ENCOURAGING EXCELLENCE, NURTURING TALENT!

SPORTING CHANCES GROUP
POLICIES & PROCEDURES

DATA PROTECTION POLICY

Lead	David Johnson
Last Reviewed	March-2025
Next Review Date	March-2026

This policy is enforced across all Sporting Chances Group provisions.

SC SURREY · SC OUTREACH PROGRAMME · MINI · CREATIVE HAIR&LASHES · SC ONLINE MENTORING PROGRAMME · SC FOOTBALL ACADEMY

CONTENTS

Sporting Chances Group (SCG), its provisions, and staff are committed to treating personal data in a responsible, open, and trustworthy manner, which maintains compliance with data protection laws.

APPLICABLE REGULATIONS & LAWS

This policy takes into account SCG's obligations in line with the:

- **UK General Data Protection Regulation** (UK GDPR)
- **Data Protection Act 2018** (DPA 2018)
- **Privacy and Electronic Communications Regulations** (PECR)

TERMINOLOGY

PERSONAL DATA	is any data relating to a living individual (i.e. staff, pupils, parents/guardians and third parties).
SPECIAL CATEGORIES OF PERSONAL DATA (Sensitive Personal Data)	is a category of personal data which is subject to additional regulation. It is defined as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, data concerning health, sex life or sexual orientation, genetic data, or biometric data for uniquely identifying someone.
DATA CONTROLLER	decides on how personal data is used and for what purpose. Holds primary legal responsibility and accountability for the protection of personal data.
DATA PROCESSOR	does something with the data, including recording, collecting, storing and analysing.
BREACH	is anything leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

DATA PROTECTION OFFICER (DPO)	is SCG's primary point of contact for data protection duties. The DPO liaises with the Information Commissioner's Office (ICO), monitoring and reporting on compliance.

Both **Personal Data** and **Special Categories of Personal Data** (Sensitive Personal Data) will be referred to as Personal Data in this policy.

DATA CONTROLLER

SCG is the Data Controller under the Data Protection Act 2018 and the Data Protection Act 2018.

DATA PROCESSORS

SCG is a Data Processor under the Data Protection Act 2018 and the Data Protection Act 2018. SCG also employs various third parties as Data Processors. Data subjects must be notified where such a processor is used, and this engagement will be covered by a contractual agreement ensuring that data protection maintained.

DATA PROTECTION OFFICER / CO-ORDINATOR (DPO / DPC)

The DPO can be contacted as follows:

emma@sportingchances.org

Emma Marshall, SCG Senior Manager
1A Downside Road
Sutton, SM2 5HR

PRINCIPLES

SCG follows these regulatory principles. **Personal data must be:**

- 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 DPA in order to safeguard the rights and freedoms of individuals; and
- 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.

SCG, as a Controller, is responsible for, and must be able to demonstrate, compliance with the above principles.

PERSONAL DATA PROCESSING

SCG processes personal and other types of data in pursuit of its responsibilities as an education centre, including admissions, governance, management, academic, pastoral, safeguarding, co-curricular, development, review, and implementation of our services.

Where applicable, explicit consent must be obtained for additional processing duties. SCG also has legal and regulatory obligations, which require the additional processing of personal data. SCG may receive and share relevant personal data in the form of references and applications for continued education.

SCG directly or indirectly processes personal data about past, current and prospective students, parents, staff, contractors, and other individuals who interact with it, including but not limited to the following data types:

- Contact details
- Financial details (i.e. for billing and payments)
- Academic, pastoral, behaviour, attendance, and activity records
- Medical information
- Incident records
- Special education needs information
- References
- Communication and meeting records
- Images
- CCTV footage (where available)

THIRD PARTIES & CLOUD PROVIDERS

SCG may engage third party processors and cloud service providers for services such as email, backups, online trip payments, ticketing platforms, counselling, management information systems, course and exam enrolment, development initiatives and communications.

Applicable data subjects must be notified of any third-party processors via data collection privacy notices.

