


# Data Protection Policy

## Amendment History

Date	
May 2018	Revised and Amended
	Signed by Miles Newton, Chair of Trustees
April 2019	To be reviewed
April 2020	

**Reviewer** Chair of Trustees

**Owner and Authorised by** Chair of Trustees and Trustee Board

## Other Associated Policies and Procedures

- Privacy Policy
- DBS and Rehabilitation of Offenders Policy
- DBS Certificate Retention Policy
- Financial Policy
- Data Retention Policy

# CONTENTS

1. Introduction
2. Principles of Data Processing
3. Types of Data
  - Personal Data
  - Special Category Data
  - Criminal Data
4. Legal Basis for Processing Data
5. Data Retention and Disposal
6. Personal Data Breaches
7. Data Security
8. Rights for individuals
  - Right to object to processing
  - The Right to Erasure
  - Right to Rectification
  - Right of access
  - Right to be informed

## 1. Introduction

Communicare in Southampton is committed to protecting the rights and privacy of individuals in accordance with the General Data Protection Regulation 2018 (GDPR). Communicare in Southampton processes information about its staff, volunteers, clients, supporters, funders and other individuals it has dealings with for a range of administrative purposes (e.g. to recruit and pay staff, to recruit and reimburse volunteers, disseminate information, match clients to volunteers, organise services such as transport for clients and comply with legal obligations to funding bodies and government). In order to comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

Communicare in Southampton is the Data Controller for data processed by Communicare in Southampton.

## 2. Principles of Data Processing

GDPR legislation lays out six principles for processing of personal data. These are:

- **Lawfulness, fairness and transparency**

This covers the primary areas of concern that data should be gathered and used in a way that is legal, fair and understandable. The public have the right to know what is being gathered and have this corrected or removed. There are some restrictions on the right to have data removed.

- **Purpose limitation**

Organisations should only use data for a legitimate purpose specified at the time of collection. This data should not be shared with third parties without permission.

- **Data minimisation**

The data collected by organisations should be limited only to what is required for the purpose stated. Organisations should not collect data en masse without purpose.

- **Accuracy**

The personal data you hold should be accurate, kept up to date, and, if it is no longer accurate, should be rectified or erased.

- **Storage limitation**

Personal data should only be stored for as long as is necessary. Data can be archived securely and used for research purposes in the future. Where possible, the personally identifiable information should be removed to leave anonymous data. (Note if a key or code is maintained by which the data subject could still be identified this is pseudonymous data and still counts as personal data.)

- **Integrity and confidentiality**

Personal data should be held in a safe and secure way that takes reasonable steps to ensure the security of this information and avoid accidental loss, misuse or destruction.

## 3. Types of Data

### Personal Data

All "processing" of personal data (including collection, holding, retention, destruction and use of personal data) is governed by the GDPR. The Act applies to all personal data - whether it

is held on a computer or similar automatic system or whether it is held as part of a manual file.

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual<sup>1</sup>.

### **Special Category data**

Communicare in Southampton also holds 'special category data' about staff, volunteers and clients. Special Category data is considered by the GDPR to be more sensitive and so needs more protection.

Special Category data is data about an individuals' race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life or sexual orientation.

## **4. Legal Basis for Processing Data**

GDPR requires organisations to determine and state their legal basis for processing personal data. Where special category data is processed organisations must identify and state an additional legal basis for processing this data.

### **Personal Data**

Communicare in Southampton uses 'legitimate interests' as the basis for processing personal data.

(f) Legitimate interests: the processing is necessary for your 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 means that we will only process personal data which is necessary for the legitimate interest and running of our services. For example we need to know client's contact details so that we can arrange to help them.

---

<sup>1</sup> (From Information Commissioner's Office Guide to the General Data Protection Regulations <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr>)

Communicare in Southampton considers it good practice to also gain consent from data subjects wherever practical, however our legal basis for processing personal data is legitimate interests.

### **Sensitive Category data**

Communicare in Southampton has determined that the additional legal basis for processing sensitive category data will be the following

For Volunteers, service users, members and supporters and other contacts including referrers and client next of kin (Special Category data will not routinely be collected from supporters or other contacts.)

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

#### For Staff

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

### **Criminal Records**

Communicare in Southampton carries out DBS checks in accordance with our DBS and Rehabilitation of offender's policy. Information disclosed by staff or volunteers is clearly marked as highly confidential and stored separately in a locked filing cabinet with restricted access and only used for risk assessment purposes in line with the policy.

Information about the criminal records of clients which have been disclosed to Communicare will only be processed if considered necessary for the safety of staff and volunteers. This decision will be made by a senior member of staff. Any such information will be marked as highly confidential and be stored in a locked filing cabinet with restricted access.

## **5. Data Retention and Disposal**

Communicare in Southampton will regularly review how long data should be stored for and communicate this with all interested parties. Full details are set out in our Data Retention Policy.

## **6. Personal Data Breaches**

Personal data breaches must be recorded and may need to be reported to the Information Commissioner's Office.

### **What is a personal data breach?**

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.<sup>2</sup>

Examples of data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

### **If a personal data breach occurs**

Staff and office volunteers should report all potential data breaches to their supervisor or manager as soon as practically possible. Volunteers who believe that personal data in their possession has been lost or stolen should inform the office as soon as possible.

All data breaches must be recorded on the Communicare data breach record.

Depending on the nature of the breach the Information Commissioner's office and individual's concerned may need to be notified. The following factors should be taken into account to determine what actions need to be taken.

- How likely is the data breach to lead to a risk to people's rights, security or freedoms? E.g. What is the risk the data could be used for identify fraud or to gain access to a vulnerable person's home.
- How much data is involved?
- How vulnerable is the person whose data has been lost? E.g. will they understand the risk
- If a device was lost what was on it and was it encrypted?

If it is likely that there is a serious risk to people's rights and freedoms the Information Commissioner's office must be notified without undue delay, but not later than 72 hours after becoming aware of it.

### When do we need to tell individuals about a breach?

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR says we must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible.

---

<sup>2</sup> Definition from Information Commissioner's Office Guide to the General Data Protection Regulations  
<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr>

Individuals must be notified if there is a high risk to their rights or freedoms and especially if they may need to take steps to protect themselves from the effects of the breach. For example if they need to inform their bank.

If a decision is made not to report a breach a record of the incident and decision must be kept.

Following all serious incidents or if a pattern of small incidents develops senior staff and or trustees shall review policies and procedures to reduce the risk of further occurrences.

## **7. Data Security**

The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used.

Communicare in Southampton will regularly review how data is processed to ensure it processed securely.

- encrypt and password protect all portable devices which will be used for personal data
- ensure databases and other similar files are password protected as necessary

## **8. Rights for individuals**

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

The rights to data portability (6) and in relation with automated decision making and profiling (8) do not apply to activities carried out by Communicare in Southampton.

## **Right to be informed**

Data subjects have a right to be informed about how their data is processed. This includes how their data has been collected, what the legal basis is for processing, how it will be used, how long it will be kept and whether it will be passed on to a third party. We will also include information about how to request access to this information and how to opt out of direct marketing if applicable.

Communicare in Southampton will take reasonable steps to ensure the identity of the person making the request before releasing information.

## **Privacy Notices**

Communicare in Southampton will provide most of this information in the form of a privacy notice tailored to each category of data subject. We will endeavour to ensure this is written in clear, understandable English. Where the data is provided directly by the individual this will be given at the time or in the case of information given over the phone posted within a week. When the information is received via a third party such as a referrer this information will be passed on as soon as possible but within one month of receiving the data.

## **Right of access**

Communicare in Southampton recognises the right of individuals to confirm that data about them is held by Communicare in Southampton and to receive a copy of this data. Information about how to do this will be included in privacy notices. In accordance with GDPR guidance Communicare in Southampton may charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

## **Right to Rectification**

Communicare in Southampton recognises that individuals are entitled to have personal data rectified if it is inaccurate or incomplete. In accordance to GDPR guidelines we will respond to such requests within one calendar month.

If personal data in question has been disclosed to others Communicare in Southampton will contact each recipient and inform them of the rectification - unless this proves impossible or involves disproportionate effort. Communicare in Southampton does not normally disclose information to third parties but if it does this must be recorded so that this can be carried out.

## **The Right to Erasure / the right to be forgotten**

Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.



- When the individual withdraws consent if consent was the basis upon which the data was processed.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.

Communicare in Southampton uses 'legitimate purposes' as the basis for processing most data, therefore Communicare can refuse to comply with request to have data erased. Communicare in Southampton can also refuse if the data may reasonably be needed in the exercise or defence of legal claims.

If a request for erasure is made it will be considered using the following points

- Is the data needed for the exercise or defence of legal claims? If yes may be kept but must be reasonably likely to be needed.
- Was the data legally collected? If no it must be erased.
- Was the data collected upon the basis of consent (this is only likely to relate to voting membership and supporters information)? If yes it must be erased.
- If the basis of collection was legitimate interest does the legitimate interest of Communicare in Southampton to keep and process the data outweigh the rights of the individual to have it erased?

If the decision is made to refuse the request this must be explained in writing.

Communicare in Southampton will consider whether it would be appropriate to destroy some of the data for example removing contact details from the database or store it only in a secure back up file (restrict processing).

There are some specific circumstances where the right to erasure does not apply and you can refuse to deal with a request.

### **The right to restrict processing**

Where an individual contests the accuracy of the personal data, Communicare in Southampton will restrict the processing until we have verified the accuracy of the personal data.

Where an individual has objected to the processing (where it was necessary for the purpose of legitimate interests), and we are considering whether our organisation's legitimate grounds override those of the individual processing will also be restricted.

### **Right to object to processing**

Individuals have the right to object to their data being processed for direct marketing. This includes promotional newsletters and information about fundraising activities. Communicare in Southampton will develop and adhere to procedures to ensure that data subjects can easily object to receiving direct marketing and that if they do object marketing is not sent.

## Communicare in Southampton Data Protection Policy

This will include

- people will only be signed up for email distribution lists on an 'opt in' basis
- registration forms for events etc. will include appropriate 'opt in' boxes to receive further information
- emails sent out for promotional or fundraising purposes will include clear instructions as to how to stop receiving such emails
- posted newsletters will include instructions for contacting us to opt out of receiving future promotional or fundraising material

Individuals can also object to the processing of data for other purposes on "grounds relating to his or her particular situation". Communicare in Southampton will consider any such requests on an individual basis.