Context and overview

Key Details

- Policy prepared by: Lizzy Pratt
- Approved by Board on: March 2, 2022
- Policy became operational on: April 6, 2022

Introduction

The Support Network needs to gather and use certain information about individuals.

These can include students, alumni, board members, business contacts, employees and other people the organization 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 organization's data protection standards — and to comply with the law.

Why This Policy Exists

This data protection policy ensures The Support Network:

- Follows good data protection practice
- Protects the rights of staff, students, alumni and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

People, Risks and Responsibilities

Policy Scope

This policy applies to:

- All offices of The Support Network
- All staff and volunteers of The Support Network

It applies to all data that the organization holds relating to identifiable individuals. This can include, but is not limited to:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers

Data Protection Risks

This policy helps to protect The Support Network from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the organization uses data relating to them.
- **Reputational damage.** For instance, the organization could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with The Support Network has responsibility for ensuring data is collected, stored and handled appropriately.

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 **Board of Directors** is ultimately responsible for ensuring that The Support Network meets its legal obligations.
- The **Data Protection Officer, Lizzy Pratt,** is responsible for:
    - Keeping the board 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 The Support Network holds about them (also called 'subject access requests').
    - Checking and approving any contracts or agreements with third parties that may handle the organization's sensitive data.
- The **IT Manager, Ben Lowenstein,** 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 organization is considering using to store or process data. For instance, cloud computing services.
- The **Marketing Manager, Sarah Dalley,** 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 Staff Guidelines

- 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, board members, and volunteers can request it through board agreement.
- **The Support Network will provide training** to all employees and applicable volunteers to help them understand their responsibilities when handling data.
- Employees and volunteers 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 unauthorized people, either within the organization 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 and volunteers **should request help** from the board or the data protection officer 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 IT manager or data controller.

When data is **stored on paper,** it should be kept in a secure place where unauthorized people cannot view.

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 unauthorized people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

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

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a USB drive), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers**, and, in the event necessary, should only be uploaded to reputable **cloud computing services.**
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the organization's standard backup procedures.
- All servers and computers containing data should be protected by **security software and a firewall**.

Data Use

Personal data is of no value to The Support Network unless the business can make use of it. 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.
- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.
- Personal data should **never be transferred outside of the United States**.
- If volunteers or employees **save copies of data to their own computers** for use with credible external programs, it should be **deleted immediately thereafter.** Always access and update the central copy of any data.

Data Accuracy

The law requires The Support Network to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort The Support Network should put into ensuring its accuracy.

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.
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they email and allowing an opt-out.
- The Support Network will make it **easy for data subjects to update the information** The Support Network holds about them. For instance, via the organization website form.
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Subject Access Requests

All individuals who are the subject of personal data held by The Support Network are entitled to:

- Ask **what information** the organization 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 organization is **meeting its data protection obligations**.

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

Subject access requests from individuals should be made via The Support Network website.

The data controller will aim to provide the relevant data within 14 days.

The data controller 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 Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, The Support Network will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the organization's legal advisers where necessary.

Providing Information

The Support Network 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 (such as via an opt-out in emails)

To these ends, the organization makes this document available via The Support Network website.