Data Protection Policy

October 2021

Definitions:

GDPR	Means the General Data Protection Regulations
Responsible Person	Means the Business Support Manager
DPO	Data Protection Officer – a named person who monitors Healthwatch Cornwall (HC) but who is external to any involvement with the running of the organisation over the compliance with GDPR and other data protection laws, our data protection policies, awareness-raising, training and audits.
Information Asset Register	Means a register of all systems or contexts in which personal data is processed by HC and includes the information retention schedule

Statement

Healthwatch Cornwall (HC), in the course of carrying out its legitimate business, will process both personal and sensitive data, as described in the Data Protection Act 2018 and GDPR. It is the policy of HC to only collect and retain personal data that is necessary to conduct its business, to respect the privacy of individuals and to ensure that any data held is secure, giving access only to those who have a lawful right to access. This applies to both automated and manual records. HC acts as both a Data Controller in relation to staff and volunteer records and a Data Processor, in terms of records collected in pursuit of its statutory functions. HC is registered with the Information Commissioners Office (ICO).

Involvement and responsibility

Everyone within HC has a responsibility to adhere to the standards of the Data Protection Policy. The Executive Board members, the HC Chief Executive Officer and all employees, including volunteers, have responsibility for the implementation and application of this policy and the associated procedure. This policy applies in

all and any areas where staff or volunteers may be working. The Responsible person shall take responsibility for HC's on-going compliance with this policy.

Data Protection Principles

HC is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Key areas

Processing

To ensure its processing of data is lawful, fair and transparent HC shall maintain an Information Asset Register. This Register will be reviewed at least annually. Individuals will be informed whether and for what purposes personal information relating to them is being processed; the nature of the information and the people to whom such information may be disclosed if appropriate to do so and with

explicit consent. Individuals have the right to access their personal data and any such requests made to HC shall be dealt with in a timely manner.

Collection and Maintenance

All data processed by HC must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interest. It is necessary for HC to collect and retain personal data about employees, clients, volunteers and members. Some of this data, such as health details, may be classified sensitive as defined by the Data Protection Act 2018 and GDPR. Personal data that is requested and kept on individuals will be relevant and not excessive in relation to the purpose for which it is required or processed. It will be accurate and kept up-to-date. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent will be clearly available and systems in place to ensure such revocation is reflected accurately in HC's systems.

Storage

HC will undertake to implement appropriate security, including technical and organisational procedures against unauthorised or unlawful processing of personal data and to prevent its accidental loss, damage or destruction. HC will ensure that personal data, both electronic and manual, is stored securely and for no longer than necessary and disposed of appropriately. Records will be disposed of in line with the information retention schedule.

Access to information will be restricted to those who are required, as part of their work, to see that information. Disclosures will be made only where a legal or justifiable need can be proven. In most cases, consent will be obtained to disclose information to parties outside of HC. Exceptions to this would be when a person may be at risk and intervention is necessary for safeguarding, or when behaviour of that person may be criminal or put another at risk.

Sensitive personal data will be treated with additional care in its storage, use and disclosure. Laptops may sometimes be used outside of the office. All laptops are password protected to restrict access to the user only. It is the responsibility of staff using these outside to ensure they are attended securely, kept with them at all times and only used where they may not be overlooked or read by members of the public. The same applies to mass storage hardware like memory sticks – it is the responsibility of the person using them to check they are secure - confidential information should never be transferred onto these devices. Managers or a delegated member of staff may be required in times of bad weather conditions or emergencies to take confidential client details home. This may be manual or computerised. That person will be held wholly responsible for that information which is not to be taken or left anywhere apart from their home and to be securely locked away when not in use. Any breaches of confidentiality direct, negligently or otherwise, or misuse of information may result in disciplinary action which could

lead to the termination of their contract of employment. Appropriate back-up and disaster recovery solutions shall be in place.

Incident Reporting

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, HC shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO. Any breach of confidentiality or loss of data should be reported immediately to the Chief Executive of HC. The incident will be thoroughly investigated and existing security measures checked.

Confidentiality

Any employee, client, volunteer or members' personal information will be treated confidentially and, apart from those who have a lawful right to access it will not be given out to anyone without their express permission. However, there are four occasions when there is no choice about what remains confidential, they are:
• if there is a real concern that a third person is at risk e.g. suspected adult or child abuse
• where another law requires us to do something;
• when it is necessary to disclose information for 'crime and taxation' purposes;
• should an employee, client, volunteer, or member, fall seriously ill while working and information needs to be given to medical personnel.

