



Ref:	PD 5
Page:	1 of 6
Date:	10/2021

DATA PROTECTION POLICY

The Data Protection Bill updates data protection laws in the UK and replaces the Data Protection Act 1998, supplementing the General Data Protection Regulation (EU) 2016/679 (GDPR) which 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 Swimming must register with the Information Commissioner's Office 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, Scottish Swimming determines the purpose for which, and the manner in which, any personal data are, or are to be, processed.

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

KEY DEFINITIONS

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

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

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 category personal data is defined as personal data revealing a data subject's:

- racial or ethnic origin;
- political opinions;
- religious or 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.

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.

PRINCIPLES OF DATA PROTECTION

Scottish Swimming must ensure that we have:

1. OBTAINED PERSONAL DATA LAWFULLY, FAIRLY AND TRANSPARENTLY

Scottish Swimming will only process personal data where it is lawful to do so under the Data Protection Laws and ensure that all individuals for whom we process personal data are given access to our privacy notice upon the collection of their personal data or within one month of receiving their personal data from a third party.

SASA CORPORATE GOVERNANCE POLICES AND PROCEDURES

2. HOLD PERSONAL DATA ONLY FOR SPECIFIC, EXPLICIT AND LEGITIMATE PURPOSES

Scottish Swimming will ensure that personal data will be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (with expedition for public interest or statistical purposes).

If we intend to use personal data for direct marketing purposes the data subjects are made aware of this and given the option to consent to having their data processed in this way. Opt-ins will be included on our online membership system (Azolve).

3. PERSONAL DATA HELD IS RELEVANT, ADEQUATE AND LIMITED TO WHAT IS NECESSARY FOR ITS PURPOSE

Scottish Swimming will monitor the quantities of personal data held for our purposes and ensure that we hold neither too much nor too little personal data in respect of the individuals about whom data is held.

4. PERSONAL DATA HELD IS ACCURATE AND UPDATED WHERE NECESSARY

Scottish Swimming updates current records as notified directly in writing by individuals or clubs. Scottish Swimming members can view their specific data protection choices using the online membership check and can make changes to their choices which will automatically reflect in Azolve.

5. PERSONAL DATA IS NOT KEPT FOR LONGER THAN NECESSARY

All personal data will be kept in an identifiable format for no longer than is necessary. Personal data will be kept for as long as necessary to provide members with membership services. Unless a member asks us not to, we will review and possibly delete personal information where a member has not renewed membership with Scottish Swimming for six years. Employee's personal data will be retained for 2 years and financial data will be retained for 7 years.

Certain personal information will be retained for longer in order to confirm identity, and to confirm previous membership with Scottish Swimming and to confirm how long they were with Scottish Swimming. Scottish Swimming needs to do this to comply with the Companies Act 2006, which requires keeping a register of members or in the event of a claim against Scottish Swimming.

For members who compete in aquatics and who have swim times that appear in the rankings list (www.swimmingresults.org), these ranked swim times are not removed from the system unless Scottish Swimming receive a request to remove them – since these can be used for historic recording purposes.

6. PERSONAL DATA SHALL BE KEPT SECURE

Scottish Swimming must ensure that adequate security precautions are in place to prevent loss, destruction or unauthorised disclosure of personal data.

All Scottish Swimming computers have a log in system, which allows only authorised personnel to access personal data. Passwords on all computers are changed frequently.

All personal, financial and wellbeing protection data is kept in a locked filing cabinet and can only be accessed by the Chief Executive, Director of Services, Finance Team, Safeguarding Officer and Chair where appropriate.

When Scottish Swimming staff use laptop computers out of the office care should always be taken to ensure that personal data on screen is not visible to strangers.

The University of Stirling server, which can be accessed at any time, automatically backs up all data held by Scottish Swimming. This server is located in a different building from the Scottish Swimming HQ.

[Please refer to policy PD37 IT Policy and PD38 ICT Strategy Policy for more information](#)

Scottish Swimming offices are locked out with office hours.

BASIS AND PURPOSES FOR PROCESSING PERSONAL DATA

POLICY DOCUMENTS

SASA CORPORATE GOVERNANCE POLICES AND PROCEDURES

Before any personal data is processed by Scottish Swimming for the first time, Scottish Swimming will:

- review the purposes of the particular processing activity and select the most appropriate lawful basis under the Data Protection Legislation. The lawful bases most commonly used by Scottish Swimming are that:
 - the individual has consented – this is only appropriate where it is not a precondition of a service or another lawful basis applies and does not apply to staff personal data;
 - the processing is necessary for performance of or to take steps to enter into a contract with the individual – this will apply to our members, staff and anyone requesting services from Scottish Swimming;
 - the processing is necessary to comply with a legal obligation – Scottish Swimming needs to process certain personal data under law, such as to comply with **sportscotland's** regulatory requirements or staff personal data for HMRC reporting purposes; or
 - the processing is necessary for Scottish Swimming's or a third party's legitimate interests – provided that the legitimate interests are not overridden by the interests of the data subject;
- where special category personal data is involved in the processing activity, identify the most appropriate special condition for processing in addition to a lawful basis above. The special conditions most commonly used by Scottish Swimming are that:
 - the individual has explicitly consented – this is only appropriate where it is not a precondition of a service or another lawful basis applies and does not apply to staff personal data;
 - the processing is necessary for Scottish Swimming 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;
 - the processing is necessary for Scottish Swimming to establish, exercise or defend legal claims; or
 - the processing is necessary for substantial public interest reasons – for example, equality monitoring, anti-doping and standards of performance in sport;
- document Scottish Swimming's decision as to which lawful basis applies, to help demonstrate compliance with the data protection principles; and
- include information about the purposes, lawful basis and special condition (if applicable) of the processing within our privacy notice provided to individuals.

