Martin Shenton
Health & Safety Consultant - Accident Investigation
SAFETY MATTERS HSE
Tel: 07976 213 812 - Email: martin@safetymatters.org - Web: safetymattershse.org

DATA PROTECTION POLICY

Safety Matters HSE has a legal duty of confidence to the children and young people in their care under the **General Data Protection Regulation (GDPR).**

1 - CONTEXT & OVERVIEW

KEY DETAILS:

- Policy Prepared by:
- Approved by:
- Policy became operational on:
- Next review date:

INTRODUCTION

Safety Matters HSE needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other persons the organisation has a relationship with or may need to contact. These policies describe how this personal data is collected, handled and stored to meet the company's data protection standards, and comply with the law.

WHY THIS POLICT EXISTS

This data protection policy ensures Safety Matters HSE :

- 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' data
- Protects itself from the risks of a data breach

DATA PROTECTION LAW

General Data Protection Regulation (GDPR) 2018 describes how organisations including Safety Matters HSE must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully. **GDPR** is underpinned by eight important principles. These say that:

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 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 be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

2 - PEOPLE, RISKS & RESPONSIBILITIES

POLICY SCOPE

This policy applies to:

- The Safety Matters HSE office
- All staff and volunteers of Safety Matters HSE
- All contractors, suppliers and other people working on behalf Safety Matters HSE

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the **General Data Protection Regulation (GDPR) 2018**. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Any other information relating to individuals

DATA PROTECTION RISKS

This policy helps to protect Safety Matters HSE from some what is potentially 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 company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

The procedure for dealing with members of staff who breach date security we have to inform the data protection authority – **ICO (Information Commissioners Office)** within 72 hours of becoming aware. **Contact 0303 123 111 3 or the ICO website.**

RESPONSIBILITIES

Everyone who works for or with Safety Matters HSE has some responsibility for ensuring data is collected, stored and handled appropriately.

Each person or 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:

1. The **board of directors** is ultimately responsible for ensuring that Safety Matters HSE meets its legal obligations.

2. The **Data Protection Officer,** Martin Shenton 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 Safety Matters HSE 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.

3. The IT Manager, Anthony Kelly 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 Manager, Martin Shenton 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.

3 - GENERAL STAFF GUIDELINES

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **is not be shared informally**. When access to confidential information is required, employees can request it from their line managers.
- Safety Matters HSE **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 officer if they are unsure about any aspect of data protection.

4 - DATA STORAGE

These rules describe how and where data is safely stored.

In most situations REGENT PARK STUDIOS **stores data on paper.** This is kept in a secure place and where unauthorised people cannot see it. The information is kept for a period in line with the **Childens Act 2004**. Limited amounts of data are stored electronically.

- When not required, paper or files are kept **in a secure drawer**.
- Employees should make sure paper and printouts are **not left where unauthorised 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 unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** and changed regularly
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
- Data is only be stored on **designated drives**, and is never uploaded to the cloud.
- Electronic information containing personal data is located only in the main offce and is not available in any space used by general public.
- Data is assessed and **backed up where necessary or deleted**. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should **never be saved directly** to mobile devices like tablets or smart phones.
- All computers containing data should be protected by approved security software and a firewall.

5 - DATA USE

Personal data is of no value to REGENT PARK STUDIOS unless the business can make use of it and limited information is kept electronically.

- 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 is never transferred or shared outside of governing bodies in the region of Lancashire.
- Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

6 - DATA ACCURACY

The law requires REGENT PARK STUDIOS 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 REGENT PARK STUDIOS 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.**
- 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.

7 - SUBJECT ACCESS REQUEST

All individuals who are the subject of personal data held by REGENT PARK STUDIOS 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 controller at **info@regentparkstudios.co.uk**. The data controller can supply a standard request form, although individuals do not have to use this.

Individuals will be charged £10 per subject access request. 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.

8 - 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. Safety Matters HSE will not disclose information to another party under any circumstances. An exception can only be made in respect of the Government, Local Authorities and police.

9 - PROVIDING INFORMATION

Safety Matters HSE 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. This is available on request. A version of this statement is also available on the company's website.