Data Protection Policy

Introduction

The purpose of this policy is to ensure compliance with UK data protection law which includes the Data Protection Act 2018 (the Act) and UK GDPR (General Data Protection Regulation) to ensure that the Spinal Injuries Association (SIA) discharges all of its legal obligations in this respect. This policy applies to all activities for which SIA is the data controller and to all staff (including permanent, temporary, and contract staff), trustees, and volunteers.

Responsibilities

SIA as an organisation is the Data Controller under the Act and is therefore ultimately responsible for implementing this policy. SIA's registration /notification entry with the Information Commissioners Office can be viewed at: www.ico.org.uk

- Hope & May – have been retained as the Data Protection Officer for SIA and are authorised to act on our behalf with the ICO (Information Commissioners Office). Hope & May provide expert advice and support on all aspects of data protection to SIA. Such advice will be recorded.

- Wayne Botha, Operations and compliance manager – Data Protection Lead, responsible for day-to-day matters in respect of Data Protection

- Dave Bracher, Head of people and operations – 2nd DP lead (SLT)

- Svetla Stallwood, Director of Finance and Operations (SLT)

- Managers/specialists/heads/directors - responsible for implementing the policy within their areas of responsibility

- All staff, trustees, and volunteers - expected to comply with data protection legislation and adhere to the procedures defined in this policy.

Policy statement

It is the policy of SIA that:

- Personal data shall be processed fairly and lawfully
- Personal data shall only be obtained for specified and lawful purposes
- Personal data shall be adequate, relevant and not excessive to the purpose(s) for which they are processed
- Personal data shall be kept accurate and up to date
- Personal data shall not be kept for longer than is necessary
- Personal data shall be processed in accordance with the rights of the data subjects
- Personal data shall be protected from unauthorised and unlawful processing and against accidental loss or destruction or damage by appropriate technical and organisational controls
- Personal data shall not be transferred to a country or territory outside the EEA unless an adequate level of protection of the rights and freedoms of the data subject(s) can be guaranteed. In such cases a Transfer Risk Assessment may be undertaken, and a suitable UK safeguard will be implemented.

Procedure

Fair and lawful processing

When asking individuals to provide personal information SIA shall be identified as the data controller. All forms used to collect personal data must clearly state the purpose for which the information is being collected. SIA will not use personal data for any purposes other than those advised to individuals directly or detailed in its entries in the Register of Data Controllers published by the Information Commissioner.

As far as possible, SIA will process personal data only where it is necessary for compliance with the law, the performance of a contract, with a view to establishing a contract, or where it is in the organisation's legitimate business interests to do so. In the case of sensitive personal data, consent of the individual may be sought to enable the personal data to be processed.

SIA will obtain the explicit consent of the individual concerned for all processing of sensitive personal data; unless an exemption applies which may include where:

- It is information relating to racial/ethnic origin, religion or disability that is being collected purely for monitoring equality of opportunity or treatment
- It relates to the employment of SIA staff
- It is necessary for the provision of advice or support and the data subject cannot reasonably be expected to give explicit consent.

SIA will not disclose personal data to third parties unless:

- It is required to do so by law
- There is an information sharing agreement in place to ensure that any processing by the third party will be within the law
- It is necessary in order to fulfil a legitimate purpose that has been advised to the data subject.

All those collecting and processing information about other people (such as members, supporters etc.) must comply with these guidelines.

Exchanging personal data

It is permissible for personal data to be exchanged internally (i.e. between staff, trustees and volunteers) provided the intention of the exchange is to fulfil a legitimate purpose related to SIA activity and is done with the consent/knowledge of the data subject. It is not permissible for staff, trustees or volunteers to use any personal data obtained in furtherance of activities connected to outside interests, be they commercial or personal.

Direct marketing

SIA will treat the following unsolicited direct communication with individuals as marketing:

- seeking donations and other financial support;
- promoting events;
- promoting sponsored events and other fundraising activities;
- promoting campaigning activity;
- marketing on behalf of other external companies or voluntary organisations

Whenever data is first collected which might be used for any marketing purpose, this purpose will be made clear, and the Data Subject will be given a clear opt out. It is SIA's policy not to share direct marketing lists with third parties. Whenever email addresses are collected, any future use for marketing will be identified and the provision of the address made optional.

