DATA PROTECTION POLICY

Key details

- Policy Prepared by: Stowmarket ASD Saturday Clubs
- Policy Became Operational: 25th May 2018
- Policy was last updated: 27th May 2022

Introduction

Stowmarket ASD Saturday Club needs to gather and use certain information about members. These can include the young people, parents, carers and other relations, suppliers, business contacts, employees, volunteers, committee members, sub-contractors and other people the company has a relationship with or need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the data protection standards and comply with the law.

Why this policy exists

This data protection policy ensures Stowmarket ASD Saturday Clubs:

- 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 individuals' data
- Protects itself from the risk of a data breach

Data protection law

The Data Protection Act 1998 and the General Data Protection Regulations Act 2018 describes how organisations, including Stowmarket ASD Saturday Clubs must handle, collect and store personal information.

These rules must 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:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not over excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of security

Policy scope

This policy applies to:

- The General Manager of Stowmarket ASD Saturday Clubs
- The Committee of Stowmarket ASD Saturday Clubs
- All staff and volunteers of Stowmarket ASD Saturday Clubs
- All other people working on behalf of Stowmarket ASD Saturday Clubs
- Members and families of Stowmarket ASD Saturday Clubs

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 and the General Data Protection Regulations Act 2018. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone Numbers
- Other information relating to individuals. (Including Registration forms, Care plans, behaviour records, safe guarding information and other personal records)

Data protection risks

This policy helps to protect Stowmarket ASD Saturday Clubs 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 information relating to them
- **Reputation damage –** for instance, the company and those it stores data about, could suffer if unauthorised access was gained to sensitive data.

Responsibilities

Everyone who works with Stowmarket ASD Saturday Clubs has a responsibility for ensuring data is collected, stored and handled appropriately.
Each individual that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

Leah Bowers is the named Data Controller and is responsible for:

- Ensuring that Stowmarket ASD Saturday Club meets its legal requirements
- 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 anyone covered by this policy
- Dealing with requests from individuals to see the data Stowmarket ASD Saturday club 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.
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards
- Performing regular checks to ensure security hardware and software is functioning properly (or if delegated, checking that this has been carried out).
- Evaluating any third-party services the company is considering using to store and process data, for instance cloud storage / backup services.
- Approving data protection statement attached to communications such as emails & letters.
- Addressing any data protection queries from staff, clients or the media
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General staff and sub-contractors 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, staff and sub-contractors can request it from the General Manager.

- Stowmarket ASD Saturday Clubs will provide training to all employees to help them understand their responsibilities when handling data.
- Employees and sub-contractors should keep all data secure, by taking sensible precautions and following 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 destroyed.
- Employees and sub-contractors **should request help** from the director if they are unsure about any aspect of data protection.

Data storage
These rules describe how and where data should be safely stored. Queries or concerns about storing data safely can be sent to the General Manager.

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, filing cabinet or folder.**
- Employees should make sure paper and printouts are **not left where unauthorised people can see them**.
- **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 or malicious attempts to access it:
- Sensitive data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on a removable media** (e.g. CD, DVD or data key) these should be kept locked away securely when not being used. USB sticks should be password protected/encrypted.
- Data should only be stored on **designated laptops, drivers or servers** and should only be uploaded to an **approved cloud computing service** which meets GDPR requirements.
- Servers containing personal data should be **sited in a secure location,** away from general office space,
- Data should be **backed up frequently.** These backups should be tested regularly and kept securely.
- Data should **never be saved directly** to mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by an **approved security software and firewall.**

Data use
In order to minimise the risks of loss, corruption, theft or misuse:
- 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 should be encrypted before being transferred electronically.**
- Personal data should **not be transferred outside of the European Economic Area, i.e. online storage/backup, unless encrypted before it leaves the server or the area meets the standards as set out within the GDPR.**

- Employees **should not save copies of personal data to their personal computers, laptops, phone or tablets.**

Data accuracy
The law requires Stowmarket ASD Saturday Clubs 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 accurate and as 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 members / family details when they call.
- Stowmarket ASD Saturday Clubs will make it **easy for parents and carers to update information** held 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.

Disposing of data
Data will only be stored whilst it is relevant.

Anyone who considers there data may be store unnecessarily or wish to have their data removed can make a **request** for erasure. Requests should be made in writing and specify the data to be removed; all requests will be executed within one month of being received.

Disposing of data may involve:
- Shredding of paper copies
- Deleting files from computers
- Deleting contact details from all devices

If a computer, phone or tablet is to be discarded, data on its hard-drive(s) will be securely destroyed currently by using a third party professional (certificates will be obtained)

Subject access requests
All individuals who are the subject of personal data held by Stowmarket ASD Saturday Clubs 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 and protecting its data protection obligations.**

If an individual contacts the club 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 leah@stowmarketsaturdayclub.co.uk .
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.
Due to the way we run the most likely way this will happen is face to face.

Disclosing data for any other reason
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, Stowmarket ASD Saturday Clubs will disclose requested data. However, the data controller will ensure the request is legitimate, seeking advice from the committee where necessary.

Providing information
Stowmarket ASD Saturday Clubs has privacy notices for both the workforce and clients. These notices ensure that both are aware of how data is being processed, how it is being used and how to exercise their rights.

Copies of these notices are available upon request.

This policy was updated on 27th May 2022 by Leah Bowers General Manager.