Data Breach Policy

# INTRODUCTION, SCOPE & APPLICATION

## Essex Metropolitan Netball Association (“EMNA”) is committed to the protection of all personal data for which it is the data controller.

## 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.

## All members of EMNA staff and volunteers must comply with this Policy when processing personal data on behalf of EMNA. Any breach of this Policy may result in disciplinary or other action.

## This Policy informs EMNA staff and volunteers on how to deal with a suspected or identified data security breach.

## In the event of a suspected or identified breach, EMNA must take steps to minimise the impact of the breach and prevent it from continuing or recurring.

## Any breach requires efficient internal management, to ensure swift and appropriate action is taken, and as far as possible, confidentiality maintained.

## EMNA must also comply with its legal and contractual requirements to notify other organisations including the Information Commissioner’s Office (“ICO”) and where appropriate, data subjects whose personal data has been affected by the breach, including any communications with the media.

## Failing to appropriately deal with and report data breaches can have serious consequences for EMNA and for data subjects including:

### Identity fraud, financial loss, distress or physical harm;

### Reputational damage to EMNA; and

### Fines imposed by the ICO.

# IDENTIFYING A DATA BREACH

## A data breach is a breach of securityleading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

## 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:-

### Leaving a mobile device on a train or plane;

### Theft of a bag containing paper documents;

### Destruction of the only copy of a document;

### Sending an email or attachment to the wrong recipient; Using an unauthorised email address to access personal data; and

### Leaving paper documents containing personal data in a place, where others could access it.

# REPORTING A DATA BREACH UPON DISCOVERY

## If any EMNA staff and/or volunteer suspects, or becomes aware, that a data breach may have occurred (by them, another staff member, a volunteer, a data processor or any other individual) then they must contact the EMNA Data Protection Lead immediately.

## 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 EMNA Data Protection Lead must always be consulted in making a decision as to whether to report a data breach to the ICO. Initial investigations will inform as to whether the data breach should be reported.

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

## The EMNA Data Protection Lead must be informed of any data breach immediately.

# INVESTIGATING A SUSPECTED DATA BREACH

## 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: -

## 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: -

### Remote deactivation of mobile devices or logins;

### Shutting down websites and IT systems;

### Contacting individuals to whom the information has been disclosed and asking them to delete the information; and

### Recovering lost data.

Breach investigation:

## When EMNA has taken appropriate steps to minimise the extent of the data breach, it must start an investigation as soon as possible to understand how and why the data breach occurred. This is critical to preventing a similar data breach from happening.

## Technical steps may include investigating, using IT forensics where appropriate, to examine processes, networks and systems to discover:

### What data/systems were accessed;

### How the access occurred;

### How to fix vulnerabilities in the compromised processes or systems; and

### How to address failings in controls or processes.

## Other steps may include discussing the matter with individuals involved to understand what occurred and why, and reviewing policies and procedures.

Breach analysis:

## It is necessary to analyse the data breach to determine its seriousness, its potential impact on data subjects, and to inform EMNA as to whether it should be reported to the ICO and data subjects notified.

## Such an analysis must include: -

### The type and volume of personal data involved in the data breach;

### Whether any special category personal data was involved;

### The likelihood of the personal databeing accessed by unauthorised third parties;

### The personal data security, including whether it was encrypted; and

### The risks of damage or distress to the data subject(s).

## For every suspected breach, a Breach Notification Report must be completed and retained securely, whether decision to report the data breach is made or not.

## This will act as evidence for EMNA in deciding whether to report the breach.

# EXTERNAL COMMUNICATION

## All external communication is to be managed and overseen by the EMNA Data Protection Lead.

## If EMNA is the data controllerof the personal datainvolved in the data breach, which is most likely, then EMNA has 72 hours to notify the ICO if it is a notifiable data breach.

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

### The type and volume of personal datainvolved in the data breach;

### Whether any special category personal data was involved;

### The likelihood of the personal databeing accessed by unauthorised third parties;

### The personal data security controls, including whether it was encrypted; and

### The risks of damage or distress to the data subject.

## When the data breach is likely to result in a high risk to the rights and freedoms of the data subject(s),then the data subject(s)must be notified immediately, as determined by the EMNA breach investigation.

## The EMNA Data Protection Lead will coordinate the communication and will include as a minimum, the following information:

### A clear and plain description of the data breach;

### The name and contact details of the EMNA Data Protection Lead;

### The likely consequences of the data breach; and

### The measures or proposed measures to be taken by EMNA, to address the data breach including, where appropriate, measures to mitigate its possible adverse effects.

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

### Appropriate technical and organisational protection measures had been implemented and were applied to the data affected by the data breach, in particular, measures which render the data unintelligible to unauthorised persons (for example encryption);

### 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; or

### It would involve disproportionate effort to contact individuals, in which case a public communication or equally effective method of communication shall be issued to the data subjects.

## For any data breach, the ICO may mandate that a communication be issued to data subjects; this must be actioned.

## Staff shall not communicate directly with the media and shall treat all potential data breaches as confidential unless otherwise instructed in writing by the EMNA Data Protection Lead.

## All media enquiries in relation to the General Data Protection Regulation or other data protection law shall be directed to the EMNA Data Protection Lead.

# PRODUCING AN ICO BREACH NOTIFICATION REPORT

## EMNA staff and/or volunteers are responsible for sharing all information relating to a data breach with the EMNA Data Protection Lead, which will enable a Breach Notification Report to be completed.

## The Report should include as much detail as possible relating to the breach, who is affected and the compromised personal data.

## As part of the investigation, the EMNA Data Protection Lead may require individuals involved in the data breach to each complete relevant parts of the Breach Notification Report.

## Following a data 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 the Report.

## The ICO requires that the EMNA Data Protection Lead send the completed Breach Notification Report to [casework@ico.org.uk,](mailto: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.

# EVALUATION AND RESPONSE

## Data breach reporting is not the final step. EMNA will seek to learn from any data breach.

## Therefore, following any breach an analysis will be conducted regarding any steps required to prevent a recurrence. Such as emailing all relevant staff to reinforce good practice, providing additional training, or may in more serious cases, require new technical systems, processes and procedures to be implemented.

# DEFINITIONS

| **Term** | **Definition** |
| --- | --- |
| Data Subjects | For the purpose of this policy, includes all living individuals about whom EMNA holds personal data. This includes volunteers, EMNA 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, in particular 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 | People whom or organisations, which determine the purposes for which, and the manner in which, any personal data, is processed. They are responsible for establishing practices and policies in line with applicable data protection law. EMNA is the data controller of all personal data used in EMNA for EMNA’s own purposes. |
| Processing | Any activity that involves use of the data. Including 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. |

2 November 2020