IT Communications and Monitoring

HC provides employees with access to various computer facilities for work and communication purposes. Technological safeguards exist to protect information stored on these devices being accessed by people other than the legitimate recipients. Further details can be found in the associated procedure.

Individual rights

Access

Everyone has the right to request to access any data held about them. Any such request should be made in writing and a response given within one calendar month. But if your request is complex or you make more than one, the response time may be a maximum of three calendar months, starting from the day after receipt. There are exceptions, which include where access could breach the confidentiality of a third party.

Alteration

Everyone has the right to expect that any inaccuracies should be corrected.

Prevention

Everyone has the right to prevent processing causing damage or distress and should write giving reasons so HC can take appropriate remedial measures.
HC does not sell data. Our only regular communication with people is via the newsletter, after they have given us explicit consent.

<table>
<tr><td colspan="6">This is a controlled document. It should not be altered in any way without the express permission of the author or their representative. On receipt of a new version, please destroy all previous versions.</td></tr>
<tr><td>Document No.</td><td colspan="3">QP017.2</td><td>Original issue date:</td><td>May 2018</td></tr>
<tr><td>Document Title:</td><td colspan="3">Data Protection Policy</td><td>Author:</td><td>Business Support</td></tr>
<tr><td>Version:</td><td>1</td><td>Pages:</td><td>5</td><td>Last reviewed:</td><td>21/07/2021</td></tr>
<tr><td>Approved by:</td><td colspan="3">Board of Directors</td><td>Next review:</td><td>21/07/2023</td></tr>
</table>

Appendix 2

Contact details for relevant personnel

if you require clarification around our process please contact:

Responsible Person	Anne Oliver, Business Support Manager 01872 273501 anne.oliver@healthatchcornwall.co.uk

In the event of any concerns over potential breaches of data protection or

Data Protection Officer	(tba – seek clarification from Jon McLeavy)

Appendix 2

Privacy Statement

This Privacy Policy sets out the data processing practices carried out by Healthwatch Cornwall.

We retain and use personal data (information that relates to and identifies living people) to help us carry out our statutory and independent role representing people views on the county's health and social care services.

Please note: This privacy policy has been revised as of April 2018 as part of our compliance with new requirements under the General Data Protection Regulation (GDPR) legislation, which replaced the Data Protection Act 1998 and became law from 25 May 2018. It has been reviewed and updated to reflect staff changes in June 2019.

The Information Commissioner's Office (ICO) has a website with all of the most up-to-date information about the GDPR and UK data protection law with which we must be compliant. That includes information about your rights under the law and advice for organisations. Click here to visit the ICO website.

We will always make sure that your information is protected and treated securely. Any information that you give will be held in accordance with:

Data Protection Act 1998

As of 25 May 2018, the new data protection legislation introduced under the General Data Protection Regulation (GDPR) and Data Protection Bill.

Our Information Asset Register will be available for people to read to give further clarity about how data relating to them is managed and kept secure. This includes our retention schedule (details of how long we will retain specific types of information) and clear details about the lawful basis for storing and keeping personally identifiable information.

Our data protection policy and asset register documents are available on request (call 01872 273501 or email enquiries@healthwatchcornwall.co.uk).

We are strongly committed to data security and we take reasonable and appropriate steps to protect your personal information from unauthorised access, loss, misuse, alteration or corruption. We have put in place physical, electronic, and managerial procedures to safeguard and secure the information you provide to us. Only authorised employees and contractors under strict controls will have access to your personal information.

Information we collect

We collect personal information from visitors to this website through the use of online forms (e.g. our Have Your Say form) and every time you email us your details. We also collect feedback and views from people about the health and social care services that they access. It is our job (in law) to do so. In addition, we receive information about our own staff and people who apply to work for us.

Examples of the information we collect include:

- Information submitted when you use our contact form.
- Information you share when feeding back about local health and social care services on our Have Your Say form or directly with our staff in a community setting.
- Emails people send to our enquiries@healthwatchcornwall.co.uk contact email address or those of our staff members.
- Information we log when you contact our information and signposting freephone service

We have included much more detail about each of the above and other various types of information we process under each of the headings listed within this statement. They are:

- Information about people who use our website
- Information about people who share their experiences with us by other means
- Information about people who contact our Information and Signposting Freephone Service
- Information about our own staff, volunteers and anybody applying to work for us
- How we will use your personal information

Personal information about you can be used for the following purposes:

- in our day-to-day work;
- to identify you as a member of Healthwatch Cornwall
- to send you our newsletter where you have requested it;
- to contact you about the work of our sub-groups if you have told us you want to hear about their work
- to respond to any queries you may have;
- to improve the quality and safety of health and social care services in accordance with our statutory purpose and functions.

This may include any personal information that you choose to share with us, but we will treat this as confidential and protect it accordingly. We will never include your personal information in published reports without a clear and recorded positive indication of your consent.

Healthwatch Cornwall will never share information that includes your personal information with a third party unless we have your permission or we believe somebody may be at risk of harm. We might, for example, believe there is cause to raise a safeguarding alert on the basis of the information you have shared.

How we share information with other organisations

We only share personal information with other organisations where it is lawful to do so and in accordance with our data protection policy. Information is shared in order to fulfill our remit which is to pass on your experiences of care to help improve services on your behalf.

We work with Healthwatch England, the Care Quality Commission (CQC), local commissioners, NHS Improvement and our local authority to make this happen. We can also engage external suppliers to process personal information on our behalf.

We will only disclose your personal information where we have your consent to do so, or where there is another very good reason to make the disclosure – for example, we may disclose information to CQC or a local authority where we think it is necessary to do so in order to protect a vulnerable person from abuse or harm. Such a disclosure will be made in accordance with the requirements of the current data protection legislation.

Wherever possible, we will ensure that any information that we share or disclose is anonymised so that you cannot be identified from it.

We sometimes use other organisations to process personal data on our behalf. Where we do this, those companies are required to follow the same rules and information security requirements as us. We will seek assurances from such organisations that they are compliant with the GDPR and this will be outlined in a Data Processing Contract. They are not permitted to reuse the data for other purposes.

Signing up to our newsletter

We use a third-party supplier to provide our newsletter service called MailChimp. By signing up to receive our newsletter, you will be agreeing to them handling your data.

The third-party supplier handles the data purely to provide this service on our behalf. This supplier follows the requirements of the GDPR Data Protection Act 1998 in how they obtain, handle and process your information and will not make your data available to anyone other than Healthwatch.

Please note: You can unsubscribe from our mailings (electronic or hard copy) at any time. Simply hit "unsubscribe" at the bottom of the email, contact us by telephone (01872 273501) or email (enquiries@healthwatchcornwall.co.uk).

The following paragraphs set out why the data processing required for our newsletter distribution is necessary for us to perform a task in the public interest.

We are required under the GDPR to identify a clear basis in either statute or common law for the relevant task, function or power for which we are using your personal data. We have several statutory duties under The Local Government and Public Involvement in Health Act 2007.

These include (among others):

- Promoting and supporting the involvement of local people in the commissions, the provision and scrutiny of local care services;

- Enabling local people to monitor the standard of provision of local care services and whether and how local care services could be improved.
- Marketing our work through the newsletter is an important part of meeting these requirements in law. This is because it encourages people and other stakeholders to share stories about local care services. It also keeps the public informed about key developments in health and care locally so that they can critically assess changes. This is central to our role as the champion for health and social care services in Cornwall.
- It is in the interests of the public to hear about any opportunities through which they may influence, shape, challenge or improve their local NHS and social care service provision.
- Healthwatch England has a duty to monitor services at a national level and stories shared anonymously by us enable this to take place. We have a duty under The Local Government and Public Involvement in Health Act 2007 to do this. These are public tasks and meet the requirements of statutory duties. These activities then are important to both the data controller and Healthwatch England.
- In our capacity as the champion for health and social care services in Cornwall, we have very specific interests and this is reflected in our members and stakeholders who share the same interests and have enrolled voluntarily to participate in our agenda locally. Personal details have been provided to us by recipients and recipients have chosen to participate in this list. Participation in no way negatively impacts your rights.
- Our mailing list is not used for profiling or other marketing activity. Email clicks and opens may be tracked to help us monitor performance. Participants can unsubscribe at any time and are reminded how to do so as well as being provided with this privacy notice.
- Certain safeguards and measures are also taken to protect the rights of data subjects:
- Recipients will be informed about GDPR and reminded how to unsubscribe;
- Recipients can unsubscribe at any time by clicking on links within emails sent to them;
- Recipients can unsubscribe at any time by contacting our office;
- Emails are processed and sent via a system that ensures that recipients cannot be identified by each other;
- Staff work in accordance with the requirements of the GDPR and our Data Protection Policy;

Contact data is held within the EEA;

Contact data may be shared with email services based in the US for use of distribution services only. These services are EU-US Privacy Shield Compliant.

