Hampstead & Westminster Hockey Club
EST 1894

Data Breach Notification Procedure

1. Purpose

HWHC Limited ("we"/"us") have this procedure in place to provide a standardised response to any reported data breach incident, and ensure that data breaches are appropriately logged and managed in accordance with the law and best practice.

2. Scope

This procedure applies in the event of a personal data breach and applies to all current and former members, players, customers, employees, contractors, sub-contractors, volunteers, office holders and participators of HWHC Limited at all times.

The document applies to all information we hold and all information technology systems utilised by us.

3. Responsibility

3.1. All employees/staff, contractors or temporary employees/staff, volunteers and third parties working for or on behalf of us are required to be aware of, and to follow this procedure in the event of a personal data breach.

3.2. All employees/staff, contractors, volunteers or temporary personnel are responsible for reporting any personal data breach to the Data Protection Officer contact details are as follows:

Name: Christine Shrimpton
Email: christineshrimpton@hotmail.com

4. Definition

The GDPR defines a "personal data breach" in Article 4(12) 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". Examples include:

4.1. Loss or theft of data or equipment on which data is stored
4.2. Access by an unauthorised third party
4.3. Sending personal data to an incorrect recipient
4.4. Alteration of personal data without permission
4.5. Loss of availability of personal data such as equipment failure
4.6. Unforeseen circumstances such as a fire or flood
4.7. Hacking attack
4.8. 'Blagging' offences where information is obtained by deceit for the purposes of this procedure data security breaches include both confirmed and suspected incidents.

If you suspect a data breach or are unsure whether the incident which has occurred constitutes a data breach, please refer the matter to the Data Protection Officer for consideration.

5. Reporting an incident

5.1. Any individual who accesses, uses or manages information within our business is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer.

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

5.3. The report will include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, the nature of the information, and how many individuals are involved.

6. Next Steps

6.1. The Data Protection Officer will, firstly, determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

6.2. An initial assessment will be made by the Data Protection Officer in liaison with relevant persons (which may include IT services) 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).

6.3. An investigation will be undertaken immediately and wherever possible within 24 hours of the breach being discovered/reported.

6.4. The Data Protection Officer will investigate the risks associated with the breach, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

6.5. The Data Protection Officer will then establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

6.6. The Data Protection Officer will identify who may need to be notified. The relevant procedures from those identified below will then be followed. Every incident will be assessed on a case by case basis.

7. Procedure – Breach notification data processor to data controller

7.1. HWHC Limited must report any personal data breach or security incident to the data controller without undue delay.

7.2. The breach notification should be made by email and/or telephone.

7.3. A confirmation of receipt of this information should be requested and made by email and/or telephone.

8. Procedure – Breach notification data controller to supervisory authority

8.1. The Data Protection Officer will determine if the supervisory authority (the Information Commissioner's Office (ICO) need to be notified in the event of a breach.

8.2. If the breach affects individuals in different EU countries, the ICO may not be the lead supervisory authority. The Data Protection Officer will also need to establish which European data protection agency would be the lead supervisory authority for the processing activities that have been subject to the breach.

8.3. The Data Protection Officer will assess whether the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach, by conducting an investigation and/or an impact assessment. If it is decided that there is no need to report the breach to the ICO, the The Data Protection Officer will justify and document this decision.

8.4. If a risk to data subject(s) is likely, the Data Protection Officer will report the personal data breach to the ICO without undue delay, and not later than 72 hours after becoming aware of it.

8.5. If the data breach notification to the ICO is not made within 72 hours, the Data Protection Officer will submit notification electronically with a justification for the delay.

8.6. If it is not possible to provide all of the necessary information at the same time we will provide the information in phases without undue further delay.

8.7. The following information needs to be provided to the supervisory authority:

8.7.1. A description of the nature of the breach;
8.7.2. The categories of personal data affected;
8.7.3. Name and contact details of the Data Protection Officer;
8.7.4. Likely consequences of the breach;
8.7.5. Any measures taken to address the breach;
8.7.6. Any information relating to the data breach;
8.7.7. Approximate number of data subjects affected;
8.7.8. Approximate number of personal data records affected.

8.8. The breach notification should be made via telephone to the ICO. Alternatively, the Data Protection Officer may choose to report it online if they are still investigating and will be able to provide more information at a later date or if they are confident that the breach has been dealt with appropriately.

8.9. In the event the ICO assigns a specific contact in relation to a breach, these details are recorded in the Internal Breach Register.

9. **Procedure – Breach notification data controller to data subject**

9.1. If the personal data breach is likely to result in high risk to the rights and freedoms of the data subject, HWHC Limited will notify those/the data subjects affected without undue delay and in accordance with the Data Protection Officer recommendation.

9.2. A ‘high risk’ means the threshold for informing individuals is higher than for notifying the ICO. In any event the Data Protection Officer will document their decision-making process.

9.3. We will describe the breach in clear and plain language, in addition to information specified in clauses 8.7.1.-8.7.8. above.

9.4. The data controller takes subsequent measures to ensure that any risks to the rights and freedoms of the data subjects are no longer likely to occur.

9.5. If the breach affects a high volume of data subjects and personal data records, we will make a decision based on assessment of the amount of effort involved in notifying each data subject individually, and whether it will hinder our ability to appropriately provide the notification within the specified time frame. In such a

scenario a public communication or similar measure informs those affected in an equally effective manner will be considered by the Managing Director whose decision will be final.

9.6. If we have not notified the data subject(s), and the supervisory authority considers the likelihood of a data breach will result in high risk, HWHC Limited will communicate the data breach to the data subject by telephone or email.

9.7. We will document any personal data breach(es) in the Data Breach Register.

10. **Documentation requirements**

10.1. Internal Data Breach Register: there is an obligation for us to document each incident, incorporating the facts relating to the personal data breach, its effects and the remedial action(s) taken.

11. **Evaluation**

11.1. Once the initial incident is contained, the Data Protection Officer will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

11.2. Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

11.3. The review will consider various points, including but not limited to:

11.3.1. Where and how personal data is held and where and how it is stored;

11.3.2. Where the biggest risks lie, and will identify any further potential weak points within its existing measures;

11.3.3. Whether methods of transmission are secure; sharing minimum amount of data necessary Identifying weak points within existing security measures;

11.3.4. Staff awareness.

Document Control

A current version of this document is available to all members of staff in the office.

This procedure was approved by Richard Sykes, Director, on 8 May 2018 and is issued on a version controlled basis under his signature.

Signature: Date:

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	Richard Sykes	08/05/2018