PENTATHLON GB

INFORMATION SECURITY POLICY

Introduction

Pentathlon GB needs to collect and use information about the members, athletes, staff and others with whom we come into contact in order to carry out our work. The law, through the GDPR (General Data Protection Regulations) requires us to collect, manage, store and deal with personal data appropriately and responsibly. This policy applies to all personal data held by Pentathlon GB.

Correct Treatment of Personal Information

Pentathlon GB places great importance on the correct treatment of personal information as a key element in the success of our working relationships, and in maintaining the confidence of those with whom we deal. We intend to ensure that personal information is treated lawfully and correctly. To that end, we will adhere to the following key GDPR principles:

1. Lawfulness, transparency and fairness: The lawful basis on which the data is processed, this must be demonstrated fairly and transparently to the data subject.
2. Purpose limitation: Ensuring data is captured for specific and legitimate purposes.
3. Data minimisation: Ensuring personal data is adequate and relevant.
4. Accuracy: Ensuring personal data is kept up to date.
5. Storage Limitation: Ensuring data is kept no longer than necessary.
6. Integrity and confidentiality: Ensuring appropriate measures are in place to ensure security of the data including the prevention of unauthorised and unlawful processing to protect against accidental loss, destruction, or damage.

***

1. Lawfulness, transparency and fairness

a) Data Storage

Information and records relating to members, competitors, Board, staff and athletes will be stored securely and will only be accessible to authorised staff and volunteers (see Section 6 c) Access Controls for more detail).

b) Breach Reporting

A data breach is defined by the GDPR 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”.

PENTATHLON GB

Process for reporting a data breach:

Action	Responsible Person	Outcome
A Pentathlon GB member, member of staff or staff at Sport80 discovers there has been a breach of security contravening the GDPR.	A Pentathlon GB member, member of staff or staff at Sport80 discovers there has been a breach of security contravening the GDPR.	Security Breach discovered.
The member of staff who has been notified by the Pentathlon GB member must take down as many details as possible including date and time breach occurred, number of records affected (if known) and how the breach occurred (if known). Or The member of staff (PGB or Sport80) who discovered the breach should have this information to hand (if known)."	Member of staff first notified	Security Breach reported to first point of contact.
The Head Office Manager should be notified immediately of the breach."	Member of staff first notified	Security Breach reported internally.
The Head Office Manager will notify the CEO and the Board Chair of the breach immediately.	Head Office Manager	Security Breach reported to Exec level.
On agreement from the CEO and the Chair, the Head Office Manager or Sport80 will notify the Information Commissioners Office (ICO) via the reporting tool on their website.	CEO Chair Head Office Manager	Security Breach reported to ICO. N.B. This must be reported within 72 hours of the breach occurring.
On agreement from the CEO and the Chair, the Head Office Manager will notify the company insurers.	CEO Chair Head Office Manager	Security Breach reported to Insurers.
On agreement from the CEO and the Chair, the Head Office Manager will notify the Pentathlon GB media officer and/or media agency, the IT Manager and SLT.	CEO Chair Head Office Manager	Security Breach reported to internal stakeholders.
The Head Office Manager will identify and brief which external provider (e.g. Sport80, IAP, Uni of Bath) and/or whichever staff members can put in place actions to mitigate further loss or damage of data.	Head Office Manager External providers. Other staff members	Further damage or loss of data mitigated.
Once extent of security breach is known, the Head Office Manager /Sport80 and IT Manager will provide a report to the CEO who will communicate with affected members/staff setting out the facts and actions being taken.	Head Office Manager IT Manager CEO	Affected members/staff notified.
The Head Office Manager will identify and brief which external provider (e.g. Sport80, IAP, Uni of Bath) and/or staff members can put in place actions to recover or fix any lost or damaged data.	Head Office Manager External providers Other staff members	Recovering and fixing of damaged or lost data.
Media officer and/or media agency to advise on further comms strategy to affected members/staff and deliver comms accordingly. This should be in consultation with insurance providers.	Media Officer and/or media agency. Insurance provider.	Affected members/staff notified of progress and final actions taken.
A report setting out what actions have been taken to prevent the breach occurring again will be written by the IT Manager/Sport80 and provided to the CEO and Chair for presentation at the next Board Meeting	IT Manager CEO	

c) Requests for Personal Data (either as an SAR or Right to Be Forgotten)

i. An SAR (Subject Access Request) is a request for personal information that our organisation may hold about an individual. If an individual wishes to exercise their subject access right, the request must be made in writing. The purpose of an SAR is to make individuals aware of and allow them to verify the lawfulness of processing of their personal data. Under the GDPR individuals have the right to obtain confirmation as to whether personal data is being processed. If personal information is being processed, they are entitled to access the following information:
- the reasons why their data is being processed;
- the description of the personal data concerning them;
- anyone who has received or will receive their personal data; and
- details of the origin of their data if it was not collected from them.

Fee: Pentathlon GB will not be able to charge for complying with a request unless the request is 'manifestly unfounded or excessive'. We may charge a reasonable administrative-cost fee if further copies are requested.

Excessive requests: if a request is 'manifestly unfounded or excessive' data Pentathlon GB can charge a fee or refuse to respond but will need to be able to provide evidence of how the conclusion that the request is manifestly unfounded or excessive was reached.

ii. A Right to Be Forgotten request
The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:
- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/ processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

PENTATHLON GB

Process for responding to a Subject Access Request (SAR) and "right to be forgotten":

Action	Responsible Person	Outcome
A Pentathlon GB member or ex member or member of staff or ex member of staff requests an SAR or Right to be Forgotten.	Requester	Request made.
The member of staff who has been notified by the requester notifies the Head Office Manager.	Member of staff first notified.	Request notified to HEAD OFFICE MANAGER.
The Head Office Manager will notify the CEO and the Board Chair of the request immediately.	Head Office Manager	Request reported to CEO.
The CEO will inform the Requester that all requests must be in writing and their request will or won't be actioned and provide rationale	Request notified to HEAD	Security Breach reported to Exec level.
The Head Office Manager will identify and brief which external provider (e.g. Sport80, IAP, Uni of Bath) and/or staff member who can deliver the request.	CEO	Requestor notified of status of request.
Head Office Manager notifies the CEO that the requested information is ready to be provided to Requestor.	Head Office Manager	CEO Notified.
The CEO provides the Requestor with the information and notifies them of the timeline should they wish to complain or require further action to be taken.	CEO	Requestor provided with information.
Case Closed Head Office Manager keeps records of request at H.O. of request. a) If an SAR then information provided should be filed in Case Notes. b) If a Right to be Forgotten then only the process notes to be filed, not the information provided to the requestor.	Head Office Manager	Case closed.

d) Data Handling, Access and Accuracy

All members have the right to access the information Pentathlon GB holds about them. We will also take reasonable steps ensure that this information is kept up to date.

In addition, Pentathlon GB will ensure that:

a) It has an appointed manager with specific responsibility for ensuring compliance with Data Protection.
b) Everyone processing personal information understands that they are contractually responsible for following good data protection practice.
c) Everyone processing personal information is appropriately trained to do so.
d) Everyone processing personal information is appropriately supervised.
e) Anybody wanting to make enquiries about handling personal information knows what to do.
f) It deals promptly and courteously with any enquiries about handling personal information.
g) It describes clearly how it handles personal information.
h) It will regularly review and audit the way it holds, manages and uses personal information.
i) Data is tracked and logged per data set.

2. Purpose limitation

a) Collection and Use of Personal Information

Members - Pentathlon GB stores the details that members provide when they apply for membership, renew their membership, enter a competition, results from that competition and details for training events camps etc. We do this in order to:

a) Maintain membership and competition records.
b) Respond to any enquiries you make.
c) Administer any events in which you participate or may wish to participate and to deal with any incidents you may be involved with.
d) Create an individual profile for you so that we can understand and respect your preferences.

e) Create statistics about members to enable us to secure funding (none of which will include personal information).
f) Contact you about pentathlon events, offers and opportunities available from Pentathlon GB or any commercial partner by post, email, online or phone.

Staff - Pentathlon GB stores the details that staff provide when applying for a job and the details required for HMRC, our payroll company and family member details for emergency contact purposes. We do this in order to:

a) Maintain HR records.
b) Respond to any enquiries from previous or new employers.
c) Response to any enquiries from HMRC.

Board Members - Pentathlon GB stores the details that Board members provide when applying for a directorship on the Board, details required for Companies House and details required for due diligence. We do this in order to:

a) Maintain Board member records.
b) Ensure compliance with the Governance Code for Sport.
c) Conduct Due Diligence to satisfy the organisation that the board member is a "Fit and Proper Person" to be holding this position of authority.

Athletes - Pentathlon GB stores the details of Athletes on the World Class Performance Programme, TASS and Talent Programme when they join the National Training Centre in Bath or are based another location. We do this to:

a) Be able to contact them to update them on the Programme, training and competitions.
b) For individualised feedback on their Training Logs.
c) Enable us to make international competition entries on their behalf.
d) Enable us to make national and international travel arrangements.
e) Analyse their training and performance.
f) Analyse historical medical information for injury prevention purposes.

b) Recording Images

Pentathlon GB may record and take pictures at competitions and events in which members participate and general images of competitors will form part of the information we hold and use. In addition to the purposes for general information set out above, Pentathlon GB may use these recordings and images for the purposes of education and training, promotion, performance, development and selection and event analysis.

