Sussex Clubs for Young People
Data Protection Policy

Reviewed **24th November 2021**

Signed

Chair of Directors: Peter Gooch

DATA PROTECTION OFFICER

Director – Jackie Cooper Jackie.cooper@sussexcyp.org.uk

Contents

Policy Statement 2
Data Protection Officer (DPO) 2
Control of data collected and stored 2
Employee records 3
Secure storage 3
Access to personal data 3
Disclosure 3
Appendix One – Data Retention 5
Data Protection Impact Assessment 6

Policy Statement

The Sussex Clubs for Young People (SCYP) Data Protection Policy aims to ensure compliance with the Data Protection Act 2018 and the General Data Protection Regulation, which refers to computerised and manual records of personal data.

SCYP is registered with the Information Commissioner's Office registration number Z1436121.

Data Protection Officer (DPO)

The Data Protection Officer is responsible for overseeing the implementation of this policy and for monitoring compliance with this policy and any other linked policies & procedures.

Control of data collected and stored

Any personal data collected by SCYP shall be stored and processed fairly and lawfully, and only for the purposes for which it has been collected. Data will be maintained accurately and updated regularly and will not be held any longer than necessary. It shall not exceed the purposes for which it is required. Specifically, personal data will be collected and stored to:

- process job applications
- maintain and process personnel and payroll records of employees
- maintain records of relevant personal details of staff, directors, volunteers, and trainees
- maintain contact details for affiliated clubs, emails, and records of visits
- maintain contact details for suppliers, contractors, and clients
- maintain personal details of clients/young people using the services/activities provided by SCYP as required by staff (paid or unpaid) to safely and efficiently carry out the service/activity.

A data retention schedule is shown in Appendix One.

Special efforts will be made to ensure that sensitive data, such as that on health, ethnic origin, trade union membership etc. will not be kept in such a way that the subject's identity is revealed inadvertently to anyone not authorised to use the data for personnel or payroll purposes.

Employee records

It is important that our employment records are up-to-date, and staff should notify the Admin Officer in writing, at the earliest opportunity of any change in relevant personal details.

Details held will only be available to staff authorised to deal with personnel matters. Such information will not be made available to any other person or organisation without consent or when legally compelled by an appropriate search by the Police or similar agency.

Staff personal data will be held on a computerised system, together with a manual file. All personal records will be held confidentially and securely and in accordance with the provisions of data protection legislation.

Secure storage

All personal data held by SCYP shall always be stored securely in locked filing cabinets in a locked office or secure online storage accessible only to approved SCYP staff, as follows:

- in the case of staff data, management, personnel, and payroll staff
- in the case of client data, relevant team staff, and project management.

All computerised data shall be protected so that it is accessible only to authorised staff as above. No personal data shall be removed from the SCYP premises except for parental and medical consent forms required for young people taking part in SCYP organised activities. Consent forms will be held in person by the designated SCYP staff member running the activity and returned to secure office storage immediately after the activity or destroyed as appropriate.

Access to personal data

Anyone on whom personal data is stored shall be informed of what information is stored and how it is processed, and of their rights to access their own records. They shall be given access to all information held on request (Subject Access Request) free of charge at the earliest available opportunity and permitted to have data corrected or erased if it is incorrect.

Anyone can request that personal data we hold about them can be erased if it is no longer necessary for us to for the purpose it was originally collected, if consent is withdrawn, there is no legitimate interest for us to retain it, to comply with legal obligations or it is being processed unlawfully.

All requests should be made to member.services@sussexcyp.org.uk or in writing to our office. The Data Protection Officer will normally respond within 30 days or as soon as is practicable.

If any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

Disclosure

No personal information shall be disclosed to another person or agency except with the express permission of the person concerned. The only exceptions to this relate to matters where SCYP are legally bound to pass on information (often referred to as a section 29 request), for example, in relation to any Child Protection issues to the relevant statutory agency or authority. In these instances, we have a legal obligation to share information that will aid in the prevention and detection of crime, the apprehension or prosecution of offenders or the assessment or collection of any tax or duty or of any imposition of a similar nature. These requests will be forwarded to and

handled by the Data Protection Officer. Data Security SCYP will ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

- Personal data must never be included within the subject line or message body of an email.
- All personal data documents legitimately transmitted via IT systems (e.g., email) must be protected using a strong password and marked “confidential”
- Wherever possible personal data should be shared via a link to cloud services restricted to access by the recipients or our staff only.
- Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using Special Delivery post and in a suitable container marked “confidential”.

