Data protection policy

Introduction

SCDA needs to gather and use certain information about individuals.

Such individuals can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures SCDA:

- Complies with data protection law and follows good practice
- Protects the rights of staff, service users and individuals
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation and describes how organisations — including SCDA, must collect, handle and store personal information.

This regulation applies regardless of whether data is stored electronically, on paper or on other materials.

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

Policy scope

This policy applies to:

- All staff and volunteers of SCDA
- All contractors, suppliers and other people working on behalf of SCDA

It applies to all data and personal information that the company holds relating to identifiable individuals, even if that information technically falls outside of the GDPR. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- …plus any other information relating to identifiable individuals

Data protection risks

This policy helps to protect SCDA and individuals from some very real data security risks, including:

- **Loss or unavailability of personal information.** For instance data storage method being lost or made inaccessible.
- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with SCDA has some responsibility for ensuring data is collected, stored and handled appropriately. Failure to comply with the requirements of this policy will be viewed very seriously by SCDA, investigated thoroughly and may ultimately lead to disciplinary action being taken under SCDA's Disciplinary Policy and Procedure, up to and including dismissal.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **[data protection lead], Andy Millward,** is responsible for:
    - Keeping the board and Senior Management Team updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data SCDA holds about them (also called 'subject access requests').
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
    - Notifying the Information Commissioner of the data it holds or is likely to hold, and general purposes that this data will be used for

- The **Systems Administrator,** is responsible for:
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure security hardware and software is functioning properly.
    - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
- The **Marketing and Communication Officer,** is responsible for:
    - Approving any data protection statements attached to communications such as emails and letters.
    - Addressing any data protection queries from journalists or media outlets like newspapers.
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General Principles

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line managers.
- **SCDA will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from their line manager or the Data Protection Lead if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Data Protection Lead.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it. Whenever possible the secure place should be a locked filing cabinet, ideally kept in a room which is also locked when unattended.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Printed personal data should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing service**.
- Servers containing personal data should be **sited in a secure location.**
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should **never be saved directly** to the hard drive or local drive of laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

Data use

SCDA 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. SCDA intends to ensure that personal information is treated lawfully and correctly. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended by pressing "control, alt, del" and selecting "Lock" or "Lock this computer"
- Workstations must be protected by a **password protected screensaver** that automatically triggers after 5 minutes of inactivity
- Personal data **should not be shared informally** verbally or electronically. Care should be taken to avoid sending bulk details by email.
- Personal information must be **accessed only for approved business** purposes and on a "need to know" basis and should not be printed, copied or otherwise reproduced.
- Remember that **individuals now have the right of access** to the personal information we hold about them so care should be taken to use appropriate language when creating records.

- Data shall not be **transferred to a country or territory** outside the European Economic Area
- Data must be **encrypted before being transferred electronically**. The Systems Administrator can explain how to send data to authorised external contacts.
- Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.
- Printers should be **switched off and locked** outside working hours. Printed materials containing personal information must be collected immediately by the originator or an approved representative.
- **Incoming and outgoing mail** collection points must be supervised so that letters cannot be stolen or lost.

Data accuracy

The law requires SCDA to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets. For example; when sending data via email, whenever possible send a hyperlink rather than attach a document which will prevent multiple copies of the data being created.
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a service user's details when they meet with them.
- SCDA will make it **easy for data subjects to update the information** we hold about them as described in our *Privacy Notice (Include link)*.
- Data should be **updated as inaccuracies are discovered and the correct data verified**. For instance, if a service user can no longer be reached on their stored telephone number, the new number should be verified and recorded and the old number should be removed from the database.

Data Breach Reporting Plan

SCDA takes its responsibilities for the security of personal information very seriously and will take all reasonable steps to ensure personal data is processed securely and remains available upon request. As part of this approach regular testing will be carried out to ensure this policy is being followed and that data processing and storage methods are secure. Such approaches will include spot checks and audits of manual and electronic systems and 6 monthly penetration tests of our IT system.

The following would constitute a data breach;

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction)

- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

If a data breach is discovered, or suspected, it should be reported, as soon as is practicably possible, to the Data Protection Lead or a member of SMT. If we are not the Data Controller we will report the incident to them as soon as is practicably possible and then follow the process described below. If we are the Data Controller the following process only applies.

A Data Breach Report *(..\Data Breach\Data Breach Report.docx)* should be completed by the reporting person and sent to the Data Protection Lead. Whether actual or suspected the breach will be fully investigated by the Data Protection Lead, or a member of the SMT, within such a timeframe as to enable reporting to ICO within 72 hours if required.

Following investigation the following decisions will be made and acted on.

- Is the breach likely to result in a high risk to the rights and freedoms of individuals?
- Are we required to report the incident to the ICO?
- Do we need to contact the individual's affected?
- What steps, if any, can we take to mitigate or minimise the impact of the data breach?
- What steps can we take to prevent reoccurrence?

An investigation report, containing findings and recommendations for improvement/change will be prepared by the Data Protection Lead and presented to SMT for consideration.

A log of actual and suspected data breaches will be maintained by the Data Protection Lead and presented to SMT on a regular basis for discussion and review.

Subject access requests

All individuals who are the subject of personal data held by SCDA are entitled to:

- Ask **what information** the company holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the company is **meeting its data protection obligations**.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the Data Protection Lead at dataprotectionofficer@sussexcommunity.org.uk . Staff wishing to make a subject access request should contact the HR department at hr@sussexcommunity.org.uk .

The Data Protection Lead will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the General Data Protection Regulation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, SCDA will disclose requested data. However, we will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

If you are contacted by anyone seeking disclosure of data please discuss with your line manager or the Data Protection Lead prior to any disclosure. Failure to comply with this may result in a data breach which in turn may be subject to investigation and possible disciplinary action, in line with the organisation's Disciplinary Policy

Providing information

SCDA aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To this end SCDA has written a Privacy Notice setting out how data relating to individuals is processed. A copy of the SCDA Privacy Notice is available on our website.

Date of Policy	December 2011
Date of Policy Review	April 2021
To be reviewed again	April 2022
Policy reviewed by	Data Protection Lead/HR
Policy ratified by	HR Sub-Committee/SCDA Board