

# UK General Data Protection Regulation (UK GDPR) and Confidentiality Policy



This document sets out the steps that Evolving Communities is taking to comply with data protection law, keep data safe and only use for stated purposes. It covers the following:

- How we comply with data protection law, including the lawful basis for us to collect data.
- How we will ensure that we collect what we need and use is solely for the intended purpose.
- How we will keep personal data safe and secure.
- How and when we share data with other organisations, including Healthwatch England (for our local Healthwatch services) and NHS England (for our local Maternity and Neonatal Voices Partnerships) and where we need to share data with other organisations because of safeguarding concerns.
- What we'll do if someone ask us to provide them with the data that we hold about them.

## Why we collect data

At Evolving Communities, we collect and process personal data for a variety of reasons:

- To give advice and information on how to resolve individuals' health or social care issues.
- To improve health and social care services at a local, regional and national level, including research.
- When people apply for a job or to volunteer for us or if we employ them.
- To send people our newsletter or other publications.
- Photographs and case studies for publicity purposes.
- In the event of a safeguarding matter.

## What data we collect and why we collect it

We'll only collect the data that we need for each stated purpose. It will depend on the situation in which we are collecting the data.

## Research, engagement, feedback, advice and signposting

We can collect personal information without asking for people's permission first. We can do this under the UK GDPR legal basis called 'performance of a public task'. This lets us carry out a task in the public interest or part of our official functions and has a clear basis in law. The law sets out our role in obtaining people's views of health and social care and

providing them with advice.

We'll only collect the data we need for that purpose and no more. This might include:

- Name and contact details.
- Details of the health or social care services people want to talk to us about.
- Details of people's experience of health and social care services.

We'll also ask people for sensitive information so that we can help them and understand how their circumstances might affect their experience of health and social care.

These include:

- Their health conditions.
- Their ethnic origin.
- Their religion.
- Their sexual orientation.

We may not ask people about all of these, and the individual may volunteer additional information about other sensitive categories of data. We tell people they don't have to provide us with the data if they don't feel comfortable doing so.

We're allowed to collect sensitive information like this because it is connected with the provision of and management of health and social care services.

### **In connection with working with or volunteering for us**

We need to use personal information to recruit people and ensure our recruitment processes are inclusive. If people apply for a job with us or to volunteer with us, we ask for the following information:

- Their name, home address, email address and telephone number
- Whether or not they have a disability or anything concerning their medical history or state of health that is relevant to the application
- Their education and employment history
- Their current status in terms of entitlement to work in the UK
- Whether there has been any disciplinary action in the last two years of their employment
- Details of any spent convictions, cautions, reprimands and final warnings in addition to any unspent convictions or criminal proceedings pending.

We also collect equality and diversity information. We don't insist that individuals provide us with this information, but if they provide it, we'll treat any diversity information as strictly confidential. We'll anonymise this information and only use it to look at trends. We won't look at people's information individually or compare it to other people, and we won't use it as part of the recruitment selection process.

We collect personal information through the application form, interview or references so we can process the application. Data protection law allows us to do this to establish a contract with an individual.

If we employ someone, we maintain personal data in connection with their employment including, but not limited to, personnel matters, sickness, performance and remuneration and payroll. We have a 'legal obligation' to process employee data.

We'll keep the following information for people who work or volunteer for us:

- Full name
- Date of birth
- Sex
- Email address
- Phone number
- Home address
- Education and qualifications
- Work experience
- National insurance number
- Tax code
- Emergency contact details
- Employment history with the organisation
- Employment terms and conditions (for example, pay, hours of work, holidays, benefits, absence)
- Any accidents connected with work
- Any training taken
- Any disciplinary action
- Race, ethnicity, politics, religion, trade union status, health, sexual orientation.

We hold the above data to allow us to establish and maintain a contract with the individual and to monitor the diversity of our staff.

**Other purposes:** including newsletter mailing list, being a case study or for publicity photos

We ask for individuals' consent to store personal data for all other purposes.

When people sign up for our newsletters, we collect personal information so we can:

- Send the information they've asked for.
- Let them know when and how we'll be contacting them in the future.

