DATA PROTECTION POLICY

1. Introduction

1.1 The Lido needs to collect and use information. The purpose of this policy is to ensure that it is handled carefully, transparently and in accordance with the latest legal regimes, specifically the General Data Protection Regulation (GDPR).

1.2 This policy applies to all individuals who use personal information on behalf of the Lido, including employees and Trustees. Together with the Privacy Notice, it sets out the basis on which we process personal information and our obligations in respect to data protection.

2. Definitions

2.1 Personal information: any information which directly or indirectly can be used to distinguish or trace a person's identity. This includes, but is not limited to: name, address, job, email address, phone number, national insurance number, IP address, date of birth, bank card details, passport number, vehicle registration plate number or biometric information of any person, whether they are a staff member's details or have another association with the Lido. For example, details held about persons identified as next of kin need to be handled as securely as those of our staff and customers. Under GDPR, this is known as 'personally identifiable information' (PII).

2.2 Special categories: information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health or medical condition, sexuality or sex life. This is sometimes known as 'sensitive personal data'. This sort of information is subject to special protections as set out in GDPR Article 9.

2.3 Criminal convictions data: Information on an individual's criminal history is treated in the same manner as special categories of data.

2.4 Data controller: an organisation that determines how and why data is used. The Lido is a data controller.

2.5 Data processor: an organisation that carries out data processing on behalf of the controller, and does not determine how and why the data is used. The Lido is not a data processor.

2.6 Data subject: the individual to whom particular personal data relates.

2.7 Information Commissioner's Office (ICO): the body that supervises data protection in the UK.

2.8 Personal Data Breach: a personal data breach means a breach of security leading to the accidental or unlawful destruction loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

A personal data breach takes place where a security incident has affected the confidentiality, integrity or availability of personal data. There will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Personal data breaches can include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission, and
- Loss of availability of personal data.

2.9 Information Asset Register/Data Audit: a document which records the main processes of personal data and the lawful basis for each process, as well as information on where it's stored, how it's transferred and who has access to it.

3. The data protection principles

3.1 The Information Commissioner's Office enforces the data protection principles and has other important responsibilities:

- The ICO upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

- The ICO has specific responsibilities set out in the Data Protection Act 1998, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.

- The ICO can take action to change the behaviour of organisations and individuals that collect, use and keep personal information. This includes criminal prosecution, non-criminal enforcement and audit. The ICO has the power to impose a monetary penalty on a data controller of up to €20,000,000, or 4% or global turnover.

- The European Union's General Data Protection Regulation (GDPR) is a new law which will apply in the UK from 25 May 2018. The UK's decision to leave the EU will not affect the commencement of the GDPR.

- Anyone who processes personal information must comply with eight principles of the Data Protection Act, which make sure that personal information is:

    1. fairly and lawfully processed;
    2. processed for limited purposes;
    3. adequate, relevant and not excessive;
    4. accurate and up to date;
    5. not kept for longer than is necessary;
    6. processed in line with your rights;
    7. secure; and
    8. not transferred to other countries without adequate protection.

3.2 You can find additional guidance on the implementation of these principles in the following sections of this policy.

4. Lawful condition for processing

4.1 Under GDPR, we are only permitted to collect, use and otherwise process personal information under certain conditions. These are known as lawful conditions for processing and are set out in more detail in the Lido's Privacy Notice.

4.2 We must identify and record at least one of these for each of our processes, including:

- Consent from the data subject
- A contractual duty
- A legal/regulatory obligation
- A legitimate interest.

4.3 Where the Lido process special categories of data (see 2.2 for definition), we must also satisfy an additional lawful basis (options are set out in Article 9 GDPR).

5. Individual's rights

5.1 Under GDPR, data subjects have certain rights when their data is being processed:

- To be informed about the collection and use of their personal data. This includes the purposes for processing their personal data, our retention periods for that

personal data, and who it will be shared with. This information should largely be provided through the Privacy Notice.

- To access their personal data, conformation their data is being processed and information with whom the data is shared. The exercise of this right is a 'subject access request' – see below.

- To erasure of certain information held about them. This applies where the Lido relies on their consent as the lawful basis of processing their data, where the information is no longer needed for the purposes for which it was collected, or where there is no overriding legitimate interest to continue the processing (such as performance of a contract). This is sometimes termed the 'right to be forgotten'.

- To have inaccurate personal data rectified, or completed if it is incomplete.

- To restrict processing. This is available while we verify the accuracy of a data subject's information, where data has been illegally processed, where we no longer need the information but the subject wants it to remain for use in legal proceedings or where the subject objects to the legitimate ground we have identified for the process.

- To object to processing on the basis of legitimate interests, unless we can demonstrate compelling legitimate grounds for the processing.

- To not be subject of automated decisions concerning them and to be able to port data if appropriate.

