Data Protection Policy for Squash Link

Context and overview

Key details

- Policy prepared by: Mark Kelly
- Policy approved by board on:
- Policy became operational on:
- Next review date:

Introduction

Squash Link needs to gather and use certain information about individuals.

These can include staff, volunteers, supporters, young people we work with 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 organization's data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures Squash Link:

- Complies with data protection law and follows good practice
- Protects the rights of staff, volunteers, supporters, service users and partners
- Is open about how it stores and processes data relating to individuals
- Protects itself from the risks of a data breach

Data protection law

The Data Protection Act 1988 and the Data Protection (Amendment) Act 2003 ("the Acts") describes how organisations — including ISEA — 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 obtained, collected and used fairly, kept accurately and (where necessary) up to date, used solely for disclosed purposes, stored safely and not disclosed unlawfully.

The eight rules of Data Protection:

1. Obtain and process information fairly

2. Keep it only for one or more specified, explicit and lawful purposes

3. Use and disclose it only in ways compatible with these purposes

4. Keep it safe and secure

5. Keep it accurate, complete and up-to-date

6. Ensure that it is adequate, relevant and not excessive

7. Retain it for no longer than is necessary for the required purpose or purposes

8. Give a copy of personal data to an individual, on request

People, risks and responsibilities

Policy scope

This policy applies to:

- All directors, company members, staff and volunteers of Squash Link; and
- All contractors, suppliers and other people working on behalf of Squash Link

It applies to all data that the organisation holds relating to identifiable individuals, even if that information technically falls outside of the Acts. 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 Squash Link from 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 organisation uses data relating to them

- Reputational damage. For instance, the organisation could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Squash Link has some responsibility for ensuring data is collected, stored and handled appropriately.

Each person that handles personal data must ensure it is managed and processed in line with this policy and data protection principles.

However, the following people have key areas of responsibility:

- ISEA's board of directors is ultimately responsible for ensuring that Squash Link meets its legal obligations.
- The Data Protection Officer, Mark Kelly, 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 Squash Link holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the organization's sensitive data.

- The Data Protection Officer, Mark Kelly, in liaison with any IT providers, 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 organisation is considering using to store or process data. For instance, cloud computing services.

- The Data Protection Officer, Mark Kelly, 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.

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, staff and volunteers can request it from their line managers.
- Squash Link will provide training to all staff and volunteers to help them understand their responsibilities when handling data.
- Staff and volunteers 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 unauthorized people, either within the organisation 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.
- Staff and volunteers should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.
- All marketing preferences should be accurately recorded and respected.
- When donor information is being obtained individuals should be made fully aware of: the identity of the persons who are collecting it (though this may often be implied); to what use the information will be put; and the persons or category of persons to whom the information will be disclosed. Individuals should be given the option to 'opt in' to their data being used in the proposed manner.
- Individuals should be given an opportunity to 'opt out' of having their details entered on a donor database. For example: "Your donation will be recorded for audit purposes and retained on Squash Link's donor database - if you do not wish to have your details stored on our donor database - please tick here."
- If donors wish to remain anonymous then their wishes should be respected. No details (bank account/address/name) should be stored except in a separate database for audit purposes.
- Generally a date of birth should not be retained except for in matters involving persons under 18 years old. Age ranges are sufficient for profiling purposes.
- Particular care should be taken when processing 'sensitive data'. Sensitive personal data" means personal data as to –

(a) the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject;
(b) whether the data subject is a member of a trade-union;

(c) the physical or mental health or condition or sexual life of the data subject;
(d) the commission or alleged commission of any offence by the data subject; or
(e) any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Data Protection Officer.

When data is stored on paper, it should be kept in a secure place where unauthorized 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.
- Staff and volunteers should make sure paper and printouts are not left where unauthorized 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 staff and volunteers.
- If data is stored on removable media (like a CD or DVD), 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, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the organisation'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 use

Personal data is of no value to Squash Link unless the organisation 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, staff and volunteers should ensure the screens of their computers are always locked when left unattended.
- If anyone wishes to use information that Squash Link already has and use it for a new purpose then we are obliged to give an option to those individuals to indicate whether or not they wish their information to be used for the new purpose.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- PPS numbers should only be retained and used for the purpose of tax relief claims.
- Data must be encrypted before being transferred electronically. The Data Protection Officer can explain how to send data to authorised external contacts.
- Personal data should not be transferred outside of the European Economic Area, unless that country or territory also ensures an adequate level of protection. In cases where Squash Link needs to transfer data to staff in countries outside of the EEA, all reasonable precautions will be taken to ensure the security of the data.
- Staff and volunteers 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 Squash Link 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 Squash Link should put into ensuring its accuracy.

It is the responsibility of all staff and volunteers 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 and volunteers should not create any unnecessary additional data sets.
- Staff and volunteers should take every opportunity to ensure data is updated. For instance, by confirming a supporter's details when they call.
- Squash Link will make it easy for data subjects to update the information Squash Link holds about them.
- Data should be updated as inaccuracies are discovered. For instance, if a supporter can no longer be reached on their stored telephone number, it should be removed from the database,

- Where applicable, marketing databases should be routinely checked against industry suppression files.

Subject access requests

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

- Ask what information the organisation 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 organisation is meeting its data protection obligations. If an individual contacts the organisation 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 squashlinkireland@gmail.com. All staff and volunteers are required to pass on anything which might be a subject access request to the Data Protection Officer without delay. The data controller can supply a standard request form, although individuals do not have to use this.

Individuals may be charged up to €6.35 per subject access request, and any charge will be made clear to the individual when they make an access request. The data controller will respond to subject access requests promptly and within 40 days.

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.

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

Providing information

Squash Link 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 organisation has a privacy statement, setting out how data relating to individuals is used by the organisation. This is available on request. A version of this statement is also available on the organisation's website.