Scottish Swimming will review the procedures above every three years.

CONTRACTS

If the data held by Scottish Swimming is passed to a third party who uses that personal data on behalf of Scottish Swimming as a 'processor' (for example, to provide services to Scottish Swimming), 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:

- only act on the written instructions of Scottish Swimming (unless required by law to act without such instructions);
- ensure that people processing personal data on behalf of Scottish Swimming are subject to a duty of confidence;
- only engage a sub-contractor to process personal data on behalf of Scottish Swimming with the prior consent of Scottish Swimming and a written contract;
- assist Scottish Swimming in responding to requests from data subjects seeking to exercise their rights under the Data Protection Laws;
- assist Scottish Swimming 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;
- delete or return all personal data to Scottish Swimming as requested at the end of the contract;

SASA CORPORATE GOVERNANCE POLICES AND PROCEDURES

- allow data protection audits and inspections by Scottish Swimming 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 Scottish Swimming immediately if asked to do something that infringes the Data Protection Laws; and
- indemnify Scottish Swimming against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

TRANSFER OF DATA

All personal data held by Scottish Swimming must 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.

DOCUMENTATION AND RECORDS

Scottish Swimming ~~+~~ keeps written records of processing activities, including:

- the name and details of Scottish Swimming;
- the purposes of the processing of personal data by Scottish Swimming;
- a description of the categories of individuals and categories of personal data processed by Scottish Swimming;
- categories of recipients of personal data with whom Scottish Swimming shares personal data;
- where relevant, details of transfers to countries out with the EU, including documentation of the transfer mechanism safeguards in place;
- details of how long Scottish Swimming keeps personal data; and
- a description of technical and organisational security measures put in place to keep personal data secure.

Scottish Swimming will issue privacy notices ~~from time to time~~ to members annually and to employees every three years (or more frequently if required) to ensure that individuals understand how their personal data is collected, used, stored, shared and deleted by Scottish Swimming.

THE RIGHTS OF INDIVIDUALS

Data subjects have the following rights in relation to their personal data:

- to be informed about how, why and on what basis that information is processed – as contained within Scottish Swimming's privacy notices;
- to obtain confirmation that their personal data is being processed by Scottish Swimming and to obtain access to it and certain other information, by making a subject access request;
- to have personal data corrected if it is inaccurate or incomplete;
- to have personal data erased if it is no longer necessary for the purpose for which it was originally collected / processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as the "right to be forgotten");
- to object to Scottish Swimming processing their personal data for direct marketing purposes or where the processing is in pursuit of Scottish Swimming's or a third party's legitimate interests;
- to restrict the processing of personal data where the accuracy of the data is contested, or the processing is unlawful (but the individual does not want the personal data to be erased), or where Scottish Swimming no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim; and
- to restrict the processing of personal data temporarily where the individual does not think it is accurate (and Scottish Swimming is verifying whether it is accurate), or where the individual has objected to the processing (and Scottish Swimming is considering whether its legitimate grounds override the data subject's interests); and
- where an individual provides Scottish Swimming with personal data and we process it with their consent or under contract by automated means, the individual can request their personal data for their own reuse (a right to data portability).

SASA CORPORATE GOVERNANCE POLICES AND PROCEDURES

Individuals can exercise any of the following rights by writing to Scottish Swimming at DP@scottishswimming.com or by logging on to their account at <https://scottishswimming.azolve.com/Account.mvc/LogIn>

Where staff receive a request from an individual that relates to their personal data and they are not authorised to handle such a request, staff must immediately notify the Data Protection Officer of the request. The Data Protection Laws only give Scottish Swimming one month to respond to requests so staff should not delay in notifying the Data Protection Officer of any request.

DATA PROTECTION OFFICER

The data protection officer is responsible for monitoring compliance with this policy and the Data Protection Laws, providing information and advice, and liaising with the ICO.

Scottish Swimming's Data Protection Officer is Francesca Carlo who will be supported by Harper Macloed. Francesca will report to the Board of Directors on all data protection matters.

DATA BREACHES

A data breach may take many different forms, for example:

- loss or theft of data or equipment on which personal data is stored;
- unauthorised access to or use of personal data either by a member of staff or third party;
- loss of data resulting from an equipment or systems (including hardware and software) failure;
- human error, such as accidental deletion or alteration of data;
- unforeseen circumstances, such as a fire or flood;
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
- 'blagging' offences, where information is obtained by deceiving Scottish Swimming.

Scottish Swimming will:

- make the required report of a data breach to the ICO without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and
- notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

It is important that staff report any suspected or actual data breach to the Data Protection Officer immediately. The Data Protection Officer will be responsible for recording and reporting data breaches.

POLICY REVIEW

As a strategic document, this Policy will be reviewed every three years. The next review will therefore take place in May 2024 or earlier to take account of:

- legislative, regulatory and good practice requirements;
- Scottish Swimming's performance; or
- the views of any stakeholder in the use of personal data.

This policy/function will have no impact on people from any of the equality groups and an Equality Impact Assessment is not required.