Data Security Breach Policy

Introduction

Special Olympics GB holds a large amount of data / information, both in hard and soft copy. This includes personal or confidential information, and also non-personal information which could be sensitive or commercial, for instance financial data.

Care will be taken to protect this type of data / information, to ensure that it is not lost, stolen or falls into the wrong hands, that its authenticity and integrity is maintained.

In the event of a breach, it is vital that appropriate action is taken to minimise associated risks.

What is a breach?

A data breach is an incident in which any of the types of data specified above is compromised, disclosed, copied, transmitted, accessed, stolen or used by unauthorised individuals, whether accidentally or on purpose. Some examples:

Accidental loss, or theft of equipment on which data is stored

- Unauthorised access to data
- Human error such as emailing data by mistake
- Failure of equipment and hence data held on it
- Loss of data or equipment through fire or flood, for instance
- Hacking attack
- Where information is obtained by deceiving a member of staff

Reporting of the breach

Data security breaches should be reported immediately to the Data Protection Officer, as the primary point of contact. The report should include full and accurate details of the incident, including who is reporting the incident, what type of data is involved, if the data relates to people, how many people are involved. The Data Officer will keep a log of this information. (*See Appendix*)

Investigation and Risk Assessment

The Data Protection Officer will initiate a Security Breach Team, who will be responsible for investigating data breaches. An investigation will be started within 24 hours of the breach being discovered, where possible.

The investigation will establish the nature of the breach, the type of data involved, whether the data is personal data relating to individuals, and if so who are the subjects and how many are involved.

The investigation will consider the extent of the sensitivity of the data, and a risk assessment performed as to what might be the consequences of its loss, for instance whether harm could come to individuals or to Special Olympics GB.

Containment and Recovery
The Team will determine the appropriate course of action and the required resources needed to limit the impact of the breach. This might require isolating a compromised section of the network, alerting relevant staff or shutting down critical equipment.

Appropriate steps will be taken to stop the breach, and recover data losses. This might entail attempting to recover any lost equipment, using backup mechanisms to restore compromised or stolen data and changing compromised passwords. Action will be also taken to stop the breach from recurring.

Notification
The Chief Executive Officer will be notified by the Team following a critical data breach involving large amounts of data, or a significant number of people whose personal data has been breached. The CEO will make a decision to inform any external organisation, such as the police or the Information Commissioner's Office based on the extent of the breach.

Notice of the breach may be made to affected individuals if it is determined that they will benefit from knowing about it, for example by being able to change passwords to help prevent potential fraudulent use of the data.

The Chief Executive Officer may decide to notify other data controllers (regions/clubs) of the personal data in question.

Review
Once the breach is contained a thorough review of the event will be undertaken by the Team, to establish the cause of the breach, the effectiveness of the response and to identify areas that require improvement.

Recommended changes to systems, policies and procedures will be documented and implemented as soon as possible thereafter.

Document Control
Approved by: Board of trustees
Date approved: 03.08.2015
Review date: One year

Appendix

Data Security Breach Log

Report #:
Date of Report:
Date of Incident:
Full Details of Incident:
Reported by:
Type of Data: (Please circle as necessary) *Confidential* *Personal* *Sensitive* *Financial*
Number of People to whom leaked information relates:
Date Breach Resolved:
Resolution Process:
Cross Reference for Repeated Events: