EXMOUTH SWIMMING AND LIFE SAVING SOCIETY
DATA PROTECTION

Exmouth Swimming and Life Saving Society is committed to complying with the General Data Protection Regulation (**GDPR**) and the Data Protection Act 2018 and to respect the privacy rights of individuals. This policy applies to all members of the Society. This Data Protection Policy sets out our approach to data protection law and the principles that we will apply to our processing of personal data. The aim of this Policy is to ensure that we process personal data in accordance with the law and with the utmost care and respect. This Society also has a Privacy Policy.

Data protection law is a complex area. This Policy has been designed to ensure that you are aware of the legal requirements imposed on you and on us and to give you practical guidance on how to comply with them. This Policy is not an exhaustive statement of data protection law nor of our or your responsibilities in relation to data protection. If at any time you have any queries on this Policy, your responsibilities or any aspect of data protection law, contact a member of the Main Committee.

Who is responsible for data protection?

We are all responsible for data protection, and we all have our own role to play to make sure that we are compliant with data protection laws. We are not required to appoint a Data Protection Officer but the Main Committee is responsible for overseeing our compliance with data protection laws.

Why do we have a data protection policy?

This data protection policy ensures that Exmouth Swimming and Life Saving Society:

- Complies with data protection law and follows good practice.
- Protects the rights of volunteers, members, employees and others.
- Is open about how it stores and processes individual's data.
- Protects itself from the risks of a data breach.

Personal data is data that relates to a living individual who can be identified from that data. For instance, names, addresses, telephone numbers and email addresses, medical and disability information, video and photographic images; information about individuals obtained as a result of Safeguarding checks, financial information.

Lawful basis for processing

For personal data to be processed lawfully, we must be processing it on one of the legal grounds set out in the Data Protection Laws.

These may include:

1. the data subject has given their consent to the processing (eg. on their membership application form when they registered).
2. the processing is necessary for the performance of a contract with the data subject (for example, for processing membership subscriptions);
3. the processing is necessary for compliance with a legal obligation to

which the data controller is subject (eg. Safeguarding checks) having first ensured that the individual has given their explicit consent and our processing of those criminal records history is necessary under a legal requirement imposed upon us.

4. the processing is necessary for the legitimate interest reasons of the data controller or a third party (eg., keeping in touch with members about competition dates, upcoming fixtures).

Data protection principles

The Data Protection Laws set out 6 principles for maintaining and protecting personal data, which form the basis of the legislation. All personal data must be:

1. processed lawfully, fairly and in a transparent manner and only if certain specified conditions are met;
2. collected for specific, explicit and legitimate purposes, and not processed in any way incompatible with those purposes;
3. adequate and relevant, and limited to what is necessary to the purposes for which it is processed ("data minimisation");
4. accurate and where necessary kept up to date;
5. kept for no longer than is necessary for the purpose ("storage limitation");
6. processed in a manner that ensures appropriate security of the personal data using appropriate technical and organisational measures ("integrity and security").

Data subject rights

Under Data Protection Laws individuals have certain rights (**Rights**) in relation to their own personal data. In summary these are:

1. The rights to access their personal data, usually referred to as a subject access request;
2. The right to have their personal data rectified;
3. The right to have their personal data erased, usually referred to as the right to be forgotten;
4. The right to restrict processing of their personal data;
5. The right to object to receiving direct marketing materials;
6. The right to portability of their personal data;
7. The right to object to processing of their personal data; and
8. The right to not be subject to a decision made solely by automated data processing.

The exercise of these Rights may be made in writing, including email, and also verbally and should be responded to in writing by the Main Committee without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary.

Where the request is made by electronic form means, any information is to be provided by electronic means where possible, unless otherwise requested by the individual.

Notification and response procedure

If a member has a request or believes they have a request for the exercise of a Right, they should pass the request to a member of the main committee.

If an email exercising a Right is received by any member, they should direct it to secretary@exmouthswimming.org.

Your main obligations

What this all means for you can be summarised as follows:

1. Treat all personal data with respect;
2. Treat all personal data how you would want your own personal data to be treated;
3. Immediately notify you're the main committee if any individual says or does anything which gives the appearance of them wanting to invoke any rights in relation to personal data relating to them;
4. Take care with all personal data and items containing personal data you handle or come across so that it stays secure and is only available to or accessed by authorised individuals; and
5. Immediately notify the main committee if you become aware of or suspect the loss of any personal data or any item containing personal data.

Practical matters

Whilst you should always apply a common sense approach to how you use and safeguard personal data, and treat personal data with care and respect, set out below are some examples of dos and don'ts:

1. Never leave any items containing personal data unattended in a public place, e.g. on a train, in a café, etc and this would include paper files, mobile phone, laptops, tablets, memory sticks etc.
2. Never leave any items containing personal data in unsecure locations, e.g. in car on your drive overnight and this would include paper files, mobile phone, laptops, tablets, memory sticks etc.
3. Do encrypt laptops, mobile devices and removable storage devices containing personal data and lock laptops, files, mobile devices and removable storage devices containing personal data away and out of sight when not in use.
4. Do password protect documents and databases containing personal data.
5. Never use removable storage media to store personal data unless the personal data on the media is encrypted.
6. Use confidential waste disposal for any papers containing personal data, do not place these into the ordinary waste, place them in a bin or skip etc, and either use a confidential waste service or have them shredded before placing them in the ordinary waste disposal.
7. Do dispose of any materials containing personal data securely, whether the materials are paper based or electronic.

8. Do ensure that your screen faces away from prying eyes if you are processing personal data, even if you are working in the office. Personal data should only be accessed and seen by those who need to see it.
9. Do not leave personal data lying around, store it securely.
10. Never act on instructions from someone unless you are absolutely sure of their identity and if you are unsure then take steps to determine their identity. This is particularly so where the instructions relate to information which may be sensitive or damaging if it got into the hands of a third party or where the instructions involve money, valuable goods or items or cannot easily be reversed.
11. Do not transfer personal data to any third party without prior written consent of the main committee.
12. Do notify the main committee immediately of any suspected security breaches or loss of personal data.
13. If any personal data is lost, or any devices or materials containing any personal data are lost, report it immediately to the main committee.
14. However you should always take a common sense approach, and if you see any areas of risk that you think are not addressed then please bring it to the attention of the main committee.

Queries

If you have any queries about this Policy please contact ESLSS Secretary at secretary@exmouthswimming.org