Information about people who use our website

Please note: This statement does not cover links within this website to other websites. Our website may contain links to other websites of interest. However, once you have used these links to leave our site, you should note that we do not have any control over that other website. Therefore, we cannot be responsible for the protection and privacy of any information which you provide while visiting such sites and such sites are not governed by this privacy statement. You should exercise caution and look at the privacy statement applicable to the website in question.

When you browse through the information on this website, it does not store or capture your personal information. We do log your IP address (as it is automatically recognised by the web server) but this is only so you can download this website onto your device rather than for any tracking purpose; it is not used for any other purpose.

The Healthwatch Cornwall website is provided and hosted by Circle Interactive

Network Security

The solution incorporates all traffic being encrypted over Secure Socket Layer (SSL) using an SSL certificate.

We will only use ciphers and protocols that are not deprecated. This means currently we only support TLS 1.2 and at least 128-bit ciphers.

Server Security

We operate stripped down systems and have total control over security updates.

Access to the servers (only by SSH) is restricted to IP addresses owned by Circle Interactive and Bytemark (the infrastructure provider)

The basic server configuration will be similar to PCI compliant servers that we run. While PCI compliance is not in the scope of this hosting, we would willingly submit the system to any penetration testing that is deemed necessary, and comply with any further recommendations that the testing generates. Additionally, we run periodic Nessus scans, especially following significant changes or attempted attacks.

We run Linux Malware Detect (LMD) on servers. This is a malware scanner for Linux released under the GNU GPLv2 license. It uses threat data from network edge intrusion detection systems to extract malware that is actively being used in attacks and generates signatures for detection.

The only ports open will be 25 (SMTP), 80 (for redirect to 443), 443, 22 (firewalled), 4949 (used for monitoring and firewalled), 5666 (used for monitoring and firewalled).

We will ensure that the web servers are fully patched and access restricted to essential\cleared staff.

Information we collect through our website

User provided information

When you use our website, as a user or as a visitor, you may provide, and we may collect Personal Data. Examples of Personal Data include your name and email address. Personal Data also includes other information, such as geographic area or your preferences, when any such information is linked to information that identifies a specific individual. We will only collect personal information provided by you.

Automatically Collected Information

When you visit our website or interact with our electronic mailings, we (or our service providers) may automatically record certain information from your devices by using various types of technology, including cookies. This “automatically collected” information may include:

IP address or other device address or ID

Web browser and/or device type

The web pages or sites visited just before or just after using our service

The pages or other content you view or interact with

The dates and times of your visit, access, or use of our communication platforms

We also may use these technologies to collect information regarding a visitor or user's interaction with email messages, such as whether you have opened, clicked on, or forwarded our electronic messages. This information is gathered from all users and visitors.

Analytics

We use Google Analytics to measure and evaluate access to and traffic on the Public Area of the website, and create user navigation reports for our site administrators.

Google operates independently from us and has its own privacy policy, which we strongly suggest you review. Google may use the information collected through Google Analytics to evaluate Users' and Visitors' activity on our Site (including the number of people who have spent time on our website and other such statistics).

The data collected will only be used on a need to know basis to resolve technical issues, administer the Site and identify visitor preferences; but in this case, the data will be in non-identifiable form. We do not use any of this information to identify Visitors or Users.

Cookies

Please be aware that some systems on our website require the use of cookies, but we will always state if this is the case. We will never collect and store information about you without your permission.

A cookie is a small file which asks permission to be placed on your computer's hard drive. Once you agree, the file is added and the cookie helps analyse web traffic or lets you know when you visit a particular site. Cookies allow web applications to respond to you as an individual. The web application can tailor its operations to your needs, likes and dislikes by gathering and remembering information about your preferences.

