SCoT
Data Protection & Information Security Policy

Version History

Version Number	Date Updated	Updated by	Comments	Approved by Board
V1	15/01/2021	Consultant	First Draft	
V2	28/1/2021	Chair	Minor Updates	31/1/2021

The CHAIR, or the Director with responsibility for membership has overall responsibility for implementing and monitoring this policy, which will be reviewed on a regular basis following its implementation (at least annually) and additionally whenever there are relevant changes in legislation or to our working practices.

Any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with the Operations Manager. Any breach will be taken seriously and may result in formal disciplinary action. Any employee who considers that the policy has been breached in any way should raise the matter with their line manager or a member of the Board.

Contents

Introduction

The Scottish Council of Taekwondo (SCoT) is fully committed to protecting the rights and privacy of individuals operating in accordance with the statutory legislation outlined within the General Data Protection Regulation (GDPR) and the forthcoming Data Protection Bill.

We are required to maintain certain personal data about individuals for the purposes of satisfying our operational and legal obligations. We recognise the importance of correct and lawful treatment of personal data as it helps to maintain confidence in our organisation and to ensure efficient and successful outcomes when using this data.

The types of personal data that we may process include information about current, past and prospective employees; members, partners, stakeholders, suppliers and other organisations with whom we have dealings.

Personal data may consist of data kept on paper, computer or other electronic media; all of which is protected under the GDPR.

This policy is not contractual but indicates how SCOT intends to meet its legal responsibilities for data protection.

1. Scope of this policy

This policy applies to all employees and workers who handle personal data, whether this relates to their colleagues, members, partners, stakeholders or anyone else. A copy will also be given to any third parties to whom we outsource any data processing or storage.

2. Aims of this policy

This policy aims to assist employees and workers to comply with the requirements of the GDPR and to minimise any risk to SCOT, by setting out clear guidelines relating to the processing, storage and disposal of data.

3. Legal considerations

The following legislation applies to this policy:

- The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)

Any codes of practice or advisory notes issued by the Information Commissioner should also be noted.

5. Definitions

Under GDPR Personal data is defined as:

"'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"

The GDPR covers the processing of personal data in two ways:

- personal data processed wholly or partly by automated means (that is, information in electronic form); and
- personal data processed in a non-automated manner which forms part of, or is intended to form part of, a 'filing system' (that is, manual information in a filing system).

Sensitive personal data is a specific set of "special categories" that must be treated with extra security. These categories are:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data; and
- Biometric data (where processed to uniquely identify someone).

Sensitive personal data should be held separately from other personal data, preferably in a locked drawer or filing cabinet. As with personal data generally, it should only be kept on laptops or portable devices if the file has been encrypted and/or pseudonymised.

6. Principles

We endorse and adhere to the eight principles of the GDPR which are summarised as follows:

Data must:

1. be processed fairly and lawfully and shall not be processed unless certain conditions are met.
2. be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
3. be adequate, relevant and not excessive for those purposes.
4. be accurate and, where necessary, kept up to date.
5. only be kept for as long as is necessary for the purpose for which it was obtained.
6. be processed in accordance with the data subject's rights.
7. be kept secure from unauthorised or unlawful processing and protected against accidental loss, destruction or damage by using the appropriate technical and organisational measure.
8. not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

These principles apply to obtaining, handling, processing, transportation and storage of personal data. Employees and agents of SCOT who obtain, handle, process, transport and store personal data for us must adhere to these principles at all times.

7. Handling of personal/sensitive information

SCOT will, through appropriate management and the use of strict criteria and controls:

- observe fully the conditions concerning the fair collection and use of personal information
- specify the purpose for which information is used
- collect and process information only to the extent that it is needed to fulfil operational needs or legal requirements
- endeavour always to ensure the quality of information used
- not keep information for longer than required (operationally or legally)
- always endeavour to safeguard personal information by physical and technical means (such as keeping paper files and other records or documents containing personal/sensitive data in a secure environment; protecting personal data held on computers and computer systems by the use of secure passwords which, where possible, are changed periodically and ensuring that individual passwords are not easily compromised)
- ensure that personal information is not transferred abroad without suitable safeguards
- ensure that the lawful rights of people about whom the information is held can be fully exercised.

In addition, SCOT will ensure that:

- there is someone with specific responsibility for data protection in the organisation (the designated Data Controller) - currently the CHAIR.

- All SCOT requirements as a data controller as required by the Information Commisioners Office (ICO) are upheld.
- all those who manage and handle personal information understand that they are contractually responsible for following good data protection practice
- all those who manage and handle personal information are appropriately supervised and trained to do so
- a clear procedure is in place to deal with any data access requests (internal or external) that ensures that such enquiries are dealt with promptly and courteously
- methods of handling personal information are regularly assessed and evaluated
- any data sharing is carried out under a written agreement, setting out the scope and limits of the sharing
- any disclosure of personal data will be in compliance with approved procedures.

SCOT also has a legal obligation to provide employee liability information to any organisation that our employees (if applicable) are transferring to, in line with the Transfer of Undertakings (Protection of Employment) Regulations (TUPE).

8. Access to personal data

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

- ask what information we hold about them and why
- ask how to gain access to it
- be informed of how to keep it up to date
- have inaccurate personal data corrected or removed
- prevent us from processing information or request that it is stopped if the processing of such data is likely to cause substantial, unwarranted damage or distress to the individual or anyone else
- require us to ensure that no decision which significantly affects an individual is solely based on an automated process for the purposes of evaluating matters relating to him/her, such as conduct or performance
- be informed what we are doing to comply with our obligations under the GDPR

This right is subject to certain exemptions which are set out in the GDPR.