Staff must only use third parties approved by the DPO and any such engagement must be subject to a contractual agreement ensuring compliant levels of data protection.

SCG must not process or use any third-party processor involving transferring personal data outside the European Economic Area (EEA).

International Transfers: Transfers of personal data outside the UK must comply with UK GDPR requirements, including adequacy decisions or appropriate safeguards.

DISCLOSURE EXEMPTIONS

SCG can disclose personal data without notification under certain instances, including:

- Data subject consent
- National security interests
- In the prevention or detection of a crime
- To prevent serious harm
- Legal and regulatory obligations
- In connection with legal proceedings or advice

PROCESSING GUIDELINES

SCG and its staff must always ensure that processing activities are compliant with the principles and rules of data protection regulations. If in any doubt, advice must be sought from the DPO.

This section covers core processing rules that all staff must follow to ensure adequate levels of data protection are maintained.

- Personal data must be kept for limited periods of time, in accordance with SCG's Data Retention Schedule (see ***Appendix 1***). Once a record has reached its retention limit, electronic version must be deleted, and physical copies destroyed and disposed.
- Electronic records including personal data must be saved within management information systems, single central records, or the relevant storage areas. Duplicates must be avoided.
- Paper records must always be filed in locked storage.
- Staff should avoid using emails to store personal data. Links to shared files should be used wherever possible, instead of attachments.
- Emails will have a retention period of six months before auto deletion, unless flagged for retention.
- Personal data records must not be on display in public areas (with exception of certain medical alert documents).
- All offices, staff rooms and staff only areas where personal data is kept, must only allow access through a lockable door. This must be kept locked when unattended or otherwise appropriate.
- Where personal data is emailed or stored online, the school/centre provisioned email and cloud storage platform must be used, unless otherwise approved by the DPO.
- Cloud services must be approved by the DPO before use.
- Teacher exercise books/referrals/records such as spreadsheets remain the property of the SCG.
- Teacher exercise books/records such as spreadsheets must employ a personal or the relevant school/centre coding system to indicate any medical, special education needs or personal data other than academic performance records.

- Contact information cannot be stored in exercise books/or on insecure physical paper.
- Electronic records must be approved by the DPO before use.
- Electronic records must have an export function.
- Attainment grades are pupil data and must be uploaded onto school/centre systems at least once per half-term.
- Any service which stores or transfers data outside the EEA must not be used.
- Usage of USB storage with personal data is strongly discouraged and remote access should be used instead. Where unavoidable, encrypted USB storage must be used.
- All school/centre mobile devices must have encryption enabled.
- Staff must use remote access platforms if working with data offsite. Where unavoidable, limited personal data can be processed by staff on personal devices in support of school/centrework. However, these devices must be password protected, ideally encrypted and the data must be erased immediately after use. Special categories (sensitive) of personal data must never be processed on personal devices.
- Personal data that is to be taken offsite, such as for trips and activities, must primarily be stored electronically on a school/centre mobile device. A backup physical copy of the required data can be taken and must be kept secure.
- Pupil images can only be used for purposes other than internal identification and security with explicit consent.

DATA SUBJECT RIGHTS

Data subjects have the following rights:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

Some of these rights are absolute and others are dependent on other factors.

- Staff must forward requests to exercise any of these rights to the DPO within one working day.
- The DPO may need to ask staff to supply information to fulfil a request. Staff must respond to any such data protection requests within three working days.
- The DPO must respond to data subjects who have made a rights request within 25 days (30 days is the regulatory limit), with: a) the answer to their requests; b) a request for an additional month to comply with a suitable reason; or c) a refusal letter explaining why.

DATA PROTECTION RESPONSIBILITIES

As part of our legal obligations for processing record keeping, it is critical that SCG has complete control and awareness over the location and processing of all personal data. SCG keeps an internal Data Processing Register, which records all data processing activities, the legal basis for processing, any associated third-party processor and risk management provision.

It is the responsibility of the Group and all staff to ensure 'data protection by design' and 'data protection by default', by considering data protection in the development and operation of the Group activities.

