eSafety4schools

DATA PROTECTION POLICY

Context and Overview

Key Details

- Policy prepared by: Paul McCarthy
- Date approved: 19th April 2017
- Date Reviewed: 27th April 2018 (To reflect GDPR requirements)
- Review Date: 1st May 2019

Introduction

eSafety4schools needs to gather and use certain information about individuals.

This 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 standard – and to comply with the law.

Why this policy exists

This data protection policy ensures Capital Bytes Limited trading as eSafety4schools:

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

Data protection law

eSafety4schools recognises the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) adopted 27 April 2016, the transition period and the application date of 25 May 2018.

The GDPR legislates eight data rights for individuals in addition to those laid out by The Data Protection Act 1998:

1. **Right to be informed** – You must be clearly informed when your data is collected and the purpose for which it is intended.
2. **Right of access** – You must be allowed to view the data companies have gathered on you.
3. **Right to rectification** – You have the right to correct erroneous information about yourself in a company's data records.
4. **Right of erasure** – Also known as the "right to be forgotten". You have the right to request the deletion of personal data held on you, although this right is not absolute.
5. **Right to restrict processing** – You can request the suppression of your personal data file or restrict its processing.
6. **Right to data portability** – You have the right to take the data a company has collected on you and share it elsewhere, e.g. to get a better customer deal.
7. **Right to object** – You have the right to object and prevent your data being used for particular purposes, e.g. for direct marketing. This right is superseded by legal claims.
8. **Rights related to automatic decision-making** – You may only be profiled with your explicit consent, where this is necessary to enter into a contract or where such processing is authorised by the state.

The Data Protection Act 1998 describes how organisations, including eSafety4schools, 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.

The Data Protection Act is underpinned by eight important principles. These say that personal 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 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 transferred outside the European Economic Area (EEA), unless that country or territory also ensure an adequate level of protection

People, risks and responsibilities

Policy scope

This policy applies to:

- The head office of eSafety4schools
- All branches and locations of eSafety4schools
- All staff and volunteers of eSafety4schools
- All contractors, suppliers and other people working on behalf of eSafety4schools

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
- …plus, any other information relating to individuals

Data protection risks

This policy helps to protect eSafety4schools 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 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 eSafety4schools has some responsibility for ensuring data is collected, stored and handled appropriately.

- The Data Protection Officer 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 those 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 eSafety4schools holds about them (subject access requests).
    - Checking and approving any contracts or agreements with third parties that may handle the company’s sensitive data.

- The IT Director, Roy Jorgensen, 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 Director, Matthew Holt, is responsible for:
  - Approving any data protection statements attached to communications such as emails and letters.
  - Addressing any data protection queries from journalists and media outlets.
  - 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 can request it from their line managers.
- eSafety4Schools will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, 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 IT manager or the data protection officer.

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 filing cabinet.**
- 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** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD/DVD or flash/external drive), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers,** and should only be uploaded to **approved cloud computing services.**
- Servers containing personal data should be **sited in a secure location,** separate from the general office space.
- Data should be **backed up frequently.** Those backups should be tested regularly, in line with the company's standard back up procedures.
- Data should **never be saved directly** to 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

Personal data is of no value to eSafety4schools 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 eSafety4schools 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.
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call.
- eSafety4schools will make it **easy for data subjects to update the information** eSafety4schools 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 marketing manager's responsibility to ensure **marketing databases are checked against industry suppression files** every six months.

Subject access requests

All individuals who are the subject of personal data held by eSafety4schools are entitled to:

- Ask **what information** the company hold 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 officer at dpo@esafety4schools.com.

Individuals will be charged £25 per subject access request. The data protection officer will aim to provide the relevant data within 14 days.

The data protection officer 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, eSafety4schools will disclose requested data. However, the data protection officer will ensure the request is legitimate.

Providing information

eSafety4schools 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.