Data Breach Notification Policy

1. INTRODUCTION, SCOPE & APPLICATION

1.1 Europe Netball is committed to the protection of all personal data for which it is the data controller.

1.2 The law imposes significant fines for failing to lawfully process and safeguard personal data and failure to comply with this policy may result in those fines being applied.

1.3 All members of staff must comply with this policy when processing personal data on behalf of Europe Netball. Any breach of this policy may result in disciplinary or other action.

1.4 This policy informs all members of staff on dealing with a suspected or identified data security breach.

1.5 In the event of a suspected or identified breach, Europe Netball must take steps to minimise the impact of the breach and prevent the breach from continuing or recurring.

1.6 Efficient internal management of any breach is required, to ensure swift and appropriate action is taken and confidentiality is maintained as far as possible.

1.7 Europe Netball must also comply with its legal and contractual requirements to notify other organisations' including the Information Commissioner's Office ("the ICO") and where appropriate data subjects whose personal data has been affected by the breach. This includes any communications with the press.

1.8 Failing to appropriately deal with and report data breaches can have serious consequences for Europe Netball and for data subjects including:

1.8.1 identity fraud, financial loss, distress, or physical harm;

1.8.2 reputational damage to Europe Netball; and

1.8.3 fines imposed by the ICO.

2. IDENTIFYING A DATA BREACH

2.1 A data breach is a **breach of security** leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, **personal data**.

2.2 This could be the result of a breach of cyber security, such as a hack or virus, or it could be the result of a breach of physical security such as loss or theft of a mobile device or paper records. A data breach includes loss of data and so does not have to be the result of a conscious effort of a third party to access the data. Some examples of potential data breaches are listed below:

2.2.1 Leaving a mobile device on a train or plane;

2.2.2 Theft of a bag containing paper documents;

2.2.3 Destruction of the only copy of a document; and

2.2.4 Sending an email or attachment to the wrong recipient; and

2.2.5 Using an unauthorised email address to access personal data; and

2.2.6 Leaving paper documents containing personal data in a place accessible to other people.

3. REPORTING A DATA BREACH UPON DISCOVERY

3.1 If any Europe Netball member, volunteer and/or Director suspects, or becomes aware, that a data breach may have occurred (either by them, another member, a volunteer, a **data processor**, or any other individual) then they must contact the Europe Netball Chair.

3.2 The data breach may need to be reported to the ICO and notified to **data subjects**. This will depend on the risk to **data subjects**. The Europe Netball Chair must always be consulted in deciding as to whether to report a data breach to the ICO. Initial investigations will inform as to whether the data breach should be reported.

3.3 If it is necessary to report a data breach to the ICO, then Europe Netball must do so within 72 hours of discovery of the breach.

3.4 It is therefore critically important that whenever a suspected data breach has occurred, this is reported internally to the Europe Netball Chair immediately.

4. INVESTIGATING A SUSPECTED DATA BREACH

4.1 In relation to any suspected data breach, the following steps must be taken as soon as possible. These do not have to be carried out as individual tasks, and the most appropriate way of dealing with any breach will depend on the nature of the breach and the information available at any time.

Breach minimisation:

4.2 The first step must always be to identify how the data breach occurred, the extent of the data breach, and how this can be minimised. The focus will be on containing any data breach and recovering any **personal data**. Relevant individuals and suppliers must be involved, to take technical and practical steps where appropriate to minimise the breach. Appropriate measures may include:

4.2.1 remote deactivation of mobile devices or logins;

4.2.2 shutting down websites and IT systems;

4.2.3 contacting individuals to whom the information has been disclosed and asking them to delete the information; and

4.2.4 recovering lost data.

Breach investigation:

4.3 When Europe Netball has taken appropriate steps to minimise the extent of the data breach, it must commence an investigation as soon as possible to understand how and why the data breach occurred. This is critical to ensuring that a similar data breach does not occur again and to enable steps to be taken to prevent this from occurring.

4.4 Technical steps are likely to include investigating, using IT forensics where appropriate, to examine processes, networks, and systems to discover:

4.4.1 what data/systems were accessed;

4.4.2 how the access occurred;

4.4.3 how to fix vulnerabilities in the compromised processes or systems;

4.4.4 how to address failings in controls or processes.

4.5 Other steps are likely to include discussing the matter with individuals involved, to appreciate exactly what occurred and why, and reviewing policies and procedures.

Breach analysis:

4.6 To determine the seriousness of a data breach and its potential impact on **data subjects**, and so as to inform Europe Netball as to whether the data breach should be reported to the ICO and notified to **data subjects**, it is necessary to analyse the nature of the data breach.