We use traffic log cookies to identify which pages are being used. This helps us analyse data about webpage traffic and improve our website in order to

tailor it to customer needs. We only use this information for statistical analysis purposes and then the data is removed from the system.

Overall, cookies help us provide you with a better website by enabling us to monitor which pages you find useful and which you do not. A cookie in no way gives us access to your computer or any information about you, other than the data you choose to share with us.

You can choose to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer, however this may prevent you from taking full advantage of the website.

Information about people who share their experiences with us by other means

There are a number of ways that we collect feedback from people about their experiences of using health and social care services day to day. This includes:

- When people complete and submit information about providers of NHS and social care services on our website Have Your Say form
- Direct to our staff working in the community – We use a comment feedback card that matches the fields on our Have Your Say
- When people submit information in response to one of our surveys or projects
- In conversation with our staff and volunteers completing Enter and View visits on our behalf. You can read about these visits here (we never identify individuals within our reports)
- When people share their experience with us by post (letters may be sent using our Freepost address)

People may also share their experience electronically direct to our staff but this is not encouraged wherever possible

We also receive phone calls and requests for information directly from members of the public as part of our Information and Signposting service (see below).

Personal data received from other sources

Where personally identifiable information is collected, we will ensure that we have your consent to keep it and we will be clear on how we intend to use your information. We will aim to anonymise information where we can but there may be instances where this is not possible in order to make change happen on your behalf. There may be exceptional circumstances where we can and will keep the data without consent but we must have a lawful basis for doing so.

We ensure that, where consent is required, it will be freely given, used only for agreed specific and unambiguous purposes and that you are well informed about how the information will be kept. This includes where it will be stored, details on security and for how long it will be kept. We will comply with current data protection legislation at all times.

On occasion we will receive information from the families, friends and carers of people who access health and social care services. We use this data to inform providers and commissioners to help them deliver services that work for you. Where it is practically possible, we will make sure that we have your consent to use information that is about you. We will only process your personal data where there is a lawful basis to do so under current data protection legislation.

Publishing information

In most circumstances, we anonymise our data to ensure that a person cannot be identified, unless this has been otherwise agreed and consent has been given.

Sharing your data with Healthwatch England

We are required to share information with Healthwatch England to ensure that your views are considered at a national level. This enables them to analyse service provision across the country and supply the Department of Health and national commissioners with the information you provide.

Click here to find out more about Healthwatch England.

The information we provide to Healthwatch England contains no personally identifiable data. Any information that is used for national publications is anonymised and will only be used with the consent of a local Healthwatch.

Our data systems

Healthwatch England provides a secure digital system for local Healthwatch to manage their data. Other organisations process the data contained within it on behalf of local Healthwatch and a Data Processing Agreement is in place to ensure that this is held securely and according to current data protection legislation.

Healthwatch England is a committee of the Care Quality Commission (CQC) but acts independently. These organisations must comply with all legal requirements and do not reuse any data for any other reason or make it available to others.

Information about people who contact our Information and Signposting Freephone Service

In addition to ensuring that the voices of service users, patients and the public are heard by decision makers within health and social care, we also provide an information and signposting Freephone service to the public about accessing health and social care services. This includes:

- A free, friendly and confidential service that is independent from the NHS and social care services.
- We will perform a signposting role only. This means that we will give the you the contact details for a range of services that best supports your request. You will then need to contact those organisations yourself.
- We can give you information about choices you have with regard to where you might get help in relation to your health, social care and wellbeing needs.
- We can put you in touch with sources of information on NHS and social care services in Cornwall.
- We can give you information about what to do when things go wrong and you don't understand how to make a complaint.
- We will process the following information when people contact our service:
- Name – It is possible to remain anonymous on our systems through use of a case number. That means you can contact us at any time to ask that information about you is removed from our systems.
- Email address – By sharing your email address with us, we will not add you to our mailing list or contact you for any other purpose than to share information about local and national sources of support appropriate to your needs (related to your signposting request).

- A telephone number – Your telephone number will be used only in connection with your particular query and not for any other purpose. We might contact you with further suggestions or to clarify details about why you are contacting our service.
- A summary of the circumstances surrounding the purpose of the call – We record this information to assist our staff in providing you with relevant information and to check that we have not missed opportunities to suggest possible sources of support. We also use it to share information with our commissioners (our funder) and other stakeholders about the types of queries we receive.
- A record of where we signposted (names of organisations and groups) – This information is recorded in order that we can demonstrate the breadth of signposting delivered by our service to our commissioner and also to the public to which we are accountable.

