Data Protection, Privacy & GDPR Policy

Context and overview

Key details

- Policy Prepared by :- Melanie Lawlee
- Approved by Ofsted : 09/10/2017
- Policy became operational on: 24/01/2023
- Planned review date: 24/01/2024

Introduction

Safe Hands After School Club needs to gather and use certain information about individuals and businesses.

These can include customers, suppliers, business contacts, employees and other people that Safe Hands After School Club 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 current law.

Why this policy exists

This data protection policy ensures Safe Hands After School Club;

- Complies with data protection law and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals and businesses data
- Protects itself from the risks of a data breach

Data protection law

The Data Protection Act 1998 describes how organizations including Safe Hands After School Club must collect, handle and store personal and business information.

These rules apply regardless of whether data is stored electronically, on paper or other formats or materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. They say that personal and business data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not to be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not to be transferred outside the European Economic area (EEA) unless that country or territory also ensure adequate levels of protection

People, risks and responsibilities

Policy scope

This policy applies to;

- Safe Hands After School Club
- All staff and volunteers
- All contractors, suppliers and others working on behalf of the company such as Ofsted. Copies of these policies are available on request.

Policy scope cont'd

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include;

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Banking data
- Documents such as drivers' licenses/passports
- Images taken during events

Data protection risks

This policy helps to protect Safe Hands After School Club from some very real data 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 company uses data relating to them.
- **Reputational damage**. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Safe Hands After School Club has some 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 Company Owner is ultimately responsible for ensuring that Safe Hands After School Club meets its legal obligations
- The Data Protection Officer, Mel Lawlee 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 that Safe Hands After School Club holds about them. This is also called 'subject access requests')
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
    - Ensuring all systems, services and equipment used for storing data meets 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
    - Approving any data protection statements attached to communications such as emails and letters.
    - Addressing any data protection queries from journalists or media outlets such as newspapers
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles

General staff guidlines

- 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
- **Safe Hands After School Club will provide training** to all employees, as necessary, 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 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 your line manager or data controller.

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

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 cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorised persons could see them,** such as on the printer.
- Data printouts 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.
- If data is stored on removable media such as a CD or memory stick, these should be kept **locked away securely** when not being used.
- Data should only be stored on **designated drivers and servers**, and should only be uploaded to **an approved cloud computing service**.
- 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 company's standard backup procedures.
- Data should **NEVER be saved directly** to laptops or other mobile devices such as smart phones or tablets.
- All servers and computers containing data should be protected by **approved security software and a firewall.**

Data use

Personal data is of no value to Safe Hands After School Club 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.
- Data must be **encrypted before being transferred electronically**.
- Personal data should **never be transferred outside of the European Economic** area.
- Employees **should not save copies** of personal data to their own computers. Always access and update the central copy of any data.

Data accuracy

The law requires Safe Hands After School Club to take reasonable steps to ensure data is kept accurate and up to date.
The more important it is that the personal data accurate, the greater the effort Safe Hands After School Club 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 call.
- Safe Hands After School Club will **make it easy** for data subjects to update the information Safe Hands After School Club holds about them.
- 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.
- It is the business owners **responsibility to ensure marketing databases are checked against industry suppression files** every 6 months

Subject access requests

All individuals who are the subject of personal data held by Safe Hands After School Club are entitled to

Ask wh**at 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 any 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 controller. The data controller can supply a standard request form, although individuals do not have to

do this. The data controller (business owner) 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, Safe Hands After School Club will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the companies' legal advisors where necessary.

Providing information

Safe Hands After School Club 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 these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

What do we store and how

What information do we collect, how do we use it and store it?

Customer contact details including mobile numbers, addresses and email.

We collate customer details and store them electronically on our secure cloud invoicing system and mailchimp for information forwarding. It is also pulled through to our online ordering site. The servers are secure and offsite. The information is only used in order to complete the service of childcare and important information sharing. We only use this information to send internal marketing and business specific emails, which can be opted out of at any time. This information is not imparted to any other companies for marketing purposes.

Staff Information

Information held on staff includes drivers' licenses, bank details, contact details, conviction information, disciplinary information and contact details for their emergency contacts. This is stored both electronically and on paper securely

GDPR Compliance

GDPR Compliance

- We have reviewed the purposes of our processing activities, and selected the most appropriate lawful basis for each activity
    a. Personal data being held for HR and Payroll – **Lawful basis for processing is CONTRACT** as in order to fulfill our staff contracts including bank details for payroll.
    b. Client information held - **Lawful basis for processing is CONTRACT** the data we hold in order to fulfill our contract to supply child care services and supply account information for payment
    c. Newsletter – **Lawful basis for processing is CONSENT** the data we hold in order to inform our clients of important product and business information. Consent has been requested
    d. Suppliers of goods In - **Lawful basis for processing is CONTRACT** information is held in order to mange goods processing and payments to fulfill our contract

We agree that we have completed the following, much of which is detailed within this policy.

- We have checked that the processing is necessary for the relevant purpose, and are satisfied that there is no other way to achieve that purpose
- We have documented our decision on which lawful basis applies to help us demonstrate compliance
- WE have included information about both the purposes of the processes and the lawful basis for the processing in our **Data Protection, Privacy and GDPR Policy**.