collect information about a person who has not given permission for his/her details to be used. In most cases, however, it is assumed that if a representative of a group contacts HWO then that group has given HWO permission to use their details.
3. Unlawful disclosure of personal information

(a) Conversations, both within and outside HWO’s premises you are committing a criminal offence if you disclose personal information ‘knowingly or recklessly’ to anyone you are not supposed to, so please be careful. Please try to ensure that conversations in any public place are as private as possible and be aware that conversations containing personal or sensitive information may be overheard by people who should not have access to such information.

(b) Use of files, books, other paper records and electronic equipment

In order to prevent unauthorised access and accidental loss or damage to personal information held on paper, please take good care of files, books and other paper records while on duty, and ensure that they are stored safely before you leave the building. If you have good reason to take any files, materials or equipment off site, these must be looked after with care to prevent unauthorised access. Particular care must be taken with lap-tops, which should routinely be transported in the locked boot of your car, and with USBs (‘memory sticks’). If you have concerns about your ability to keep information secure, please raise this immediately—do not wait until there is a problem.

(c) Disposal of scrap paper

Be aware that names_addresses_phone numbers and other information written on scrap paper are also considered to be confidential. Please shred such notes before disposing of them.
Appendix 2

DATA SUBJECT ACCESS REQUEST FORM

If you want us to supply you with a copy of any personal data we hold about you, please complete this form and send it the address below. You are currently entitled to receive this information under the General Data Protection Regulation (GDPR) and Data protection Act 2018 (DPA 2018). We will also provide you with information about any processing of your personal data that is being carried out, the retention periods which apply to your personal data, and any rights to rectification, erasure, or restriction of processing that may exist.

The information you supply in this form will only be used for the purposes of identifying the personal data you are requesting and responding to your request.

Section 1: Details of the person requesting information

<table>
<thead>
<tr>
<th>Your full name:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your address:</td>
</tr>
<tr>
<td>Your telephone number:</td>
</tr>
<tr>
<td>Your email address:</td>
</tr>
</tbody>
</table>

Section 2: Are you the data subject?

Please tick the appropriate box.

**YES:** I am the data subject. I enclose proof of my identity (see below). Please proceed to Section 4.

**NO:** I am acting on behalf of the data subject. I have enclosed the data subject’s written authority and proof of the data subject’s identity and my own identity (see below). Please proceed to Section 3.

To ensure we are releasing data to the right person we require you to provide us with proof of your identity and of your address. Please supply us with a photocopy or scanned image (do not send the originals) of one of both of the following:

**Proof of Identity.** We need one of the following: passport, photo driving license, national identity card, birth certificate.

**Proof of Address.** We need one of the following: utility bill, bank statement, credit card statement (no more than 3 months old); current driving license; local authority tax bill.
If we are not satisfied you are who you claim to be, we reserve the right to refuse to grant your request.

SECTION 3: DETAILS OF THE DATA SUBJECT

<table>
<thead>
<tr>
<th>Your full name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Your address:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Your telephone number:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Your email address:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

SECTION 4: WHAT INFORMATION ARE YOU SEEKING?

Please describe the information you are seeking. Please provide any relevant details you think will help us to identify the information you require.

……………………………………………………………………………………………………………………
……………………………………………………………………………………………………………………
……………………………………………………………………………………………………………………
……………………………………………………………………………………………………………………
……………………………………………………………………………………………………………………
……………………………………………………………………………………………………………………
……………………………………………………………………………………………………………………………………
……………………………………………………………………………………………………………………………………
……………………………………………………………………………………………………………………………………
……………………………………………………………………………………………………………………………………
……………………………………………………………………………………………………………………………………

Please note that if the information you request reveals details directly or indirectly about another person we will have to seek the consent of that person before we can let you see that information. In certain circumstances, where disclosure would adversely affect the rights and freedoms of others, we may not be able to disclose the information to you, in which case you will be informed promptly and given full reasons for that decision.

While in most cases we will be happy to provide you with copies of the information you request, we nevertheless reserve the right, in accordance with Article 12 of the GDPR to charge a fee or refuse the request if it is considered to be “manifestly unfounded or excessive”. However, we will make every effort to provide you with a satisfactory form of access or summary of information if suitable.

Section 5: Information about the data collection and processing

If you want information about any of the following, please tick the boxes:

- Why we are processing your personal data
- To whom your personal data are disclosed
- The source of your personal data
Section 6: Declaration

Please note that any attempt to mislead may result in legal action.

I confirm that I have read and understood the terms of this Data Subject Access Request Form and certify that the information given in this application to Healthwatch Oxfordshire is true. I understand that it is necessary for Healthwatch Oxfordshire to confirm my / the data subject’s identity and it may be necessary to obtain more detailed information in order to locate the correct personal data.

.................................................................................................................. ............................
Signature  Date

Attachments:

I am enclosing the following copies as proof of identity:

..........................................................................................................................................................
..........................................................................................................................................................
..........................................................................................................................................................
..........................................................................................................................................................
..........................................................................................................................................................
..........................................................................................................................................................
..........................................................................................................................................................
..........................................................................................................................................................
..........................................................................................................................................................
..........................................................................................................................................................
..........................................................................................................................................................
Appendix 3: Lawful reasons for controlling or processing personal data:

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

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;

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

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

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

5. Public task: the processing is necessary for HWO 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 HWO 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;

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 HWO cannot use this as a legal ground.
Appendix 4 - Confidentiality agreement

When working or volunteering for HWO you will often need to have access to confidential information which may include, for example:

Personal information about individuals who have made contact with or are otherwise involved in the activities organised by HWO.

Information about the internal business of HWO.

Personal information about staff or volunteers working for HWO.

HWO is committed to keeping this information confidential, in order to protect people and HWO itself. ‘Confidential’ means that all access to information must be on a ‘need to know’ basis and properly authorised basis. You must use only the information you have been authorised to use, and for purposes that have been authorised. You should also be aware that under the GDPR, unauthorised access to data about individuals is a criminal offence.

You must assume that information is confidential unless you know that it is intended by HWO to be made public. Passing information between HWO and a mailing house, or vice versa does not count as making it public, but passing information to another organisation does count. You must also be particularly careful not to disclose confidential information to unauthorised people or cause a breach of security. In particular you must:

- not compromise or seek to evade security measures (including computer passwords);
- be particularly careful when sending information to other agencies and organisations;
- not gossip about confidential information, either with colleagues or people outside HWO;
- not disclose information — especially over the telephone — unless you are sure that you know who you are disclosing it to, and that they are authorised to have it.

If you are in doubt about whether to disclose information or not, do not guess. Withhold the information while you check with an appropriate person whether the disclosure is appropriate. Your confidentiality obligations continue to apply indefinitely after you have stopped working or volunteering for HWO.

I have read and understand the above statement and the Confidentiality Policy. I accept my responsibilities regarding confidentiality.

Signed:

Date: