# Data Protection Policy

Community Southwark collects and uses information about members and other organisations and individuals who we come into contact with as we carry out our work. This information must be collected and dealt with appropriately– whether on paper, electronically, or recorded on other material - and there are safeguards to ensure this under the Data Protection Act 1998.

**Data collection**

Community Southwark will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form

When collecting data, Community Southwark will ensure that the Individual/Service User:

a) Clearly understands why the information is needed

b) Understands what it will be used for and what the consequences are should the Individual/Service User decide not to give consent to processing

c) As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed

d) Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress

e) Has received sufficient information on why their data is needed and how it will be used

Information and records relating to service users will be stored securely and will only be accessible to authorised staff and volunteers.

Information will be stored for only as long as it is needed and will be disposed of appropriately.

It is Community Southwark's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

## Data access and disclosure

All Individuals/Service Users have the right to access the information we hold about them. Community Southwark will also take reasonable steps to ensure that this information is kept up to date by asking data subjects whether there have been any changes.

Community Southwark will not share data with other organisations. The only circumstances where Community Southwark can disclose data without the data subject's consent are where the data subject has already made the information public.

In addition Community Southwark is committed to:

- meeting our legal obligations as laid down by the Data Protection Act 1998
- ensuring that data is collected and used fairly and lawfully
- taking steps to ensure that personal data is up to date and accurate
- establishing appropriate retention periods for personal data
- ensuring that data subjects' rights can be appropriately exercised
- providing adequate security measures to protect personal data
- observe fully conditions regarding the fair collection and use of information;
- collect and process appropriate information only to the extent that it is needed to fulfil our operational needs or to comply with any legal requirements
- ensuring the quality of information used
- ensuring that the information is held for no longer than is necessary
- ensuring that the rights of people about whom information is held can be fully exercised under the Act (i.e. the right to be informed that processing is being undertaken, to access one's personal information; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as wrong information)
- taking appropriate technical and organisational security measures to safeguard personal information
- ensuring that personal information is not transferred abroad without suitable safeguards.

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 made to the Data Protection Act 1998.

## Data protection principles

1. Personal data shall be processed fairly and lawfully

2. Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
4. Personal data shall be accurate and, where necessary, kept up to date
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998
7. Appropriate technical and organisational measures shall be taken against unauthorised and unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

**Definitions**

"Personal data" is information that relates to an identifiable person who can be directly or indirectlyidentified from that information, for example, a person's name, identification number, location, onlineidentifier. It can also include pseudonymised data."Special categories of personal data" is data which relates to an individual's health, sex life, sexualorientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includesgenetic and biometric data (where used for ID purposes)."Criminal offence data" is data which relates to an individual's criminal convictions and offences."Data processing" is any operation or set of operations which is performed on personal data or on sets ofpersonal data, whether or not by automated means, such as collection, recording, organisation,structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure ordestruction.

**Employee Rights**

You have the following rights in relation to the personal data we hold on you:a) the right to be informed about the data we hold on you and what we do with it;b) the right of access to the data we hold on you. More information on this can be found in

thesection headed "Access to Data" below and in our separate policy on Subject Access Requests"; c) the right for any inaccuracies in the data we hold on you, however they come to light, to becorrected. This is also known as 'rectification'; d) theright to have data deleted in certain circumstances. This is also known as 'erasure'; e) the right to restrict the processing of the data; f) the right to transfer the data we hold on you to another party. This is also known as 'portability'; g) the rightto object to the inclusion of any information;h) the right to regulate any automated decision-making and profiling of personal data. More information can be found on each of these rights in our separate policy on employee rights under GDPR.

**Responsibilities**

In order to protect the personal data of relevant individuals, those within our business who must processdata as part of their role have been made aware of our policies on data protection.We have also appointed employees with responsibility for reviewing and auditing our data protection
systems.G)

**Lawful Basis of Processing**

We acknowledge that processing may be only be carried out where a lawful basis for that processingexists and we have assigned a lawful basis against each processing activity.Where no other lawful basis applies, we may seek to rely on the employee's consent in order to processdata.However, we recognise the high standard attached to its use. We understand that consent must be freelygiven, specific, informed and unambiguous. Where consent is to be sought, we will do so on a specificand individual basis where appropriate. Employees will be given clear instructions on the desiredprocessing activity, informed of the consequences of their consent and of their clear right to withdrawconsent at any time.

**Access to Data**

As stated above, employees have a right to access the personal data that we hold on them. To exercisethis right, employees should make a Subject Access Request. We will comply with the request withoutdelay, and within one month unless, in accordance with legislation, we decide that an extension isrequired. Those who make a request will be kept fully informed of any decision to extend the time limit. No charge will be made for complying with a request unless the request is manifestly unfounded,excessive or repetitive, or unless a request is made for duplicate copies to

be provided to parties otherthan the employee making the request. In these circumstances, a reasonable charge will be applied.Further information on making a subject access request is contained in our Subject Access Requestpolicy.

**Data Discolosures**

The Company may be required to disclose certain data/information to any person. The circumstancesleading to such disclosures include: a) any employee benefits operated by third parties; b) disabled individuals -whether any reasonable adjustments are required to assist them at work; c) individuals' health data -to comply with health and safety or occupational health obligationstowards theemployee;d) for Statutory Sick Pay purposes; e) HR management and administration - to consider how an individual's health affects his or herability to do their job; f) the smooth operation of any employee insurance policies or pension plans;g) to assist law enforcement or a relevant authority to prevent or detect crime or prosecute offenders or to assess or collect any tax or duty. These kinds of disclosures will only be made when strictly necessary for the purpose.

**Types of Data Held**

We keep several categories of personal data on our employees in order to carry out effective and efficientprocesses. We keep this data in a personnel file relating to each employee and we also hold the datawithin our computer systems, for example, our holiday booking system.Specifically, we hold the following types of data:a) personal details such as name, address, phone numbers, b) information gathered via the recruitment process such as that entered into a CV or included in a CV cover letter, references from former employers, details on your education and employmenthistory etcc) details relating to pay administration such as National Insurance numbers, bank account detailsand tax codesd) medical or health informatione) information relating to your employment with us, including:i) job title and job description, sii) your salary, iii) your wider terms and conditions of employmentiv) details of formal and informal proceedings involving you such as letters of concern,disciplinary and grievance proceedings, your annual leave records, appraisal and performanceinformationv) internal andexternal training modules undertaken. All of the above information is required for our processing activities. More information on thoseprocessing activities are included in our privacy notice for employees, which is available from your manager.

**Third Party Processing**

Where we engage third parties to process data on our behalf, we will ensure, via a data processingagreement with the third party, that the third party takes such measures in order to maintain theCompany's commitment to protecting data.

**International Data Transfers**

We use systems to save and store your details with platforms that are based outside EEA, for example oncloud based Salesforce CRM database or cloud based Microsoft Office 365.M)

**Requirement To Notify Breaches**

All data breaches will be recorded on our Data Breach Register. Where legally required, we will report abreach to the Information Commissioner within 72 hours of discovery. In addition, where legallyrequired, we will inform the individual whose data was subject to breach.More information on breach notification is available in our Breach Notification policy

If you have any queries in relation to this policy, please email our Data Protection Policy Lead Jo Palmer at: info@communitysouthwark.org

Date: December 2018

Review Date: July 2022