Stainland Lions Running Club – Data Protection Policy

Stainland Lions aims for full compliance with all applicable data protection legislation - GDPR in particular.

Any breaches or formal requests relating to data protection will be made to the Chair and/or Vice Chair and the appropriate action taken.

Club volunteers will be provided with guidance to ensure they are clear about their responsibilities.

All members will confirm they have read and agree to the club's Privacy Notice, which will be available on the club website.

The club committee will review compliance against GDPR quarterly.

Data Retention

Activity	Owner	Deletion timescales	Notes
Beginners course	Beginners Captain	4wks after course finishes	Beginners' personal details
Race reports	Publicity Officer	Local files deleted within 12 months	All publicly available information
Coaching plans	Coaches	N/A	No personal data stored
Membership data	Membership Secretary / Treasurer	4yrs after member leaves the club	
Financial information	Treasurer	Any personal / bank account data destroyed within 4yrs	The club's financial data is kept indefinitely
Relays	Men's & Ladies Captains	Within 4wks of the end of the race	
Club race entries	Race Director / Entries Secretary	Deleted from personal computers / paper entries destroyed within 4wks of race evaluation submitted to England Athletics	Results retained on our website indefinitely because participants may want to compare their times from previous years – covered by entry form wording
Club race results	Race Director / Entries Secretary / Results Secretary		
Social events	Social Secretary	Destroyed 4wks after the event has taken place	Personal information is rarely needed / obtained
Welfare/discipline	Welfare Officer	Files relating to a welfare issue are destroyed within 1yr of an issue being concluded	Some exceptions may be required and will be noted separately by the committee
WYWL	XC Captain	Files deleted within 4wks of the end of the XC season	
Vets	Vets Captain	N/A	No records – all managed by Vets
Club Championship	Club Championship Manager	Locally stored personal data for the previous year to be destroyed within 4wks of results presentations, i.e. annual dinner	Retained on the website indefinitely because participants may want to compare their results from previous years. Only name and result stored.
Away runs	Away Run Co-ordinator	Destroyed within 7 days of away run	Food orders

Data Breach Escalation Process

What is a data breach?

A data breach is defined by the Information Commissioners Office (ICO) as:

“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.”

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.

What breaches do we need to notify the ICO about?

When a personal data breach has occurred, we need to establish the likelihood and severity of the resulting risk to people’s rights and freedoms. If it’s likely that there will be a risk then we must notify the ICO; if it’s unlikely then we don’t have to report it. However, if we decide we don’t need to report the breach, we need to be able to justify this decision, so we should document it.

In assessing risk to rights and freedoms, it’s important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:

“A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.”

What process will we follow to meet the ICO’s 72hr deadline for escalating breaches?

1) The Chair and/or Vice Chair receive details of a breach within 24hrs of it occurring.
2) The Chair and Vice Chair review the breach together, specifically to:
    a. Consider the risk to individuals as a result of the breach.
    b. Escalate to the ICO within 48hrs using either the online form or helpline if there is a risk, if not then document the details / rationale.
    c. Arrange for affected individuals to be advised of the breach and actions we and they should take as soon as possible if there is a high risk to their rights and freedoms.
    d. Put any mitigating actions in place.
    e. Update at the next committee meeting or by email to committee members if more urgent discussion is required.
3) If either the Chair or Vice Chair are unavailable, then either the Welfare Officer or Membership Secretary will provide support (TBC).