
## Strength & Conditioning Education

# Policy

## Data Protection Policy

1. **PURPOSE**

1.1 This document sets out Strength & Conditioning Education ("SCE")'s policy on data protection. It provides an overview of data protection requirements and directs you to more detailed guidance as appropriate.

1.2 If you have any questions relating to this policy please contact SCE's Data Protection Officer via Info@strengthandconditioningeducation.com

2. **BACKGROUND TO THIS POLICY**

2.1 The General Data Protection Regulation (GDPR), to be incorporated into UK law via a new Data Protection Act (DPA), establishes a framework of rights and duties which are designed to safeguard personal data. These are referred to in this policy as 'Data Protection legislation'. The legislation is underpinned by a set of six straightforward principles, which define how data can be legally processed.

2.2 These six principles are:

2.2.1 Personal data shall be processed fairly, lawfully and transparently.

2.2.2 Personal data shall be held only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or purposes. There is an exemption for research data.

2.2.3 Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is processed.

2.2.4 Personal data shall be accurate and where necessary kept up to date.

2.2.5 Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose. There is an exemption for research data.

2.2.6 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of the data.

2.3 The GDPR also sets out rights of data subjects relating to their personal data. These rights include:

2.3.1 the right to access

2.3.2 the right to rectification

2.3.3 the right to erasure (in certain circumstances)

2.3.4 the right to stop processing

2.3.5 the right to portability (in certain circumstances)

2.3.6 the right to object to marketing. and

2.3.7 the right to have human intervention with regards to automated processing, including profiling

2.4 The GDPR sets out the conditions under which information can be transferred to countries outside the European Economic Area. These include adequacy, appropriate safeguards, binding corporate contracts and explicit consent, amongst others.

2.5 The Act defines both **personal data** and **special categories personal data**.

2.5.1 Personal data is any information that can identify a living individual and can include such items as home and work address, personal email address, age, telephone number and schools attended, and even photographs and other images.

2.5.2 Special categories personal data consists of racial/ethnic origin, political opinion, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life and information relating to legal proceedings and convictions.

2.5.3 Personal data comes under the categories of confidential or restricted information in the Information Classification Standard depending on the volume. Special categories personal data comes under the category of confidential information only in the Information Classification Standard.

2.6 The GDPR sets out certain lawful bases that must be satisfied to justify the holding or use of personal data. These are set out in Article 6 of the GDPR and include: contract; legal; vital interests, public duty, legitimate interests and consent. Special categories data requires that (an) additional lawful basis as set out in Article 9 of the GDPR. These lawful basis are recorded in the School's Information Asset Register. Staff who are unsure what lawful bases apply to personal data they intend to process should seek advice from the Data Protection Officer.

## 3. **POLICY AND GUIDANCE**

3.1 SCE is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data.

3.2 This Policy and the further SCE guidance it refers to apply to all personal data processed for the SCE's purposes, regardless of where it is held, and in respect of automatically processed data, the ownership of the equipment used.

3.3 Links to relevant School guidance are set out at the end of this policy. This list is not exhaustive.

## 4. **APPLICATION OF THIS POLICY**

4.1 SCE holds personal information about individuals such as employees, students, graduates and others, defined as **data subjects** in the DPA. Such data must only be processed in accordance with the DPA. This Policy and the SCE Guidance are written to ensure such compliance. Any breach of this Policy and/or SCE Guidance may result in SCE as the **Data Controller** (and in some cases individuals), being in breach of the DPA and therefore liable in law for the consequences of such breach.

4.2 Heads of Department are responsible for ensuring that SCE complies with the DPA. All students and staff must ensure they have read and understand this Policy and the SCE Guidance.

4.3 It is the responsibility of all users of personal data throughout SCE to ensure that personal data is kept securely. Personal data should not be disclosed to any unauthorised third party in any form, either accidentally or otherwise.

4.4 Any breach of or failure to comply with this Policy or the SCE Guidance, particularly any deliberate release of personal data to an unauthorised third party, may result in disciplinary or other appropriate action.

4.5 SCE will continue to perform periodic audits to ensure compliance with this Policy and Data Protection legislation and to ensure that all guidance and support is kept up to date.

4.6 Any unauthorised access to or disclosure of personal data or other data security breaches should be reported to the Data Protection Officer and/or the Incident Response Team as soon as possible.

4.7 The DPO is responsible for ensuring that the SCE community remain informed of their obligations under Data Protection legislation, with operational duties of advice and support devolved to the GDPR Readiness Team.

4.8 The Data Protection Officer is required by Data Protection legislation to report to the highest levels of management at SCE, which will normally be done through the Operations Director.

4.9 Staff procuring cloud-based services or mobile apps storing personal data for SCE must check with the Information Security team that these meet the security requirements of Data Protection legislation.

## 5. **HANDLING OF PERSONAL DATA BY STUDENTS**

5.1 A student should only use personal data for an academic or SCE-related purpose, with the knowledge and express consent of an appropriate member of staff. The use of personal data by students should be limited to the minimum consistent with the achievement of academic objectives.

5.2 For an undergraduate, responsibility would lie with the course leader of the relevant class/course. Wherever possible, data should be de-personalised so that students are not able to identify the subject.

5.3 Any confidentiality or consent agreements should normally be signed off by the Director of Research & Development. For advice, contact the Data Protection Officer

## 6. **ACCESS TO DATA**

6.1 The DPA gives data subjects a right to access to personal data held about them within a set timescale. Therefore, it is important that the Data Protection Officer be notified of any request to SCE for access to an individual's personal data as soon as they are received.

6.2 There are specific provisions which apply to examination marks and comments.

6.3 If you have any questions relating to access to personal data please contact one the Data Protection Officer.

## 7. **RETENTION OF DATA**

7.1 Personal data must only be kept for the length of time necessary to perform the processing for which it was collected. This applies to both electronic and non-electronic personal data.

## 8. **DATA TRANSFER**

8.1 If data is being sent outside the European Economic Area by SCE, there will be a need by SCE to put in place certain safeguards. Please contact the Data Protection Officer if for any reason related to SCE you may need to send personal data outside the EEA.

8.2 Information published on the web must be considered to be an export of data outside the EEA.

8.3 No web-based, or 'Cloud' services, should be used for storing or sending sensitive personal data unless this has been agreed with the Data Protection Officer.

8.4 Any transfers of personal data outside the EEA and/or extraordinary transfers of data should be signed off by the Board of Directors.

9. **COMPLIANCE, POLICY AWARENESS AND DISCIPLINARY PROCEDURES**

9.1 The loss or breach of confidentiality of personal data is an infringement of the Data Protection legislation and may result in criminal or civil action against SCE. Therefore, all users of personal data at SCE's information systems must adhere to the Data Protection Policy and its supporting policies as well as the Information Security Policy.

9.2 All current staff, students and other authorised users will be informed of the existence of this policy and the availability of supporting policies, codes of practice and guidelines.

9.3 Any breach of this policy will be handled in accordance with all relevant School policies and the appropriate disciplinary policies.

## Annex A – Further information

**External resources**

Data Protection Act
http://www.legislation.gov.uk/ukpga/1998/29/contents

Information Commissioner's Office
http://www.ico.gov.uk/

Information Commissioner's Office Guidance on Cloud Computing
http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/online/%7E/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx

Register of Data Controllers
http://www.ico.gov.uk/ESDWebPages/search.asp

**School Guidance**

Data Protection and Security:

https://strengthandconditioningeducation.com/data-protection/

Guidance on cloud-based services:

**Data Protection Officer / Incident Response Team**

Email: Info@strengthandconditioningeducation.com