Images may be disclosed to those regions and clubs for which you are a member for promotional purposes. They may also be disclosed to the media for promoting pentathlon and the reporting of events.

c) Disclosure of Your Information

Details of your achievements in events will be included on the Pentathlon GB website as well as reported on Facebook and Twitter, which will be available to the general public. We will retain competition results as a matter of public interest and to create Ranking Lists. If you do not want your results published this way contact **admin@pentathlongb.org** to request their removal.

Regions and clubs may publish details on the Pentathlon GB website and if you wish to remove this information you should contact the region or club directly.

d) Doping Control

If you enter competitions, you may be subject to doping control as part of the Pentathlon GB commitment to clean sport. At the time of sample collection, your personal data will be collected by the UK Anti-Doping Agency which undertakes the testing and administers the programme. The Pentathlon GB Privacy Policy can be found on the PGB website.

3. Data minimisation

a) Obtaining Consent to make contact

We will specify if the type of communication we want to send is either operational or marketing e.g.
- Marketing = Club or regional activity promotion, e-shop promotion, Competition promotion, etc.

- Operational = Timetable for a comp already entered, membership renewal date, notification of ranking list, admin message, AGM invite etc.

If the communication holds a Marketing message then we will only send this to members from whom we've capture prior consent via the Sport80 platform.

b) Competition Organisers, Regions and Clubs

We will ensure that we don't allow competition organisers, regions or clubs to send you Marketing messages unless we have received your specific consent via you setting your Marketing Preferences captured on the Sport80 platform.

4. Accuracy

a) Accuracy

We will ensure that all data we hold is up to date and that the Sport80 platform is user friendly and easy to navigate to facilitate capturing the correct data from the member/competition organiser.

5. Storage Limitation

Ensuring data is kept no longer than necessary.

a) Member Records

We will ensure that lapsed memberships are archived on the Sport80 platform in such a way as to be retrievable in the case of an SAR request but invisible to all users.

b) Staff Records

We will ensure that when a member of staff or Board member leaves the organisation their paper records will be archived and held in secure storage.

c) Athlete Records

We ensure that any documentation regarding Athlete Review Meetings is archived in a paper filing system which is securely locked away accessible only to the Performance Director.

Medical records are stored, and destroyed, by EIS in compliance with:
a) EIS own GDPR policies.
b) UK Sport requirements as set out in the Athlete Agreement.
c) GDPR requirements.

6. Integrity and confidentiality

a) Employee Handbook

The Pentathlon GB Employee Handbook specifies that:
- Staff must regularly change passwords.
- Staff must update software when prompted to do so by IT support.
- Staff must adhere to strict email and internet use practices to minimise potential cyber risk.
- Privacy proofing of all new projects and initiatives.

b) Employee Training

We will ensure that all staff undertake a programme of annual Mandatory Training which will include:
- Familiarisation with this Policy.
- Knowledge of what to do in the event of a data security breach, SAR and Right to be Forgotten request.
- Detail how movement of data will be tracked and logged i.e.
• Map out, against each data set:
  Where that data/set goes (includes EIS footage).
  Who it was sent to

When it was sent
Why it was sent

- Create a disposal tracking policy to remind us when to dispose of personal data that is no longer required.
- Detail how data will be destroyed and disposed of.

c) Access Controls

We will ensure that access to data is controlled as follows:

i. On the Sport 80 platform by Sport80 assuming the role of Data Processor and running their operations in strict accordance with GDPR and the terms set out in their Contract with Pentathlon GB.
ii. By individual Teams at Pentathlon GB - See Appendix 1.
iii. By running a Tracking Log of when data sets are provided to any persons or organisations who are not staff members of Pentathlon GB.

d) Physical Security

i. Pentathlon GB's location at the Sports Training Village, University of Bath means that physical access to our office and facilities is managed and protected by the University's security system.
ii. No personal information captured on the Sport80 platform will be released either face to face or via a telephone calls by Pentathlon GB Head Office unless 3 security questions are correctly answered. The security questions will be:
- Membership number and/or date of birth.
- Last competition they competed at.
- First line of address and/or school they attend
iii. All staff of Pentathlon GB will know how to dispose of data securely and within the parameters of the Regulations.

e) Network Security

i. File Access - Pentathlon GB's location at the Sports Training Village, University of Bath means that network security is managed and protected by the University's Security protocols.
ii. Email accounts – the management of the email accounts are provided to Pentathlon GB staff by a Microsoft Solution Provider (IAP UK Ltd). The email server is provided by Microsoft through their Office 365 service.

f) Data Use Outside of the EU

If an athlete applies for, or takes part in, an event that takes place outside the European Union, their information will be disclosed to the relevant event organiser(s) in the host nation. These nations may not have laws as stringent as ours to protect your personal data although all means to interrogate the validity of any data requests will be undertaken.