IT02-P01 DATA PROTECTION POLICY

VERSION CONTROL

Version No.	Date Amended	Amended By	Reason
1.0	01/12/2014		New logo
2.0	10/07/2019	Risk & Compliance Sub Committee	Full review
3.0	18/05/2020	Risk & Compliance Sub Committee	Review due
4.0	12/04/2021	Risk & Compliance Sub Committee	End of cycle review due
5.0	11/04/2022	Risk & Compliance Sub Committee	End of cycle review due
6.0	10/07/2023	Risk & Compliance Sub Committee	End of cycle review due

DATA PROTECTION POLICY

The data protection laws in the UK include the Data Protection Act 2018 and the General Data Protection Regulation (EU) 2016/679 (GDPR) which both came into effect on the 25th May 2018 (together referred to in this policy as the Data Protection Laws). Having completed a self-assessment guide, Scottish Squash Limited (SSL) must register with the Information Commissioner's Office (the ICO) as a controller of personal data and we are required to comply with the data protection principles set out in the Data Protection Laws.

As a controller of the personal data that we hold, SSL determines the purpose for which, and the manner in which, any personal data are, or are to be, processed.

SSL is fully committed to complying with the requirements of the Data Protection Laws and recognises the importance of protecting the rights of individuals on whom SSL processes personal data.

Key Definitions

SSL – means Scottish Squash Limited.

Information Commissioner's Office (the ICO) – is the supervisory authority responsible for enforcing and monitoring compliance with Data Protection Laws in the UK.

Controller – the organisation that determines the purposes for which and manner in which personal data is used, in our case, SSL.

Data subject – a living individual who is the subject of personal data, for example, our members, current, past and prospective employees, members of our clubs, athletes, coaches, volunteers, etc.

Personal data – any information relating to an identifiable person who can be directly or indirectly identified from that information, in particular by reference to an identifier.

Special categories of personal data is defined as personal data revealing a data subject's:

- Racial or ethnic origin;
- Political opinions;
- Religious of philosophical beliefs;
- Trade Union membership;
- Health;
- Sex life or sexual orientation; and
- Genetic or biometric data where processed for the purpose of uniquely identifying a data subject.

Responsible person – means SSL's Chief Operating Officer.

Register of Systems – means a register of all systems or contexts in which personal data is processed by SSL.

Processing – any operation performed on personal data, including collecting, recording, storing, using, disclosing and deleting.

Processor – means a third party who processes personal data on behalf of a controller.

1. Data Protection Principles

a) SSL is committed to processing personal data in accordance with its responsibilities as set out in the Data Protection Laws. SSL will ensure that personal data shall be:
   i. "Processed lawfully, fairly and in a transparent manner in relation to the data subject;
   ii. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
   iii. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
   iv. 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;
   v. 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; and
   vi. 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."

2. General Provisions

a) This policy applies to all personal data processed by SSL.
b) The Responsible Person shall take responsibility for SSL's ongoing compliance with this policy.
c) SSL shall register with the ICO as an organisation that processes personal data.
d) SSL shall take reasonable steps to ensure personal data is accurate and, where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

3. Basis and Purposes for Processing Personal Data

a) To ensure its processing of personal data is lawful, fair and transparent, SSL shall maintain a Register of Systems [IT02-G01 Data Protection Information Audit].
b) Before any personal data is processed by SSL for the first time, SSL will review the purposes of the particular processing activity and select the most appropriate lawful basis under the Data Protection Laws, namely:
   i. Consent;
   ii. Contract;
   iii. Legal obligation;
   iv. Vital interests;
   v. Public task; or
   vi. Legitimate interests.
c) As well as a lawful basis, before any special categories of personal data are processed by SSL for this first time, SSL will select a special condition under the Data Protection Laws, namely:

i. The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
ii. The processing is necessary for SSL to perform our obligations or exercise rights under employment law – this would apply to staff personal data, for example, to maintain attendance and performance records;
iii. Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
iv. The processing is necessary for substantial public interest reasons – for example, equality monitoring, anti-doping and standards of performance in sport.

d) SSL shall note the appropriate lawful basis and special condition in the Register of Systems.
e) SSL shall include information about the purposes and lawful basis of the processing within our privacy notice provided to individuals.

