ST-EDS
Employability skills for young people

GDPR POLICY (General Data Protection Regulation)

Introduction

St Edmunds Society needs to gather and use certain information about individuals.

These can include students, 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 Society's data protection standards — and to comply with the law. The Society is registered with the Information Commissioners Office (ref ZA122888)

We may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding.

Why this policy exists

This data protection policy ensures St Edmunds Society

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

The GDPR Policy states that the data we keep is:

- processed lawfully, fairly and in a transparent manner in relation to individuals

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and

organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals

- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The lawful basis under which we process data are

Consent: the individual has given clear consent for us to process their personal data for a specific purpose.

Contract: the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.

Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations).

Vital interests: the processing is necessary to protect someone's life.

Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Policy scope

This policy applies to:

- The head office of St Edmunds Society
- All branches or offices of St Edmunds Society
- All staff and volunteers of St Edmunds Society
- All contractors, suppliers and other people working on behalf of St Edmunds Society

Data protection risks

This policy helps to protect St Edmunds Society 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 society uses data relating to them.
- **Reputational damage.** For instance, the society could suffer if hackers successfully gained access to sensitive data.

Responsibilities

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with relevant legislation.

It applies to all computerised data and manual files if they come within the definition of a filing system. Broadly speaking, a filing system is one where the data is structured in some way that it is searchable on the basis of specific criteria (so you would be able to use something like the individual's name to find their information), and if this is the case, it does not matter whether the information is located in a different physical location.

Everyone who works for or with St Edmunds Society has some responsibility for ensuring data is collected, stored and handled appropriately.

- The Data 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 as required
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data St Edmunds Society holds about them (also called 'subject access requests').
    - Checking and approving any contracts or agreements with third parties that may handle the society's sensitive data.
- The Society employ IT Company Browntech who are 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 society is considering using to store or process data. For instance, cloud computing services.
- Staff are 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 can request it from their line managers.
- St Edmunds Society will provide training as required 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 society 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.
- Ensuring that the same guidelines apply when working from home as required by the Society.

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT Supplier 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 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, Memory stick), 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 an approved 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 society's standard backup 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 Storage

Personal data is of no value to St Edmunds Society 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. The IT manager can explain how to send data to authorised external contacts.
- 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 St Edmunds Society 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 St Edmunds Society 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.
- St Edmunds Society will make it easy for data subjects to update the information St Edmunds Society holds about them. For instance, by speaking to the Data Controller.
- 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.
- There is a responsibility to ensure marketing databases are checked regularly.

Subject Access Requests

All individuals who are the subject of personal data held by St Edmunds Society are entitled to:

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

If an individual contacts the Society 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 admin@st-eds.org.uk. The data controller can supply a standard request form, although individuals do not have to use this.

Individuals may be charged a reasonable fee for a subject access request. The data controller will aim to provide the relevant data without undue delay depending on the complexity of request.

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.

For safeguarding reasons if we believe a young person is at risk of harm we can breach any Data Protection regulations in the best interest of the young person.

Under these circumstances, St Edmunds Society will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the Society's legal advisers where necessary.

Providing Information

St Edmunds Society 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 Society has a privacy statement, setting out how data relating to individuals is used by the Society.

The Society also has a privacy statement relating to students.

St Edmunds Society

Lead Data Protection Officer – Debbie Grantham

Deputy Data Protection Officer – Andy Risborough