Our responsibilities include:

- The Data Processing Register must be reviewed and updated every year by the DPO
- Staff must consult the DPO before engaging in any new activity, which involves personal data
- A data protection impact assessment (DPIA) query form (see ***Appendix 2***) must be completed by staff and submitted to the DPO for approval for any new activity processing personal data; a DPIA must be conducted and if approved, the results added to the Data Processing Register
- Up to date malware and system monitoring tools must be used to assist in automatic detection of potential breaches
- Information systems must be adequate and kept up to date
- The DPO must liaise with the supervisory authority and notify relevant parties of any applicable data breaches
- Documented staff training must be conducted annually and awareness maintained throughout the year
- All new staff must complete recorded data protection training as part of their formal induction before being granted access to information systems
- All staff leavers must return any personal data to SCG (such as data in personal electronic exercise books/referrals/spreadsheets/profiles/referrals) as part of their formal exit process
- Personal data must be disposed of properly. Physical copies must be shredded before disposal

SCG is responsible for demonstrating compliance. Staff must be trained on data protection. Data breaches must be reported. Records of Processing Activities must be recorded and maintained as required by the UK GDPR and regular reviews of this policy must be carried out.

APPENDIX 1: SCG DATA RETENTION SCHEDULE

DATA RETENTION SCHEDULE

The following table represents the periods for which specified information and data records must be retained.

The list is not exhaustive and where a particular retention guide does not exist, staff are expected to apply the best practice approach of retaining data for no longer than is necessary. Further guidance can be sought from the relevant senior member of staff or the Data Protection Co-ordinator.

Once a retention period has expired the information/data must be erased.

Type of Record / Document	Retention Period [1]
Governance Records	
Registration documents of School/ Centre	Permanent (or until closure of the school/ centre)
Attendance Register	6 years from last date of entry, then archive
Meeting minutes	6 years from date of meeting
Annual curriculum	From end of year: 3 years (or 2 years for other class records: e.g. marks/timetables/ assignments)
Pupil Records	
Admissions: application/referral forms, assessments, records of decisions	25 years from date of birth (or, if pupil not admitted, up to 7 years from that decision)
Examination results (external or internal)	7 years from pupil leaving school/centre
Pupil file including: - **Pupil reports** - **Pupil performance records** - **Pupil medical records**	ALL: 25 years from date of birth (subject where relevant to safeguarding considerations). Any material which may be relevant to potential claims should be kept for the lifetime of the pupil.

Special educational needs records *(to be risk assessed individually)*	Date of birth plus up to 35 years (allowing for special extensions to statutory limitation period)
Safeguarding	
Policies and procedures	Keep a permanent record of historic policies
DBS disclosure certificates (if held)	***No longer than 6 months*** from decision on recruitment, unless DBS specifically consulted – but a record of the enhanced DBS checks and information must be kept and monitored to ensure compliance.
Accident / Incident reporting	Keep on record for as long as any living victim may bring a claim (NB civil claim limitation periods can be set aside in cases of abuse). Ideally, files to be reviewed from time to time if resources allow and a suitably qualified person is available. [2]
Child Protection files	If a referral has been made / social care have been involved or child has been subject of a multi-agency plan – indefinitely. If low level concerns, with no multi-agency act – apply applicable school/centre low-level concerns policy rationale (this may be 25 years from date of birth OR indefinitely).
Corporation Records	
Certificates of Incorporation	Permanent (or until dissolution of the company)
Minutes, Notes and Resolutions of Boards or Management Meetings	Minimum – 10 years
Annual reports	Minimum – 6 years