4. Documentation and Records

a) SSL's Register of Systems records details of all processing activities, including:
   i. A description of the categories of individuals and categories of personal data processed by SSL;
   ii. As per 3. d), the lawful basis and special condition (if applicable) of the processing of personal data by SSL;
   iii. Categories of recipients of personal data with whom SSL shares personal data;
   iv. A description of technical and organisational security measures put in place to keep personal data secure;
   v. Details of how long SSL keeps personal data; and
   vi. Where relevant, details of transfers to countries out with the EU, including documentation of the transfer mechanism safeguards in place.

5. Contracts

a) If the data held by SSL is passed to a third party who uses that personal data on behalf of SSL as a 'processor' (for example, to provide services to SSL), the third party must sign a data processing agreement or an agreement with a data processing clause included. Such agreement or clause must include, as a minimum, that the third party shall:
   i. Only act on the written instructions of SSL (unless required by law to act without such instructions);
   ii. Ensure that people processing personal data on behalf of SSL are subject to a duty of confidence;
   iii. Only engage a sub-contractor to process personal data on behalf of SSL with the prior consent of SSL and a written contract;
   iv. Assist SSL in responding to requests from data subjects seeking to exercise their rights under the Data Protection Laws;

v. Assist SSL in meeting its obligations under the Data Protection Laws in relation to security of processing, the notification of personal data breaches and data protection impact assessments where applicable;
vi. Delete or return all personal data to SSL as requested at the end of the contract;
vii. Allow data protection audits and inspections by SSL of personal data held on its behalf (if requested) to ensure that both parties are meeting their requirements under the Data Protection Laws and tell SSL immediately if asked to do something that infringes that Data Protection Laws; and
viii. Indemnify SSL against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

6. Security

a) SSL shall ensure that personal data is stored securely using modern software that is kept up to date.
b) Access to personal data shall be limited to personnel who need access and appropriate security will be in place to avoid unauthorised sharing of information.
c) When personal data is deleted, this will be done safely such that the data is irrecoverable.
d) Appropriate back-up and disaster recovery solutions shall be in place.

7. Archiving/Removal

a) To ensure that personal data is kept for no longer than necessary, SSL shall put in place a process for archiving data in each area of personal data processed. This process will be reviewed annually.
b) The archiving process shall consider what personal data should/must be retained, for how long, and why.

8. Transfer of Data

a) All personal data held by SSL will not be transferred 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 or a safeguard is put in place.
b) The safeguards that SSL normally use are:
    i. Where the recipient is based in the US and are certified under the EU-US Privacy Shield framework; or
    ii. Where the recipient enters into a contract with SSL including the EU Commission's approved standard contractual clauses.

9. The Rights of Individuals

a) Individuals can exercise any of the following rights by writing to us at info@scottishsquash.org
b) Data subjects have the following rights under the Data Protection Laws:

i. A right to request access to the personal data that SSL holds by making a "subject access request";
ii. A right to request that SSL corrects or completes personal data;
iii. A right to request that SSL restricts the processing of personal data for specific purposes;
iv. A right to request that SSL deletes personal data; and
v. A right to ask SSL to provide personal data for the data subject's reuse for their own purposes.

c) Any requests received by SSL will be considered under the Data Protection Laws as certain rights only apply in specific circumstances.
d) If the data subject is dissatisfied with how SSL has handled their request, they have a right to raise a complaint with the ICO at www.ico.org.uk

10. Data Breaches

a) In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, SSL shall notify:
   i. The ICO within 72 hours where the breach puts individuals' data at risk
   ii. The individuals concerned as soon as possible where there is a high risk to them as a result of the breach.

11. Policy Review

a) This policy shall be reviewed at least annually.
b) This policy/function will have no impact on people from any of the equality groups and an Equality Impact Assessment is not required.