4.7 Such an analysis must include:

4.7.1 the type and volume of **personal data** which was involved in the data breach;

4.7.2 whether any special category personal data was involved;

4.7.3 the likelihood of the **personal data** being accessed by unauthorised third parties;

4.7.4 the security in place in relation to the **personal data**, including whether it was encrypted;

4.7.5 the risks of damage or distress to the **data subject**.

4.8 A breach notification report must be completed in every case of a suspected breach, and retained securely, whether or not a decision is ultimately made to report the data breach.

4.9 This will act as evidence as to the considerations of Europe Netball in deciding whether to report the breach.

5. EXTERNAL COMMUNICATION

5.1 All external communication is to be managed and overseen by the Europe Netball Chair.

5.2 If Europe Netball is the **data controller** in relation to the **personal data** involved in the data breach, which will be the position in most cases, then Europe Netball has 72 hours to notify the ICO if the data breach is determined to be notifiable.

5.3 A data breach is notifiable unless it is unlikely to result in a risk to the rights and freedoms of any individual. Europe Netball will assess the data breach against the following criteria taking into account the facts and circumstances in each instance:

5.3.1 the type and volume of **personal data** which was involved in the data breach;

5.3.2 whether any special category personal data was involved;

5.3.3 the likelihood of the **personal data** being accessed by unauthorised third parties;

5.3.4 the security in place in relation to the **personal data**, including whether it was encrypted;

5.3.5 the risks of damage or distress to the **data subject**.

5.4 When the data breach is likely to result in a high risk to the rights and freedoms of the **data subjects**, then the **data subject** must be notified without undue delay. This will be informed by the investigation of the breach by Europe Netball.

5.5 The communication will be coordinated by the Europe Netball Chair and will include at least the following information:

5.5.1 a description in clear and plain language of the nature of the data breach;

5.5.2 the name and contact details of the Data Protection Lead (the Europe Netball Chair);

5.5.3 the likely consequences of the data breach;

5.5.4 the measures taken or proposed to be taken by Europe Netball to address the data breach including, where appropriate, measures to mitigate its possible adverse effects.

5.6 There is no legal requirement to notify any individual if any of the following conditions are met:

5.6.1 appropriate technical and organisational protection measures had been implemented and were applied to the data affected by the data breach measures which render the data unintelligible to unauthorised persons (e.g., encryption);

5.6.2 measures have been taken following the breach which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise;

5.6.3 it would involve disproportionate effort to contact individuals. In which case a public communication or similar equally effective measure of communication to the data subjects shall be issued.

5.7 For any data breach, the ICO may mandate that communication is issued to **data subjects**, in which case such communication must be issued.

5.8 Staff shall not communicate directly with the press and shall treat all potential data breaches as confidential unless otherwise instructed in writing by the Europe Netball Chair.

5.9 All press enquiries in relation to the General Data Protection Regulation shall be directed to the Europe Netball Chair.

6. PRODUCING AN ICO BREACH NOTIFICATION REPORT

6.1 All Europe Netball members are responsible for sharing all information relating to a data breach with the Europe Netball Chair, which will enable a Breach Notification Report to be completed.

6.2 As much detail as possible should be provided in the Report relating to the nature of the breach, who is affected and the personal data that has been accessed or lost.

6.3 The Europe Netball Chair may require individuals involved in relation to a data breach to each complete relevant parts of the Breach Notification Report as part of the investigation into the data breach.

6.4 In the wake of a data protection breach, swift containment and recovery of the situation is vital. Every effort should be taken to minimise the potential impact on affected individuals, and details of the steps taken to achieve this should be included in this form.

6.5 The ICO requires that Europe Netball's Chair send the completed Breach Notification Report to casework@ico.org.uk, with "DPA breach notification report" in the subject field, or by post to: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

7. EVALUATION AND RESPONSE

7.1 Reporting is not the final step in relation to a data breach. Europe Netball will seek to learn from any data breach.

7.2 Therefore, following any breach an analysis will be conducted as to any steps that are required to prevent a breach occurring again. This might involve a step as simple as emailing all relevant members of staff to reinforce good practice, or providing additional training, or may in more serious cases require new technical systems and processes and procedures to be put in place.

8. DEFINITIONS

Term	Definition
Data Subjects	This includes all living individuals about whom Europe Netball holds personal data. This includes volunteers, Europe Netball staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.
Personal Data	Any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person 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 natural person.
Data Controllers	The people who or organisations which determine the purposes for which, and the way, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Law. Europe Netball is the data controller of all personal data used in its organisation for its own purposes.
Processing	Any activity that involves use of the data. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction. Processing also includes transferring personal data to third parties.