People can sign up by:

- Ticking a consent box on a sign-up form.
- Completing a form or survey on our website.
- Asking our staff to add them to a mailing list.

We provide a means for people to unsubscribe at any time by selecting 'unsubscribe from this list' at the bottom of our e-bulletin, or by asking a member of staff to remove them from the mailing list.

We collect:

- First and last names.
- Email address

For other purposes, we'll ask people to sign a consent form explaining how we intend to use their information and how they can withdraw their consent.

### **How we use people's information in accordance with the law**

At Evolving Communities, we commit to:

- Only asking for what data we need for each purpose.
- Only using the data for the stated purpose.
- Providing people with:
  - A clear explanation of how we'll use their data.
  - The legal basis for processing it.
  - How they can access their data.
  - How they can withdraw consent (if applicable).
- Training our staff, Board members and volunteers on safe data handling in compliance with data protection law:
  - The training is tailored to Healthwatch's unique legal status.
  - Staff and volunteers have to undertake the training as part of their induction process.
  - We ask them to complete refresher training regularly.
  - Ensuring that the data we store about people is accurate and that they have the opportunity to correct it.
  - Having a data protection officer to advise us on how to comply with data protection legislation.

### **How long we keep people's data for**

We keep personal data for no longer than is necessary for the purpose we need it. Our data retention schedule sets out the time limits for keeping each type of personal data that

we collect. Wherever possible, we shall fully or partly anonymise any personal information.

## **How we keep people's data safe**

We have rigorous technical and organisational measures to keep people's data safe.

Our data is stored in Microsoft 365 within UK Data Centres. All Microsoft 365 Data is backed up to a third party backup system called Dropsuite. Hard copy data is stored in locked filing cabinets. Data held by SmartSurvey, MailChimp and Fixed.net is stored securely through their online platforms.

Personal data and intelligence that is captured in hard copy format is logged or scanned and stored electronically and the original hard copy is shredded before disposal. Where personal data is transferred online through email, the document (Word/Excel) is password protected.

### **We use the following systems to store data:**

- Microsoft 365 to store email, SharePoint and OneDrive data.
- SmartSurvey stores partially identifiable data, for example, IP addresses but also non-identifiable data.
- Mailchimp stores full names and email addresses.
- Fixed.net hosts our WordPress website which includes a webform for people to get in touch/share their feedback.
- Microsoft Forms is used to collect and store feedback, advice, information or signposting data. The data is then downloaded into a linked Excel sheet in a protected shared drive. Only the staff members that need to access this data can access this.

We store data from subjects in the United Kingdom.

### **Organisational measures we take to keep data safe**

- Evolving Communities ensures that all hard copy personal and sensitive data that it collects is secured in lockable cupboards at all times. This cupboard will be accessible only to appropriate and relevant staff within the organisation.
- No sensitive data or personal information is stored on mobile devices, local laptop drives or on memory sticks. The *Bring your own device and acceptable use of internet, email and social media policy* lays down the requirements for acceptable use and should be read in conjunction with this policy.
- Staff, Directors, Board members and volunteers do not use business computers or tablets to attempt to gain unauthorised access to any other computer system.
- Staff, Directors, Board members and volunteers do not knowingly carry out any action which could endanger the computer systems.
- Staff lock their computer screens when away from their desk and make efforts to ensure that no unauthorised person (for example, visitors) can view data when it is on display.

- All staff members are automatically prompted to change their passwords on a three-monthly basis.
- All laptops and tablets supplied to Staff, Directors, Board members and volunteers are encrypted to increase security.
- Staff, Directors, Board members and volunteers do not reveal their computer, tablet and/or database passwords to third parties or write passwords down in places where they may be accessible to those outside of the organisation.
- All electronic data is kept on Microsoft 365 which is secure and password protected.
- Staff do not download unauthorised computer programmes that may compromise the security of the computer. Should a member of staff require a particular piece of software for their ongoing work, they must first gain approval from the Data Protection Officer.

