General Data Protection Regulation (GDPR) & Confidentiality Policy

Policy title	**GDPR & Confidentiality Policy**
Purpose and summary of policy	This document sets out Evolving Communities position on confidentiality and protecting the data that it holds. The purpose of this policy document is to establish a clear and agreed understanding of what confidentiality and data protection means
Ratified by and when	Evolving Communities Board DATE: January 2016

Document Control

Version no.	1.5
Target Audience	All Evolving Communities staff, all local Healthwatch staff, directors, local board and steering group members and volunteers

Change Control

Date	Author	Version	Change description	Document status
February 2017	Sara Nelson	1.1	Reviewed	Final
December 2017	Sara Nelson	1.2	Edited to reflect the change from Healthwatch Wiltshire CIC to Evolving Communities CIC	Final
December 2017	Rhiannon Norfolk	1.3	Applying EC logo and branding	
May 2018	Rachel Martin	1.4	Updated in line with GDPR	
August 2019	Shona Holt	1.5	Minor changes	

General Data Protection Regulation(GDPR) and Confidentiality Policy

1. Scope

This document sets out Evolving Communities position on GDPR and confidentiality. It aims to ensure that the collecting and handling of personal data and confidential information is carried out sensitively and in line with the GDPR and its subsequent amendments.
Evolving Communities is committed to equality and diversity. It will never use any information it receives to discriminate against its staff, Evolving Communities Board or Steering group Members, or volunteers or the wider community, or for any other purpose than is stated by the person who gave it.

2. Definitions

For the purposes of this policy, the ***data subject*** is the individual whose personal data is being processed; examples include:

- Employees (current and past)
- Volunteers
- Board members
- Job applicants
- Members of the public

Processing means the use made of personal data including:

- Obtaining and retrieving data
- Holding and storing data
- Making available within or outside the organisation
- Printing, sorting, matching, comparing, destroying

Special Category data means personal data consisting of information such as:

- Race
- Ethnic origin
- Politics
- Ethnic origin
- Politics
- Religion
- Trade union membership
- Genetics
- Biometrics (where used for ID purposes)
- Sex life; or
- Sexual orientation

3. Responsibility

Evolving Communities has a legal and moral obligation to ensure that specific personal information that it collects as part of its business is treated confidentially. The primary

function of local Healthwatch organisations is to gather the views and experiences of local people in relation to health and social care services. In addition, the consultancy arm of Evolving Communities may collect sensitive information from a wide range of individuals in the course of its business. Sensitive information may be passed in confidence to staff employed by Evolving Communities, its directors, local board and steering group members and volunteers by individuals, groups or communities.

3.1 Commercially confidential information

Evolving Communities CIC may at times, tender competitively for contracts and work in partnership with other agencies to submit bids for external funding. All information concerning our commercial activities must remain confidential.

As part of their everyday business, staff, volunteers, directors of Evolving Communities, local board and steering group members, may come into contact with information of a confidential nature which may include:

- Information about the Evolving Communities Board, local board and steering group members, staff, volunteers and members of the public
- Information about our work, for example our plans, finances and funding bids
- Information about other health, care and voluntary and community sector organisations with whom we work. This may include plans and decisions about current or future services commissioning information, contractual information, commissioning decisions, issues relating to quality and finance information.

An assumption of confidentiality enables people to be open and honest in sharing their experiences. In most cases, confidentiality is maintained. Any data that is used in reports and publications produced either by Evolving Communities or local Healthwatch will be anonymised. Evolving Communities reserve the right, in certain circumstances, to break confidentiality should it be deemed necessary. These circumstances include:

- If it is believed that a person could cause danger to themselves and others;
- If there is suspicion of a safeguarding issue;
- If information is given which indicates that a crime has been committed;
- If disclosure is required by law, for example, by the police.

The decision on whether to break confidentiality will be decided on a case by case basis by either the Manager of the relevant local Healthwatch or if the matter concerns data gathered by the central Evolving Communities staff, the CEO or Data Protection Officer.