SCYP will ensure that the following measures are taken with respect to the storage of personal data:

- All electronic copies of personal data should be stored securely either by using passwords or restricted permissions on folders.
- All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar.
- Personal data should only be stored on SCYP mobile devices (including, but not limited to, laptops, tablets, and smartphones), where there is appropriate security measures (e.g. PIN/Password) to make the device secure. Any exceptions to this should not take place without approval of the appropriate member of the Data Protection Officer and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is necessary.
- No personal data should be transferred to any personal device belonging to an employee, and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of SCYP where the party in question has agreed to comply fully with this policy and all Data Protection Legislation (which may include demonstrating to SCYP that all suitable technical and organisational measures have been taken).
- When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of.
- All paper copies of records should be disposed of by use of a cross-cut shredder or sent to a suitable processor for destruction.

Data should always be protected; this includes practical approaches such as locking away laptops when not in use and being careful who has access to where data is stored.

Any loss of personal data is a security breach, and all breaches, near-misses and incidents must be reported immediately to the Data Protection Officer.

The Data Protection Officer must ensure that the Information Commissioner’s Office and The Charities Directors are informed of any significant breach without delay, and in any event, within 72 hours after being made aware of it.

If a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Officer will ensure that all affected data subjects are informed of the breach directly and without undue delay.

Appendix One – Data Retention

Data Processed	**Length of time stored**
Job applications, CVs and covering letters for failed candidates	12 months
Employees records including job applications, CVs, and details of pensions	7 years
Media and Health Consent forms for young people and registers for project sessions	2 years
Media images of young people	2 years
Statistical information without personal data	7 years
Affiliate Members Records	Until they cease to be a member through resignation or closing
Financial records	7 years
Records of incidents / accidents	7 years
Business contracts and service level agreements	7 years after the end of the contract
Emails and electronic documents created by employees in allocated accounts	Archived after 1 year; removed 3 months after resignation.

Records will only be retained beyond the 7-year period if their retention can be justified for statutory, regulatory, legal or security reasons or for their historic value.

Data Protection Impact Assessment

Data to process	Reason for processing	Risks in processing / impact on individuals	Measures to reduce risk
Members of charity: contact details, postal address, email and websites, services offered, quality assurance checks	To support members by providing services for their activity To maintain records of consent for data sharing with 3rd parties e.g. UK Youth	Loss of contact details through disclosure or access to systems	- All data to be stored on cloud services provided by Microsoft Office 365 and / or Intuit Quickbooks - All users to use strong passwords - All group emails to be sent as BCC or through mailing service i.e., MailChimp - All users to be aware of duty to maintain confidentiality
Suppliers: contact details, postal address, email and websites, quality assurance checks, financial records	To conduct business lawfully and with due diligence	Loss of contact details through disclosure or access to systems Data shared with 3rd Parties i.e. Marsh & Co to examine accounts / Oltia Books for book-keeping services	- All data to be stored on cloud services provided by Microsoft Office 365 and / or Intuit Quickbooks - All users to use strong passwords - All group emails to be sent as BCC or through mailing service i.e., MailChimp - All users to be aware of duty to maintain confidentiality

Data to process	Reason for processing	Risks in processing / impact on individuals	Measures to reduce risk
Staff, volunteers and Directors: contact details, postal address, email, payroll and expenses information, contracts, CVs	To conduct the employment of everyone working for the business voluntarily or paid	Loss of personal data through disclosure or access to systems Data shared with 3rd Parties i.e., Marsh & Co to process payroll / Oltia Books for book-keeping services	- All data to be stored on cloud services provided by Microsoft Office 365, Intuit Quickbooks, PeopleHR - All users to use strong passwords - All group emails to be sent as BCC or through mailing service i.e. MailChimp - All users to be aware of duty to maintain confidentiality - Ensure 3rd Parties have adequate control mechanisms in place

Data to process	Reason for processing	Risks in processing / impact on individuals	Measures to reduce risk
Young people: parents and guardians, contact details, postal address, equality monitoring, DOB	To support young people who access our services To maintain records of parental and media consent for our activities	Loss of personal data through disclosure or access to systems Data shared with 3rd Parties e.g. Funders requiring evidence of impact / attendance Use of social media for contact with young people Loss of personal data through poor handling of paper records	- Paper records to be stored securely by workers in charge responsible for club sessions and activities at all times - All electronic data to be stored on cloud services provided by Microsoft Office 365, Intuit Quickbooks, PeopleHR or UPSHOT - All users to use strong passwords - All group emails to be sent as BCC or through mailing service i.e. MailChimp - All users to be aware of duty to maintain confidentiality - Ensure 3rd Parties have adequate control mechanisms in place - Ensure social media policies followed when linking contacts to groups / forums