Personal data quality

All forms used to collect personal data shall only ask for information which is relevant to the purpose of the form. All monitoring and evaluation forms should be anonymised unless there is justifiable reason for including the capture of personal data as related to fair and lawful processing.

Notification of data held and processed

All staff and others are entitled to:

- Know what information SIA holds and processes about them and why
- Know how to gain access to it
- Know how to keep it up to date
- Know what SIA is doing to comply with its obligations under the Data Protection Act 2018

Approximately once a year, staff will be provided with an opportunity to confirm the accuracy of personal data held by the HR department.

All members and any other person's personal data held on SIA's CRM (Customer Relationship Management) system will be updated as soon as this information is received.

It is the responsibility of a staff member to:

- Check that any information provided to SIA in connection with their employment is accurate and up to date;
- Inform SIA of any changes to information previously provided. i.e. changes of address;
- Check the information that SIA will send out from time to time, giving details of information kept and processed about staff; and
- Inform SIA of any errors or changes. SIA cannot be held responsible for any errors unless the staff member has informed SIA of them.

Changes in personal data relating to members, supporters etc. must be promptly and accurately updated on the appropriate computer system(s).

Access by data subjects

A data subject may make a subject access request (SAR) at any time to find out more about the information that SIA holds about them.

- SARs (Subject Access Requests) may be made in writing, by email or verbally and addressed to the Data Protection Officer.
- A SAR may be made using SIA's Subject Access Request Form but does not have to be. If it is not, it should be clearly identifiable as a SAR.
- SARs must make it clear whether it is the data subject themselves that is making the request or whether it is a person acting on his or her behalf. In either case, proof of identity must be provided. If the SAR is made on another's behalf, the individual making the request must provide clear evidence of their authorised capacity to act on behalf of the data subject.
- SIA does not normally require a fee for each SAR unless the administrative costs of complying with a request are manifestly unfounded or excessive; or an individual requests further copies of their data following a request.
- If we intend to charge a fee, we will notify individuals of this, and SIA need not comply with a request until the fee has been received.

- In some cases, SIA has the right to request 'scope' to the request to access data. If the individual is unable to assist us with identifying the information they require, and where there may be a large volume of personal data, SIA may claim the request is excessive.
- Upon receipt of a SAR, SIA shall respond within one calendar month of receipt of a request. This time may be extended by a further two months if the request is complex or an individual has submitted several requests and SIA will inform the person making the request as to why the extension is necessary. The following information will be provided to the data subject:

    - Whether or not SIA holds any personal data on the data subject;
    - A description of any personal data held on the data subject;
    - Details of what that personal data is used for;
    - Details of how to access that personal data and how to keep it up to date;
    - Details of any third-party organisations that personal data is passed to; and
    - Details of any technical terminology or codes;
    - The contact details for the DPO.

Right to rectify/erase

Where information being kept is found to be factually incorrect, the Data Protection Act 2018 and the UK GDPR gives data subjects the right to have that information rectified or, in some cases, erased. Requests to rectify information must be addressed to the DPO of SIA and should explain the details deemed inaccurate. Additionally, if the person making such a request feels SIA has no good reason to hold the information (i.e., it is irrelevant or excessive for the purpose or has not been obtained fairly) then they may request that the information be erased. SIA must comply with this request, or indicate why it will not do so, within one month of receipt of the request, which may be extended by a further two months in exceptional circumstances.

Data security

SIA has implemented appropriate security measures as required under the Data Protection Act 2018 and the UK GDPR. All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely
- Photocopies of any personal data made for legitimate purposes are collected promptly from the copier and stored securely
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party

Staff should note that unauthorised disclosure may be a disciplinary matter and could be considered gross misconduct in some cases. Personal information should be:

- Kept in a locked filing cabinet; or
- In a locked drawer; or
- If it is computerised, be password protected

Visitors to SIA House are prevented from gaining access to personal information and are supervised at all times whilst in the building. Computer systems are installed with user-profile password controls to prevent unauthorised access. Manual filing systems are held in secure locations and are accessed on a need-to-know basis only.