All staff employed by Evolving Communities and volunteers are committed to ensuring that the confidentiality and GDPR policy is applied to all aspects of their work. To this end, it is the responsibility of each member of staff, directors, local board and steering group members and volunteers to be familiar with this policy, and to act in accordance with its aims and objectives.

All staff, directors, local board and steering group members and volunteers involved in internal and external task/working groups are bound by this policy and the terms of reference of the specific group.

4. General Data Protection Regulation and usage principles

All directors, local board and steering group members, volunteers and staff should be guided by the Caldicott Principles relating to personal information. The 1997 report of the review of patient-identifiable Information, chaired by Dame Fiona Caldicott (the Caldicott Report), made a number of recommendations for regulating the use and transfer of person identifiable information between NHS organisations in England and to non-NHS bodies.

The Caldicott Principles - revised September 2013
Principle 1: Justify the purpose for using confidential information Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian/s. Any transfer of sensitive information outside of Evolving Communities should be authorised by one of the management team prior to transfer.
Principle 2: Don't use personal confidential data unless absolutely necessary Personal confidential data items should not be collected unless it is essential for the specified purpose(s) of a specific project or as requirement of statutory business. The need for individuals to be identified should be considered at each stage of satisfying the purpose(s).
Principle 3: Use the minimum necessary personal confidential data Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.
Principle 4: Access to personal confidential data should be on a strict need-to-know basis Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes. Evolving Communities CIC have in place access controls on selected folders and drives on their secure file servers across the organisation. These folders include information pertaining to human resources, finance and quality surveillance data (intelligence and insight data). Access is controlled by the relevant Healthwatch Manager or the Data Protection Officer. In the event of role change, dismissal or a member of staff leaving the organisation, access to all systems is revoked.

Principle 5: Everyone with access to personal confidential data should be aware of their responsibilities Action should be taken to ensure that those handling personal confidential data are made fully aware of their responsibilities and obligations to respect confidentiality.
Principle 6: Understand and comply with the law Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.
Principle 7: The duty to share information can be as important as the duty to protect confidentiality All staff should have the confidence to share information in the best interests of the individuals within the framework set out by these principles. They should be supported by the policies of their employers and regulators bodies.

All directors, local board and steering group members, volunteers and staff should also be aware of their legal duties under Article 5 of the GDPR that sets out seven key principles which lie at the heart of the general data protection regime

GDPR compliance principles – May 2018
A: Lawfulness, fairness and transparency Personal data collected by Evolving Communities must be provided with the consent of the individual (verbal or written). Staff, directors, local board and steering group members and volunteers must be transparent and ensure clients are fully informed and understand what will happen to their personal information.
B: Purpose limitation Information collected by Evolving Communities must only be held and used for the reasons given to the Information Commissioners Office (ICO) and the data subject. Personal information must not be processed in any manner incompatible with the original purpose(s). If Evolving Communities wishes to use certain information for purposes outside of the original need they must gain further permission from the individual.
C: Data minimisation All data collected must be necessary to complete the business of Evolving Communities. Staff, directors, local board and steering group members and volunteers should not ask for or hold any personal data that is outside their concern as this would be in breach of the General Data Protection Regulation.
D: Accuracy Evolving Communities must make every effort available to ensure the information they use is accurate, authentic, complete and reliable. Data collected by the organisation is often of a sensitive nature and therefore misinterpretation may unfairly represent the data subject.

E: Storage limitation

GDPR states that a company must not hold onto data for any longer than is necessary. Therefore, data documents will be retained in line with current legislative requirements and best practice. Where data is being collected on behalf of another organisation for example, as part of an evaluation or consultation, Evolving Communities should consult with the project lead of that body to confirm their required data retention period. This specified time may differ between projects to allow for further review, and aid any future queries or disputes regarding, conduct or the actual results of the work. A regular audit of all data will be carried out and overseen by the Data Protection Officer, on a yearly basis to ensure that nothing is kept for longer than defined in this policy. An agreed data retention schedule is a supplementary document to this policy and therefore should be read in conjunction with this policy.

