Registered Charity No. 1101450
Company No. 4958843

DATA PROTECTION POLICY

Author: **Karen Mitchell**
Date: **April 2018**
Next review due **April 2019**

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 relevant legislation. This update covers the requirements of the GDPR (General Data Protection Regulations) which come into effect on 25th May 2018.

In case of any queries or questions in relation to this policy please contact the South Derbyshire CVS Data Protection Officer and Data Controller: Michelle Skinner , CEO

The Information Commissioner's Office (ICO) provides independent advice and guidance about data protection and freedom of information.

Regular updates can be found on its website www.ico.gov.uk

LINKS TO OTHER POLICIES

Please note this policy should be read in conjunction with other CVS policies

Acceptable use of ICT and the Internet Policy

Data Retention Policy

Safeguarding

1. INTRODUCTION

South Derbyshire CVS collects, transfers and processes personal information about staff, service users and other individuals who come into contact with the organisation. This information is gathered in order to enable it to provide support services and other associated functions to individuals and groups in the Local Community. In addition there may be a legal requirement to collect and use information to ensure that the organisation complies with statutory obligations.

This personal information must be collected and dealt with appropriately. South Derbyshire CVS has safeguards in place to ensure data is held in accordance with the Data Protection Act 1998 and is registered under the act as Data Controller with the Information Commissioner's Office (ICO). We have also reviewed our practice in light of the introduction of General Data Protection Regulations (GDPR).

As an organisation we process personal information to enable us to provide help and support to the community and offer advice on voluntary services; administer membership records; carry out fundraising to support the CVS and to manage our employees. A full copy of the registration can be found at https://ico.org.uk/ESDWebPages/Entry/Z8580156

In May 2018 the General Data Protection Regulations (GDPR) came into force. There were 2 key reasons why GDPR was introduced.

1. To bring all EU member states under one common regulation
2. To update regulations to reflect the new digital age as technology develops and personal data is being used and shared in new ways

As EU regulation is currently to be adopted this will not immediately change when the UK exits the European Union.

2. PURPOSE

This policy is intended to ensure that personal information is dealt with correctly, securely and in accordance with current related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed and irrespective of whether it is held electronically or in paper files.

All staff and volunteers involved with the collection, processing and disclosure of personal data will be made aware of their duties and responsibilities to adhere to this policy.

3. PERSONAL INFORMATION

Personal information or data is defined as data which relates to a living individual who can be identified from that data or other information held. GDPR aims to protect any personal data an organisation holds about an individual including name, address, e-mail address, images, social networking accounts,

IP address or medical history. It also covers more sensitive data such as sexual orientation and ethnicity.

4. DATA CONTROLLER

South Derbyshire CVS is Data Controller, which means that the organisation under the guidance of the CEO determines what purposes personal information held and will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

5. DATA PROTECTION PRINCIPLES

South Derbyshire CVS regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

South Derbyshire CVS intends to ensure that personal information is treated lawfully and correctly. To this end, we will continue to adhere to the 8 Principles of Data Protection, as detailed in the Data Protection Act 1998.

Specifically, make sure the information is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to people's data protection rights
- kept safe and secure
- not transferred outside the European Economic Area without adequate protection

CVS is committed to maintaining the above principles at all times. As well as adhering to the additional responsibilities placed on the organisation under 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."

Article 5(2) requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

Therefore we will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, why and with whom
- Check the quality and accuracy of the information we hold
- Ensure that information is not retained for longer than is necessary
- Ensure that obsolete information is destroyed and that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information
- Ensure all our staff and volunteers are aware of and understand our policies and procedures relating to Data Protection

4. Data Collection

Informed consent is when:-

- an individual/service user clearly understands why his/her information is needed, with whom it will be shared, the possible consequences of his/her agreeing or refusing the proposed use of the data

- and then gives his/her consent.

South Derbyshire CVS 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, South Derbyshire CVS 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 his/her data is needed and how it will be used

5. Data Storage

Information and records 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 or required by statute and will be disposed of appropriately.

It is the responsibility of South Derbyshire CVS 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 or scrapped.

6. Disclosure to Third Parties

South Derbyshire CVS may share data with other agencies such as the Local Authority, funding bodies and other voluntary agencies.

The Individual/Service User will be made aware in most circumstances how and with whom his/her information will be shared. There are circumstances where

the law allows South Derbyshire CVS to disclose data (including sensitive data) without the data subject's consent.

These are:

a) Carrying out a legal duty or as authorised by the Secretary of State

b) Protecting vital interests of an individual/service user or other person

c) The individual/service user has already made the information public

d) Conducting any legal proceedings, obtaining legal advice or defending any legal rights

e) Monitoring for equal opportunities purposes – i.e. race, disability or religion

f) Providing a confidential service where the individual/service user's consent cannot be obtained or where it is reasonable to proceed without consent, for example where we would wish to avoid forcing stressed or ill Individuals to provide consent signatures

7. Data Accuracy

South Derbyshire CVS will also take reasonable steps to ensure that information is kept up to date by asking data subjects whether there have been any changes when communicating with them.

