The Whitehead Sports & Social Club
Data Breach Policy

The Whitehead Sport & Social Club (the Club) is committed to a policy of protecting individuals' right to privacy in accordance with the UK General Data Protection Regulation (GDPR)
and the Data Protection Act 2018 (the DPA).

This document sets out the guidance and procedure for data breach incidents at the Club and must be read in conjunction with the Club's Privacy Policy (add link).

The Club is required to take appropriate measures against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The GDPR requires the Club to report all sufficiently serious personal data breaches to the Information Commissioner's Office within 72 hours of becoming aware of the breach, and to maintain a log of all breaches. It is therefore crucial that the Club has a robust breach detection, investigation and internal reporting procedure in place.

This procedure applies to Club staff, Directors, customers, volunteers, contractors and third-party agents who may process data for or on behalf of the Club, and it must be complied with in the event of a data security breach.

What is a personal data breach?

The GDPR defines a **personal data breach** *as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.*

Personal data is any information relating to an identified or identifiable individual; an identifiable individual is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

A personal data breach can happen for a number of reasons. In general terms, a breach will occur whenever any personal data is lost, destroyed, corrupted or disclosed. Data breaches can fall into three categories:

(1) "Confidentiality breach" - where there is an unauthorised or accidental disclosure of,
or access to, personal data.

(2) "Integrity breach" - where there is an unauthorised or accidental alteration of personal data.

(3) "Availability breach" - where there is an accidental or unauthorised loss of access to,
or destruction of, personal data.

Examples of data breaches include:

- Loss or theft of data or equipment on which data is stored (e.g. loss or theft of a computer, portable device, such as a laptop or data stick)
- Unauthorised access to, use, or alteration of personal data
- Deliberate or accidental action (or inaction)
- Loss of availability of personal data (e.g. encrypted by ransomware, or accidentally lost or destroyed) or through equipment failure (e.g. data cannot be accessed and is not backed up)
- Human error (e.g. sending data to the wrong recipient or accidentally deleting it)
- 'Phishing' offences where information is obtained by a third party through deception.

What should I do when a breach occurs?

Any individual who accesses, uses or manages the Club's information is responsible for reporting a personal data breach and information security incidents **immediately** to the

- Data Protection and GDPR Officer (at GDPROfficer@whiteheadclub.co.uk), and
- The Secretary (at secretary@whiteheadclub.co.uk)

If the breach occurs or is discovered outside normal working hours, it must be reported **as soon as is practicable**.

If you know or suspect a personal data breach has occurred you should IMMEDIATELY:

- complete a data breach report form (see Annex), and
- email the completed form to GDRPOfficer@whiteheadclub.co.uk or hand deliver to a Director of the Club in person.

In the absence of the GDPR Officer, the breach report will be dealt with by another Director of Club.

Once a report form has been submitted and receipt of the report has been acknowledged, you should take NO FURTHER ACTION in relation to the breach unless specifically asked to do so.

Set out below is a guide to the procedure that the GDPR Officer will follow when he/she is made aware of a personal data breach.

On discovery of a breach

If the breach is a continuing breach, steps must be taken immediately to minimise the effect of the breach, e.g. to shut down a system or alert relevant staff.

Following receipt of a report of a suspected breach GDPR Officer will confirm whether a breach has occurred and assess the risks associated with it. They will ask the person reporting the breach to provide full and accurate details of the incident, when the breach occurred (dates and times), if the data relates to people, the nature of the information, and how many individuals are involved.

All staff should be aware that any breach of the Data Protection Act may result in the
Club's Disciplinary Procedures being instigated.

An initial evaluation will be made by the GDPR Officer in liaison with relevant Club staff to establish the severity of the breach and who will take the lead investigating the breach (this will depend on the nature of the breach in most cases it will be a member of the Senior Board.

The evaluation of the breach will include an assessment of:

- the type of data involved
- its sensitivity
- the protections which are in place (e.g. encryptions)
- what has happened to the data (e.g. has it been lost or stolen)
- whether the data could be put to any illegal or inappropriate use
- who the individuals are, number of individuals involved and the potential
- effects on those data subject(s)
- whether there are wider consequences to the breach

The person leading the investigation will contact the relevant members of staff to explain:

- the nature of the breach
- an indication of the seriousness of the breach
- any action the Club must take immediately; in order to

  (i) to contain the breach and
  (ii) to become compliant with the UK GDPR/DPA and/or
  (iii) to prevent a similar situation from arising in the future.

The GDPR Officer will continue to monitor the situation to ensure that the department or persons responsible for the breach completes any required actions as soon as possible.

Managing the consequences of a breach

Depending on the seriousness of the breach and following guidance issued by the Information Commissioner's Office (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/). The Data Protection and GDPR Officer may advise on what further steps should be taken, which may include:

- informing the Board of Directors;
- informing the Information Commissioner's Office (this is mandatory where there is a serious risk to people's rights and freedoms);
- informing the data subjects affected by the breach.

Record keeping

The Club maintains a Personal Data Breach Register to record details of all breaches. This record is maintained by the GDPR Officer.

Preventing a repetition of a breach

After completing the procedures set out above, the GDPR Officer will evaluate the breach and the effectiveness of the Club's response to it.

The Data Protection and GDPR Officer will consider any changes that may be required to be made to Club policies and procedures to prevent a breach from recurring.

ANNEX: Data breach reporting template

1	Summary:		
2	Date / time of incident:		
3	Date / time incident was discovered:		
4	Details:		
5	How was breach discovered:		
6	Cause:		
7	Numbers affected by breach:		
8	Numbers receiving the information		
9	Date / time reported to Data Protection and GDPR Officer		
10	Type of personal data involved in breach:		
11	Source of incident:		