F: Integrity and confidentiality (security)

- Evolving Communities will ensure 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.
- All paper copies of collected sensitive and personal information will be shredded before disposal.
- No sensitive data or personal information will be 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 the document.
- Staff will lock their computer screens when away from their desk and will make efforts to ensure that no unauthorised person (e.g. visitors) can view data when it is on display.
- All staff members will be automatically prompted to change their passwords on a 3-monthly basis.
- All laptops and tablets supplied to staff, directors, local board and steering group chairs will be encrypted to increase security.
- Staff, directors, local board and steering group chairs are not permitted to reveal their computer, tablet and/or database passwords to third parties or to write passwords down in places where they may be accessible to those outside of the organisation.
- All electronic data will be kept on secure, password protected servers based either in local Healthwatch offices or Evolving Communities head office in Melksham. Only Evolving Communities staff across the organisation have access to their respective servers. All access is password controlled. Data is also kept on a secure, Access database. Access to the database is by individual password only. Only relevant staff within the organisation are issued with passwords. These passwords must not be shared with anyone else.
- The Servers and associated back-up disks (RAID array) should be kept in a locked cabinet and accessible only to Evolving Communities and local Healthwatch staff and current IT management company (Priority IT).

- Staff may not download unauthorised computer programmes that may compromise the security of the computer and associated server. 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 must be kept up to date (this is currently carried out on an automatic basis through a contract with an IT company).

G: Accountability

GDPR specifically requires that an organisation takes responsibility for complying with the principles, and to have appropriate processes and records in place to demonstrate compliance. Evolving Communities has retained the services of a Data Protection Officer, who reviews that the policy and procedure for data and personal information are compliant across the organisation under the GDPR principles.

5. Additional IT Security

- Staff, directors, local board and steering group chairs must not use business computers or tablets to attempt to gain unauthorised access to any other computer system.
- Staff, directors, local board and steering group chairs must not knowingly carry out any action which could endanger the computer systems.

6. Training

All staff, directors, local board and steering group members and volunteers who have access to personal/sensitive data will be given a copy of this policy during their induction process and will be expected to read and adhere to the policy. All staff, directors, local board and steering group members and volunteers will need to attend a data protection awareness session on a yearly basis and sign to say that they have read and understood the policy. If anyone requires further clarification on any part of the policy, they should contact the Data Protection Officer before signing the training sheet. If volunteers are unable to attend the training awareness day, they may access the training slides on the secure volunteer portal of the relevant Healthwatch website. They must sign the training sheet to say that they have read and understood the slides.

7. Monitoring Information

The local Healthwatch run by Evolving Communities report on their contract to the relevant local authority and Healthwatch England and keep a range of paper and electronic information to facilitate this. Individuals will not be identified in such reports without their explicit consent. As part of their developing local intelligence programme Healthwatch England gather information and insights about the local Healthwatch network. This will help to inform their policy and priorities for national research and consumer insight work. Local Healthwatch commit to share anonymised data with Healthwatch England. All data that that is shared will be anonymous, focusing on the service types, themes and institutions involved. All information received by Healthwatch England will be securely held, and not shared beyond the

Healthwatch England intelligence team. A data sharing agreement has been entered into between the local Healthwatch and Healthwatch England to manage this access.

Evolving Communities works to ensure that it provides information to the community about its work through different mechanisms including its local Healthwatch websites and annual reports and its own organisational website. All reports will be anonymised so that individual data subjects will not be recognised.

General Data Protection Regulation and Confidentiality Policy

Agreement

I confirm that I have read and understood the contents of the Evolving Communities General Data Protection Regulation and Confidentiality policy and agree to abide by the policy.

Signed .....

Name .....

Date .....