CEREBRAL PALSY SPORT DATA BREACH POLICY

Purpose

Cerebral Palsy Sport believes that sound policies in the following areas will significantly benefit the overall efficiency of the organisation with a focus on supporting the organisation in all aspects of the effective management of data.

1. Statement of Policy

a. This policy defines the principles and methods employed by Cerebral Palsy Sport to ensure the effective and safe management of data and personal information and the policy and procedures in the event of a data breach.

2. Scope of Policy

a. Cerebral Palsy Sport needs to keep certain information about its employees, service users, volunteers and other users to allow it to monitor performance, achievements, and health and safety etc.

b. It is also necessary to process information so that the organisation can comply with its legal obligations, staff recruitment and payment as well as courses and events organised. To comply with the law, information must be collected and used fairly, stored

safely and not disclosed to any other person unlawfully. To do this, Cerebral Palsy Sport must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 and the General Data Protection Regulation (Regulation (EU) 2016/679).

c. Cerebral Palsy Sport has been registered with the Information Commissioner's Office since 24th September 2009 and this registration is reviewed annually. The Registration reference number is: **Z1929253**

3. Policy

a. Unauthorised disclosure or loss of personal data

i. Cerebral Palsy Sport is required under the Data Protection Act 1998 and the General Data Protection Regulation (Regulation (EU) 2016/679) to ensure the security and confidentiality of all the personal and sensitive personal data it processes including that processed by third parties acting on its behalf. Every care should be taken by staff to protect the personal data they work with and to avoid the unauthorised disclosure or loss of personal data.

ii. This policy applies to all personal and sensitive personal data processed by the charity or anyone acting on behalf of the charity, as defined by sections 1 and 2 of the Data Protection Act and in full compliance with the General Data Protection Regulations 2018.

b. Legislative framework

i. There are eight Data Protection Principles contained in the Data Protection Act which must

be complied with when processing personal data. Failure to comply with any of these Principles is a breach of the Data Protection Act.

ii. Seventh Data Protection Principle
    1. This policy is concerned with the Seventh Data Protection Principle: 'Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.'

iii. Examples of a breach of this Principle would include:
    1. personal data accidentally being sent to someone (either internally or externally) who does not have a legitimate need to see it;
    2. databases containing personal data being compromised, for example being illegally accessed by individuals outside the charity.
    3. loss or theft of laptops, mobile devices, or paper records containing personal data;
    4. paper records containing personal data being left unprotected for anyone to see, for example:-
        a. files left out when the owner is away from their desk and at the end of the day;
        b. papers not properly disposed of in secure disposal bins that can then be extracted or seen by others;
        c. papers left at photocopying machines;

5. staff accessing or disclosing personal data outside the requirements or authorisation of their job;
6. being deceived by a third party into improperly releasing the personal data of another person; and
7. the loss of personal data due to unforeseen circumstances such as a fire or flood.

4. The difference between a security breach and a data breach and the notification process to follow.

a. A data breach relates to the loss of personal data and should be notified following the procedure described. A security breach relates to the loss of equipment containing personal data. Where a security breach has been notified that also involves personal data staff must also follow the data breach policy.

5. Action to be taken in the event of a data breach

a. On discovery of a data breach the following actions should be taken:-

i. Containment and recovery - Action to be taken

1. The immediate priority is to contain the breach and limit its scope and impact.
2. Where personal data has been sent to someone not authorised to see it staff should:
    a. tell the recipient not to pass it on or discuss it with anyone else;
    b. tell the recipient to destroy or delete the personal data they have received
    c. and get them to confirm in writing that they have done so;
    d. warn the recipient of any implications if they further disclose the data; and
    e. inform the data subjects whose personal data is involved what has

happened so that they can take any necessary action to protect themselves.

ii. The officer responsible for the area where the breach occurred must be notified and they must immediately report it to Chief Operating Officer providing the following information:
    1. date and time of the breach;
    2. date and time breach detected;
    3. who committed the breach;
    4. details of the breach;
    5. number of data subjects involved; and
    6. details of actions already taken in relation to the containment and recovery.

iii. The COO will ensure the Chair is made notified of the breach.

6. Assessing the risk

a. Who is responsible for action? – Senior Manager / COO

b. Action to be taken

i. The COO or a nominated person will conduct an investigation into the breach and prepare a report. This report will follow the ICO's guidance on Breach Management and will consider the following:
    1. How the breach occurred.
    2. The type of personal data involved.
    3. The number of data subjects affected by the breach.
    4. Who the data subjects are.
    5. The sensitivity of the data breached.
    6. What harm to the data subjects can arise? For example, are there risks to physical safety, reputation or financial loss?

7. What could happen if the personal data is used inappropriately or illegally?
8. For personal data that has been lost or stolen, are there any protections in place such as encryption?
9. Are there reputational risks from a loss of public confidence in the service Cerebral Palsy Sport provides?

7. Notifying the Information Commissioner

a. Who is responsible for action? – the COO
b. Action to be taken:
    i. The COO and the NSDM will determine whether the breach is one which is required to be notified to the ICO.
c. Who is responsible for notifying the ICO?
    i. Responsibility for notifying the ICO rests with the COO. They will complete a breach notification form.

8. Evaluation and response

a. Who is responsible for action?
    i. The managers or officers in the area where the breach occurred, COO and the NSDM.
b. Action to be taken
    i. Once the breach has been dealt with the cause of the breach needs to be considered. There may be a need to update policies and procedures, or to conduct additional training.
    ii. A report will be provided to the governance, Compliance and Human Resources committee with all elements of the breach as well as the evaluation and remedial action taken.

Document Control:

Policy Details			
Policy	CPS053 Cerebral Palsy Sport Data Breach Policy		
Status	Approved	**Version number**	V5
Approved by	Board of Trustees	**Date Approved**	07.02.2019

Cerebral Palsy Sport, Lytchett House, 13 Freeland Park, Wareham Road, Poole, Dorset BH16 6FA

Registered Charity No. 1088600