Personal data retention

Personal information will only be retained as long as it is required for its purpose or as is required by law (see SIA's policy on Data Retention policy.docx) Manual files relating to previous staff shall have all non- essential information removed and securely destroyed prior to being archived.

Disposal of data

When personal data is no longer required, or has passed its retention date, paper records will be shredded and disposed of using the services of a reputable contractor, who will provide a Certificate of Destruction. Computerised records will be permanently deleted, with particular care taken to ensure that 'hidden' data cannot be recovered.

Confidentiality statement

All staff, trustees, sessional workers and volunteers must read and abide by the following Confidentiality Statement:

When working for, or representing, SIA you may need to have access to confidential information which may include, for example:

- Personal information about individuals who use our services
- Information about our internal business
- Personal information about individuals working for or representing SIA

SIA is committed to keeping this information confidential in order to protect individuals and the charity itself. 'Confidential' means that all access to information must be on a need-to-know and properly authorised basis. You must use only the information you have been authorised to use, and for purposes that have been authorised. You should also be aware that under the Data Protection Act 2018 s170, unauthorised access to data about individuals may be a criminal offence.

You must assume that information is confidential unless you know that it is intended by SIA to be made public. Passing information between staff, trustees or volunteers does not count as making it public, but passing information to another organisation, or using it on their behalf, does count. The passing of personal data internally should have a clear and specific purpose that can be demonstrated as being necessary by the person making the data request. Any data collected should only include personal data when there is a clearly identified need.

You must also be particularly careful not to disclose confidential information to unauthorised people or cause a breach of security. You must:

- not compromise or seek to evade security measures (including computer passwords);
- be particularly careful when sending information outside the office;
- not discuss confidential information, either with colleagues or people outside SIA;
- not disclose information, especially over the telephone, unless you are sure that you know who you are disclosing it to, and that they are authorised to have it

If you are in doubt about whether to disclose information or not, do not guess. Withhold the information while you check with an appropriate person whether the disclosure is appropriate. Your confidentiality obligations continue to apply indefinitely after you have stopped working for or representing SIA.

Breach of data protection

If confidential information is inadvertently disclosed to an unauthorised person or people, this is a breach of SIA's Data Protection policy. At the earliest opportunity after the breach has been identified, you must:

- Contact Wayne Botha, SIA's Data Protection Lead responsible for day-to-day matter in respect of Data Protection, with full details of the breach.
- In Wayne's absence, please contact Dave Bracher (2nd DP Lead) or Svetla Stallwood to report the breach.
- The DP Lead will then liaise with the 2nd DP Lead to determine the extent and implications of the breach and consider the next steps.
- The DP Lead will then liaise with Hope & May to report the breach and get their impartial advice about whether the breach is reportable to the Information Commissioners Office (ICO) and what additional actions may be required.
- If the breach is classed as high level and reportable to the ICO, Hope & May will action this and advise of the outcome. Hope & May are authorised to act on SIA's behalf with the ICO.
- If the breach is classed as low level and not considered to be reportable to the ICO, details of the breach and any remedial actions/learnings will be shared with the Senior Leadership Team.
- If the breach is classed as high level and reportable to the ICO, details of the breach and any remedial actions/learnings must immediately be escalated to the FP&O committee via the committee Chair by way of a flash report. The Chair will then share this with the Board.
- All breaches will continue to be reported in the quarterly Compliance Report for the FP&O Committee for monitoring and trend analysis purposes.

Please see Appendix 1 for a process flow to illustrate the breach process.

Conclusion

Compliance with UK data protection law is the responsibility of all those working at SIA. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the SIA's DP Officer.

Policy Owner (responsibility)	Director of finance and operations
Review schedule	Annually
Date of last review	August 2025
Next review	August 2026
Approval level	SLT if significant changes
Related policies and documents	Data retention policy Computer security policy Communications, email, and internet policy Social media policy Health & Safety – Working in offsite locations Privacy notices Data Protection Impact Assessments (DPIAs) Records of Processing Activities (RoPAs)

Appendix 1: Process flow - Breach of Data Protection