Please note: If there is a safeguarding concern, Healthwatch Cornwall will take immediate steps to safeguard people from harm in accordance with our safeguarding policies (available on request). We will not share your personal information with other bodies unless we feel it is necessary to protect your vital interests or the interests of another person. This might include information sharing with the Cornwall and Isles of Scilly Safeguarding Adults team [http://www.cornwall.gov.uk/safeguardingadults] and / or the Cornwall and Isles of Scilly Safeguarding Children Partnership [http://ciossafeguarding.org.uk] if we believe somebody to be at risk of abuse or harm.

If contact with our service is made by telephone, people will be asked to verbally indicate their consent for us to store information about them and a record of this consent will be maintained on our Customer Relationship Management (CRM) database.

Information about our own staff, volunteers and people applying to work with us

We need to process personal data about our own staff (and people applying to work for us) so that we can carry out our role and meet our legal and contractual responsibilities as an employer. We also process information about people who are applying to volunteer for us. The personal data that we process includes information about racial or ethnic origin, religion, disability, gender and sexuality. We use this information to check we are

promoting and ensuring diversity in our workforce and to make sure we are complying with equalities legislation.

Our employees decide whether or not to share this monitoring data with us, and can choose to withdraw their consent for this at any time. Employees who wish to withdraw their consent for us to process this data can let us know.

Other personal data that we are required to process includes information on qualifications and experience, pay and performance, contact details and bank details.

We check that people who work for us are fit and suitable for their roles. This may include asking people to undertake Disclosure and Barring Service(DBS) checks.

People joining Healthwatch Cornwall will be asked to complete a 'declaration of interests' form to identify any services with which they have close links (for example, because they have previously worked there or because the service is run by a close relative) or any other issues which could cause a perceived conflict of interest. Staff are regularly asked to update these forms.

We have a legal obligation to comply with the Freedom of Information Act 2000 and this may include the requirement to disclose some information about our employees – especially those in senior or public facing roles. We also publish some information about our staff, including the names and work contact details of people in some roles.

Information about people that take part in our research projects

The information we collate when conducting research may vary for a number of reasons that might include the type of research conducted or the subject matter. We might ask for your name and contact details (in case we need to get in touch about your participation in the research), anonymised demographical information (e.g. your age, gender and ethnicity) and other details if relevant.

Healthwatch Cornwall will only collate information that is relevant to the research and we will never publish your name, or other information about you, without your consent (e.g. case studies). You will have the right to withdraw your consent at any time.

Retention and disposal of personal data

We publish a retention and disposal schedule which explains how long we keep different types of records and documents for, including records and documents containing personal data. Personal data is deleted or securely destroyed at the end of its retention period.

Your rights

Your right to access information about you: If you think we may hold personal data relating to you and want to see it please email enquiries@healthwatchcornwall.co.uk or call 01872 273501.

Correcting or deleting your personal data: If you know that we are holding your personal data and believe that it may be wrong, or if you want it to be deleted or for us to stop using it, you have a right to request that it can be deleted or amended. Please email your request to enquiries@healthwatchcornwall.co.uk or write to: Freepost RTUL-UBEJ-ERCA, Healthwatch Cornwall, 6 Walsingham Place, Truro, TR1 2RP (no stamp required).

Complaints about how we look after or use your information: If you feel that we have not met our responsibilities under data protection legislation, you have a right to request an independent assessment from the Information Commissioner's Office (ICO). You can find details on their website.

Our contact details and key roles: Healthwatch Cornwall is data controller for all of the personal data that you provide us with. Any issues relating to the processing of personal data by or on behalf of Healthwatch Cornwall may be addressed to Freepost RTUL-UBEJ-ERCA, Healthwatch Cornwall, 6 Walsingham Place, Truro, TR1 2RP (no stamp required). You can also call us on 01872 273501 or send an email to enquiries@healthwatchcornwall.co.uk.

Healthwatch Cornwall's designated Data Protection Officer under Article 37 of the GDPR is Jon McLeavy, Chair of Healthwatch Cornwall.