Accounting Records [3]	
Accounting records *(normally taken to mean records which enable a company's accurate financial position to be ascertained & which give a true and fair view of the company's financial state)*	Minimum – 6 years for UK charities (and public companies) from the end of the financial year in which the transaction took place
Tax returns	Minimum – 6 years
VAT returns	Minimum – 6 years
Budget and internal financial reports	Minimum – 3 years
Contracts & Agreements	
Signed or final/concluded agreements *(plus any signed or final/concluded variations or amendments)*	Minimum – 7 years from completion of contractual obligations or term of agreement, whichever is the later
Deeds (or contracts under seal)	Minimum – 13 years from completion of contractual obligation or term of agreement
Intellectual Property Records	
Formal documents of title (trademark or registered design certificates; patent or utility model certificates)	Permanent (in the case of any right which can be permanently extended, e.g. trademarks); otherwise expiry of right plus minimum of 7 years
Assignments of intellectual property to or from the school/centre	As above in relation to contracts (7 years) or, where applicable, deeds (13 years)
IP / IT agreements (including software licences and ancillary agreements e.g. maintenance; storage; development; coexistence agreements; consents)	Minimum – 7 years from completion of contractual obligation concerned or term of agreement
Personnel Records	
Single Central Record of employees	Keep a permanent record of all mandatory checks that have been undertaken (not certificate)

Contracts of employment	7 years from effective date of end of contract
Employee appraisals or reviews	Duration of employment plus minimum of 7 years
Staff personnel file	As above, but ***do not delete any information which may be relevant to historic safeguarding claims.***
Payroll, salary, maternity pay records	Minimum – 6 years
Pension or other benefit schedule records	Possibly permanent, depending on nature of scheme
Job application and interview/rejection records (unsuccessful applicants)	Minimum 3 months but no more than 1 year
Immigration records	Minimum – 4 years
Health records relating to employees	7 years from end of contract of employment
Insurance Records	
Insurance policies (will vary – private, public, professional indemnity)	Duration of policy (or as required by policy) plus a period for any run-off arrangement and coverage of insured risks: ideally, until it is possible to calculate that no living person could make a claim.
Correspondence related to claims / renewals / notification re: insurance	Minimum – 7 years
Facilities & Health and Safety Records	
Maintenance logs	10 years from date of last entry
Accidents to children [4]	25 years from birth (unless safeguarding incident)
Accident at work records (staff) [4]	Minimum – 4 years from date of accident, but review case-by-case where possible

Staff use of hazardous substances [4]	Minimum – 7 years from end of date of use
Risk assessments (carried out in respect of above) [4]	7 years from completion of relevant project, incident, event, or activity
Digital Activity Record	
Digital logs (e.g. computer activity, internet browsing, CCTV files)	Maximum – 1 year

1. General basis of suggestions include mandatory legal requirements (e.g. under the Companies Act 2006 or the Charities Act 2011); practical considerations for retention such as limitation periods for legal claims, and guidance from Courts, weighed against whether there is a reasonable argument in respect of data protection.
2. The High Court has found that a retention period of 35 years was within the bracket of legitimate approaches. It also found that it would be disproportionate for most organisations to conduct regular reviews, but at the time of writing the ICO still expects to see a responsible assessment policy (e.g. every 6 years) in place.
3. Retention period for tax purposes driven by legal or accountancy guidelines.
4. Latent injuries can take years to manifest, and the limitation period for claims reflects this: a note should be kept of all procedures as they were at the time, with a record that they were followed. Relevant insurance documents should also be kept.

APPENDIX 2: SCG DATA PROTECTION IMPACT ASSESSMENT (DPIA) QUERY FORM

SPORTING CHANCES GROUP

ENCOURAGING EXCELLENCE, NURTURING TALENT!

DATA PROTECTION IMPACT ASSESSMENT (DPIA) QUERY FORM

*Required.

Staff Full Name*	
Staff Job Title*	
Date* (dd/mm/yyyy)	

DESCRIPTION OF ACTIVITY*

PURPOSE OF THE ACTIVITY*

WHAT PERSONAL DATA WILL BE INVOLVED?*

HOW LONG WILL THE PERSONAL DATA TO BE KEPT?*

WHAT ARE THE POTENTIAL PERSONAL DATA RISKS?*

HOW WILL PERSONAL DATA BE PROTECTED?*

WHERE WILL THE DATA BE STORED?*
(If online, which country?)