Any person who wishes to exercise this right should make a request in writing to the Chair or Membership Director. We reserve the right to charge the maximum fee payable for each subject access request. If personal details are inaccurate, they will be amended upon request. If by providing this information we would have to disclose information relating to or identifying a third party, we will only do so provided the third party gives consent, otherwise we may edit the data to remove the identity of the third party.

Unless we are under a legal obligation to release data, or the individual has given us permission, personal information will only be released to the individual to whom it relates. The disclosure of such information to anyone else without their consent may be a criminal offence. Any employee who is in doubt regarding a subject access request should check with the Chair. Information must under no circumstances be sent outside of the UK without the prior permission of the Chair.

We aim to comply with requests for access to personal information as quickly as possible, but will ensure that this is provided within 30 days of receipt of a written request unless there is good reason for delay. In such cases, the reason for the delay will be explained in writing to the individual making the request.

Under the GDPR, subject to certain conditions being met, an individual has the right to have their data erased. If such a request is received from an individual, SCOT as the Data

Controller must assess the request in the context of the personal data that is held and the needs that exist to retain data including legal, commercial, contractual and other factors. In some circumstances, whilst it will be possible to erase some data it may not be possible to erase all data about an individual due to these considerations.

9. Employee responsibilities

All employees must ensure that, in carrying out their duties, SCOT is able to comply with its obligations under the GDPR. In addition, each employee is responsible for:

- checking that any personal data that they provides to us is accurate and up to date
- informing us of any changes to information previously provided, such as change of address
- checking any information that we may send out from time to time, giving details of information that is being kept and processed
- ensuring that if, as part of their responsibilities, they collect information about other people or about other employees, they comply with this policy. This includes ensuring that information is processed in accordance with the GDPR, is only processed for the purposes for which it is held, is kept secure, and is not kept any longer than is necessary.

Employees are reminded that the GDPR does not just apply to records relating to our employees (if applicable), but also to any members, partners, stakeholders files/records. Information stored on members, partners, stakeholders should be reviewed regularly to ensure it is accurate and up to date. All documents, whether hand written or stored in emails (current or deleted) are potentially disclosable in the event of a request from an employee or client/customer.

10. Employee records

If there are any employees employed by SCoT at any point, we will hold personal information about all employees as part of our general employee records. This includes address and contact details, age, date of birth, marital status or civil partnership, educational background, employment application, employment history with SCOT, areas of expertise, details of salary and benefits, bank details, performance appraisals and salary reviews, records relating to holiday, sickness and other leave, working time records and other management records. We may receive and/or retain this information in various forms (whether in writing, electronically, verbally or otherwise).

This information is used for a variety of administration and management purposes, including payroll and benefits administration, facilitating the management of work and employees, performance and salary reviews, complying with record keeping and other legal obligations.

We also process information relating to employees' health, some of which may fall under the definition of 'sensitive personal data'. This includes pre-employment health questionnaires, records of sickness absence and medical certificates (including self-certification of absence forms), night worker assessments, VDU assessments, noise assessments and any other medical reports. This information is used to administer contractual and Statutory Sick Pay, monitor and manage sickness absence and comply with our obligations under health and safety legislation and the Working Time Regulations.

From time to time we may ask employees to review and update the personal information we hold about them. We ask employees inform us immediately of any significant change(s) to their personal information

11. Data security

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted.

Data retained on laptops, smartphones and any other electronic equipment that is used must be password protected.

All employees (if applicable) and workers are responsible for ensuring that any personal data that they hold is stored securely and that personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

References that disclose personal information will not be provided to any third party without the data subject's prior authority (unless this is required or permitted by law such as by the police, HMRC, Contributions Agency or similar body).

Third party processors (such as our outsourced payroll) will be required to provide sufficient guarantees for their data security measures and compliance with them.

Any employee who discovers personal or sensitive data in an inappropriate place (for example unknowingly sent to the wrong email) should immediately pass this to the Chair ensuring that its contents are not revealed to anyone else.

12. Publication of information

Information that is already in the public domain is exempt from the Act. This would include, for example, information contained within externally circulated publications such as brochures and other sales and marketing aids.

Any individual who has good reason for wishing their details not to be included in such publications should contact the Chair or Membership Director..

13. Subject consent

Our contracts of employment (if applicable) require the consent of employees to the processing of personal data for the purposes of administration, managing and employing them. This includes: payroll, benefits, medical records, absence records, sick leave/pay information, performance reviews, disciplinary and grievance matters, pension provision, recruitment, family policies (maternity, paternity, adoption, shared parental leave etc) and equal opportunity monitoring.

Information about an individual will only be kept for the purpose for which it was originally provided. Employees and managers must not collect data that is simply "nice to have" nor use data for any purpose other than what it was provided for originally.

14. Retention and disposal of data

All employees (if applicable) and Directors are responsible for ensuring that information is not kept for longer than necessary.

Documents containing any personal information will be disposed of securely, and paper copies will be shredded (not disposed of directly into a normal bin or recycling bin). Information stored on obsolete electronic equipment (desktops, laptops and other devices) will be erased prior to the equipment being sold, disposed of or reallocated to other employees.

15. Registration

The Data Protection Act 1998 requires every data controller who is processing personal data, to notify and to renew their notification on an annual basis. Failure to do so is a criminal offence.

SCOT is registered in the Information Commissioner's public register of data controllers.

The CHAIR or if no CHAIR is employed, the Operations Manager in conjunction with the Director responsible for Data Protection and Governance is our Data Controller and is responsible for ensuring compliance with the Data Protection Act, for notifying and updating the Information Commissioner of our processing of personal data, and for the monitoring and implementation of this policy on behalf of SCOT.

Any changes made to the information stored and processed must be brought to the attention of the CHAIR immediately.

16. Related policies and documents

We also have the following related policies and documents:

SCoT Privacy Notice (need web link)

SCoT IT Policy