5.2 A request to exercise any of these rights can be made verbally or in writing. The Lido **must respond within 30 days**. Contact the Lido manager if you receive such a request.

6. Right of access

6.1 Anyone whose information is held by the Lido has the right to request access to personal information held about them. An exercise of this right is called a 'subject access request'.

6.2 These requests can be made in writing or verbally. The Lido must respond within 30 days free of charge, unless the request is demonstrably excessive or unfounded.

6.3 As well as giving access to the data subject's personal information itself, individuals can also request confirmation that their data is being processed and other supplementary information such as that set out in our Privacy Notice.

6.4 Bear in mind that when giving access to a data subject's information, third party information must not also be shared without the consent of that third party.

7. Privacy Notice

7.1 The Lido is committed to being transparent in relation to the collection and use of personal information and this is set out in our Privacy Notice which is readily available to staff, customers and anyone else whose personal data we process.

The Privacy Notice is available on the Lido website and sets out:

- Who the data controller is;
- The purpose or purposes for which the information will be processed; and
- Any other important information, such as who the data is shared with and why; and
- Will be kept up to date so as to accurately reflect data processing activities.

8. Information security

8.1 Personal information must be kept appropriately safe against unauthorised processing, accidental loss, destruction or damage.

8.2 The Lido has a data audit that sets out what information is held, why, the risks associated with that data, where it is stored, security/back-up arrangements and for how long it is kept, including details of the personal data held.

8.3 The storage, backup and security associated with protecting personal data is designed to reflect the identified risks.

8.4 Transmission of personal data (e.g. to our payroll supplier) will be via a password protected ttransfer.

9. Data sharing

9.1 The Lido will only share data with a third party where there is a lawful basis to do so (such as a contractual, legitimate interest or legal/regulatory basis) and examples of this are set out in the Lido's Privacy Notice (such as the HMRC), otherwise we will seek your consent.

9.2 Data protection requirements (including privacy by design and privacy impact assessments) should be built into any new contract negotiations and any tender processes.

9.3 We should only share data with organisations with whom we have a written agreement that details how personal information will be used (e.g. our payroll supplier). Compliance with this policy will be required as part of any data sharing agreement we have with third parties.

9.4 We must inform the relevant data subjects about data sharing activities in advance unless there are exceptional circumstances, such as where data sharing is necessary for the prevention and detection of a crime.

10. Data Retention

10.1 We retain as a general rule all information until the end of the following swimming season or following event (such as the Auction of Promises where intervals between events vary).

10.2 Data held for other lengths of time is set out in the Lido's Data Audit.

11. Responsibilities

11.1 The Lido Trustees are ultimately responsible for ensuring that the Lido processes the personal data of its staff, customers, volunteers, donors, teachers/contractors or any other individuals in compliance with data protection rules.

11.2 Many of these responsibilities are managed on a day-to-day basis by the Lido manager and the duty managers.

11.3 All those working with the Lido's personal data will be asked to read the Privacy Notice and this Data Protection Policy.

11.4 All of those listed in 11.1 and 11.2 are responsible for the careful handling of personal information in accordance with this policy. Failure to adhere to this policy may result in legal action against the Lido or the individual employee, or internal disciplinary action.

12. Reporting a Breach

12.1 Staff, the Trustees and customers are responsible for reporting possible or suspected personal data breaches (see Definitions section above).

Step 1: If you suspect that a personal data breach could have taken place, immediately report this to the duty manager or directly to the Lido's manager (the duty manager will report the incident to the Lido manager immediately).

Step 2: The Lido manager, in consultation with a Lido Trustee, will:

(i) Determine whether a breach has taken place.
(ii) If there has been a breach, an assessment will be made to decide if it is a notifiable breach i.e.is there a risk to individuals' rights and freedoms (referencing the guidelines set out on the ICO's website).

(iii) If it is a notifiable breach, then it must be reported to the ICO **within 72 hours of becoming aware of the breach, see www.ico.org.uk/for-organisations/report-a-breach.**

(iv) If there is also a 'high risk' to individuals' right and freedoms then inform the individuals without undue delay – the ICO website gives examples of what is meant by 'high risk'.

(v) Determine if the breach also meets the definition of a serious incident as set out by the Charity Commission and needs to be reported to them also – see https://www.gov.uk/guidance/how-to-report-a-serious-incident-in-your-charity

(vi) Record all decisions and justifications (including any decision not to report) and complete an Incident Report.

13. Discipline and other consequences

- The ICO has the power to levy fines of up to €20m, or 4% of turnover if an organisation fails to be compliant with GDPR.
- Any member of staff who violates this policy will be subject to appropriate disciplinary action or other remedial measures, up to and including termination of employment if warranted under the circumstances and permissible under applicable law.

Related Documents:	• Privacy Notice • Data Audit

Administrative purposes only:

Approved by: The Lido Trustees Date of Approval: October 2022 Review Date : October 2023