In addition**,** South Derbyshire CVS will ensure that:-

- it has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection
- everyone processing personal information understands that they are contractually responsible for following good data protection practice
- everyone processing personal information is appropriately trained to do so
- everyone processing personal information is appropriately supervised
- it will regularly review and audit the ways it holds, manages and uses personal information
- all staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them

9. Data Breach

Any data breach will be reported to the relevant authorities within 72 hours and if there is risk involved to the data subject/s (the people the data concerns) they should also be informed.

10. Data Subjects' Rights and Access Requests

The 1998 Data Protection Act gave data subjects certain rights in relation to personal data held about them by others however this has been enhanced and strengthened by the GDPR.

The right to be informed – a data subject has a right to know how data about them will be used by an organisation

The right to access personal data held by an organisation – a data subject can ask the organisation to share any data they hold about them

The right to rectification – the data subject has the right to update any information held if it's inaccurate or if something is missing

The right to erasure – this means that the data subject has the right to request that an organisation delete any personal data they hold about them. There are some exceptions for example some information can be held by employers and ex employers for legal reasons. The data retention policy will have more information on this.

The right to restrict processing- if the data subject thinks that there is something wrong with the data held or if they believe the organisation may not be complying with the rules they can restrict further use of the data until they are satisfied that everything is in order.

The right to data portability – a data subject can request data held on them in a way that can be digitally read such as a PDF file of a hard copy document to enable them to share information with other organisations

The right to object – the data subject has the right to object to the way that data is being used for example data given to enable delivery of a service then used to enable marketing of an event. The CRM enables the recording of a contacts preferences and wishes

Rights in relation to automated decision making and profiling – this protects the data subject in cases where a decision is being made about them based entirely on an automated process rather than human input.

A data subject can write to the organisation requiring exercising any of the above rights and where processing or holding of data is likely to cause unwarranted substantial damage or substantial distress to them or another person.

However, this right is unavailable if any one of the following conditions for processing can be complied with:

- Data is necessary or the performance of a contract with the data subject
- There is a legal obligation
- To protect vital interests of the data subject

When a Data Subject Access request is received it should be logged against the contact record on the CRM, acknowledged and then responded to in writing within 21 days.

A data subject whose details are held has the right to receive a copy of information held about them. To obtain this information they will need to make a Data Subject Access Request in writing. They will then be entitled to be told whether the organisation is processing their personal data and if so be given:

- The personal data
- The purpose(s) for which it is being processed
- To whom the data is or maybe disclosed
- The source of the information
- Logic behind processing

A charge can be made to the individuals making Data Subject Access Requests as set down from time to time by the Information Commissioner. Requests should be responded to within 21 calendar days.

The following points should be noted:

- The data subject has the right to see all of their personal information unless covered by an exemption
- A copy of all information sent should attached to the Contact record on the CRM
- All codes should be explained
- Third party details should not be sent without written concent of the third party
- If dealing with a joint application parties must only be given their own information

Some information maybe exempt and the Data Subject should therefore be told "South Derbyshire CVS do not hold any personal data that I am required to reveal to you.

Further details of these exemptions are available from the Information Commissioner's Office

https://ico.org.uk/for-organisations/guide-to-data-protection/exemptions

More information on GDPR can be found at

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/

It includes links to relevant sections of the GDPR itself, to other ICO guidance and to guidance produced by the EU's Article 29 Working Party. The Working Party includes representatives of the data protection authorities from each EU member state, and the ICO is the UK's representative.

There are five recommendations compiled by the ICO specifically for charities.

This is the minimum expected from a charity under the GDPR:

1. Tell people what you are doing with their data and who it will be shared with
2. Make sure your staff are adequately trained on how to store and handle personal information
3. Use strong passwords (we would recommend always using a random password generator)
4. Encrypt all portable devices such as memory sticks and laptops
5. Only keep people's information for as long as necessary

CVS is working towards compliance with these recommendations.

Glossary of Terms

Data Controller – The person who (either alone or with others) decides what personal information will be held and how it will be held or used.

Data Protection Act 1998 – The UK legislation that provides a framework for responsible behaviour by those using personal information.

Data Protection Officer – The person(s) responsible for ensuring that South Derbyshire CVS follows its data protection policy and complies with the Data Protection Act 1998.

Individual/Service User – The person whose personal information is being held or processed by South Derbyshire CVS for example: a client, an employee, or supporter.

Explicit Consent – is a freely given, specific and informed agreement by an individual/service user in the processing of personal information about her/him. Explicit consent is needed for processing sensitive data.

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.

Processing – means collecting, amending, handling, storing or disclosing personal information.

Personal Information – Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers or employees.

Sensitive Data – refers to data about:-

- Racial or ethnic origin
- Political affiliations
- Religion or similar beliefs
- Trade Union membership
- Physical or mental health
- Sexuality
- Criminal record or proceedings.