All computer systems are kept up-to-date (this is currently carried out on an automatic basis through a contract with an IT company)

When people leave employment/volunteering with us, we remove their work email address from our system so that they can no longer access it.

## Sharing data with other organisations

### Healthwatch England

The law requires us to share data with Healthwatch England so that they can carry out their statutory functions.

We share the following data with them:

- Feedback and signposting data.
- Survey data.

We share this with them via a secure system directly into their Central Data Store on a quarterly basis.

### Other organisations

We will share data with other organisations if there is a lawful basis for doing so, and we have a signed data-sharing agreement in place with them.

Currently, our local Healthwatch services have data sharing agreements with Healthwatch England.

## Staff who have access to NHS email accounts

As an organisation providing services to NHS system some staff have access to NHS email accounts. This is because through the nature of their work and their strategic level representation role they may have access to patient data and information. This ensures the data is held with the NHS system as data controller.

Where this is the case the staff member is responsible for managing the data in line with the NHS system's Information Governance policies and procedures. This involves reading

and acknowledging the following policies and procedures and undertaking GDPR training.

The NHS system remains the data controller for all data held within the NHS account and Evolving Communities remains the data controllers for data held within their Evolving Communities email account.

### **What we do if there is a data breach**

Organisations which process personal data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data. Many organisations take the view that one of those measures might be the adoption of a policy on dealing with a data security breach.

This policy relates to all personal and sensitive data held by Evolving Communities regardless of format and applies to all staff at Evolving Communities including temporary or casual staff, contractors, consultants, suppliers and data processors working for, or on behalf of Evolving Communities.

We will make every effort to prevent a data breach, but should one occur, we will do the following:

- Within 24 hours of becoming aware of the data breach, we will assess the possible negative consequences for individuals as a result of the data breach.
- Within 72 hours, we will inform the Information Commissioner's Office if we assess that there are negative consequences for the individuals involved. We will take proactive mitigation actions and commit to taking any further remedial action they require to address the breach.
- Within 24 hours, we will start to address the root cause of the breach so that no further data is lost and, wherever possible, retrieved.
- If local Healthwatch related, we will inform Healthwatch England of the data breach within 48 hours.
- Tell any individuals concerned if the breach is likely to result in a 'high' risk to their rights and freedoms without any undue delay.
- Undertake an exercise to ensure that we learn from the data breach to prevent the recurrence of this problem.
- Keep a record of all data breaches and our actions to deal with them.

### **If someone requests access to data or objects to us and processing the data that we hold about them**

If someone makes a subject access request for details of the information that we hold about them, we will:

- If they are unknown to us, ask for reasonable proof of their identity.
- Once we have this, we will make all reasonable efforts to provide, in a secure permanent or electronic format, all data that we hold on them within a month of the request.

- Tell them about their rights about their data under Article 15 of the UK GDPR:
  - The purpose of processing their data.
  - The types of personal data concerned.
  - To whom we will disclose their data.
  - How long we'll keep their data for.
  - Their right to ask us to correct their data or stop processing it.
  - Their right to complain to the Information Commissioner's Office.
  - Whether any data is processed in countries outside the UK (for example, where you are using an online survey tool whose servers are based in another country).
- Not charge a fee for providing the information.
- Deal promptly and fairly with requests for inaccurate personal data to be corrected or deleted or object to us processing their data.

If someone asks us to correct or delete data that we hold about them, we will act on their request where:

- Processing is based on consent, and that consent is withdrawn.
- Processing is based on our legitimate interests.
- The personal data is no longer required
- The personal data has been unlawfully processed.
- Where there are no overriding reasons to continue processing the data.

### **The organisational policies that we have in place to ensure that we comply with data protection law**

We will maintain sufficient policies to ensure that we can show that we comply with data protection legislation. This includes:

- Keeping and maintaining a register of all our data and where it is held (an information asset register).
- A register/record of any data subject access requests made.
- A log of any data breaches.
- Evidence of consent where required.
- A historical list of privacy policies and permission statements.
- Training records on data protection for each member of staff/volunteer.
- Evidence of secure destruction of documents and devices.