Record Keeping

5.5 Data Breaches

Statement of Intent
This policy has been written to take into account of the General Data Protection Regulation (May 2018), Data Protection Act 2018 (DPA), together with advice from the Information Commissioner's Office (ICO), and should be read in conjunction with Policy 5.3 'Data Protection'.

Aim
The aim of this policy is to reassure parents of how we will deal with a reported breach.

As an organisation should we experience a personal data breach under the GDPR or the DPA we will report such incidents to the ICO based on the following:

- Does the breach pose a risk to people?
- We will consider the likelihood and severity of the risk to the people's right and freedoms, following the breach.
- If, after assessment, it is likely there will be a risk we will notify the ICO; if it is unlikely then we do not have to report.
- We will ensure that we record all breaches, regardless of whether or not they need to be reported to the ICO. Any that we do not report to the ICO we will make sure that we have a written record of the justification for this decision.

Definition of a "personal data" breach
This means a breach of security leading to the accidental or unlawful destruction loss, alteration, unauthorised disclosure or, or access to, personal data. This includes both accidental and deliberate events.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission;
- loss of availability of personal data.

At the beginning of (and during) the investigation we will record:

- what happened and why;
- how many people were involved;
- a timeline when it happened; and
- what actions have been taken so far.

If we can recover the data we shall do so immediately. For example, if it has been sent to someone by mistake (eg. via email), we will ask them to delete it, or if in paper format to send it back to us securely (eg. Special Delivery), or we will arrange for a member of St Joseph's Nympsfield Out of School Club (OOSC) to collect it.

We will review our working practices and put into place any measures to prevent such a breach/potential breach occurring again.

Failure to notify the ICO of a notifiable breach

Failing to notify a breach when required to do so can result in a heavy fine up to £8.7 million or 2 per cent of your global turnover (ref ICO website). The fine can be combined with the ICO's other corrective powers under Article 58.

Responsibilities of Employees, Committee Members and Volunteers

All employees, committee members and volunteers will:

- take steps to ensure the security of personal data at all times;
- know how to recognise a personal data breach;
- IMMEDIATELY report any breach of which they become aware to the Data Protection Officer (DPO[1]. Prompt action is essential, because reports to the Information Commissioner's Office (ICO) must take place within 72 hours of the breach being discovered[2];
- record the nature of the breach and the action they have taken on a Data Breach Form (attached to this procedure).

Responsibilities of the DPL

Dealing with a personal data breach must be treated as an urgent priority and given adequate resources.

1. *Assessment*
    - Assess the severity and likelihood of the potential adverse risks of the breach – see Appendix 1 'Level of Risk'. This assessment will include:
        - nature of data involved;
        - sensitivity of data;
        - security mechanisms in place, eg. password protection;
        - information which could be conveyed to a third party about the individual;
        - number of individuals affected by the breach;
        - the risk of harm to those affected (eg. safeguarding issues)*.

* If we do not think there is a high risk to those affected, then ICO advises that we do not have to let them know about the incident. However, if we do think there is a high risk, then by law we will tell them without undue delay.

2. *External reporting*
    - Based on the assessment, decide whether the breach requires external reporting to:
        - the ICO**. If it needs reporting, this must be done within 72 hours of the initial discovery of the breach even if full details are not yet known. Reasons must be given for any delay. Failure to notify the ICO when required to do so can result in a significant fine;
        - the individual/s concerned: this must be done directly and without undue delay;
        - data processors for which the setting is a data controller;

[1] St Joseph's Nympsfield Out of School Club's DPO is the Committee Chairperson

[2] NOT when it occurred

    - a description of the nature of the personal data breach; including:
    - data controllers for which the setting is a data processor;
- Reports to the ICO must include:
    - a description of the nature of the personal data breach; including:
        - the categories and approximate number of individuals concerned;
        - the categories and approximate number of personal data records.
    - the name and contact details of the OOCS's DPO;
    - a description of the likely consequences of the personal data breach;
    - a description of the measures taken or proposed to be taken to deal with the breach, including measures to mitigate any possible adverse effects.
- Reports to individuals must be in clear and plain language and must include:
    - the name and contact details of the setting's DPO;
    - a description of the likely consequences of the personal data breach;
    - a description of the measures taken or proposed to be taken to deal with the breach, including measures to mitigate any possible adverse effects.
- Reports to data processors and data controllers must be according to their contracts.

** If the breach is reportable, we will call the ICO person data breach advice line, on 0303 123 1113 (open Monday to Friday 9am to 5pm. However, if we are unsure if the breach is reportable we will use the ICO self-assessment tool to help us decide or call the ICO personal data breach advice line.

3. *Containment and Action*
    - Decide what action needs to be taken to contain the breach and by whom.
    - Decide what action can be taken to recoup losses and/or limit damage caused by the breach.
    - Inform all relevant individuals of the action they need to take.

4. *Internal Investigation and Review*
    - Carry out an internal investigation into how the data breach occurred.
    - Determine whether the breach was a result of human error or a systemic issue.
    - Identify ways of preventing a recurrence, eg. through better processes or training.
    - Review and update processes as appropriate
    - Review and update training and information for Employees, Volunteers and Committee Members as appropriate.

5. *Recording and Internal Reporting*
    - Record full details of the breach, its effects and all decisions and action taken on a Data Breach Form (attached to this procedure).
    - Provide a written report on the breach to the Committee.

6. *Responsibilities of Committee Members (for Charitable Settings)*
    - Individual Committee Members have the same responsibilities as employees and volunteers, as stated above.
    - The Committee Members are responsible for advising the DPO, for receiving and making reports on data breaches, and for reviewing the setting's responses to data breaches.

Level of risk[3]

Low Low risk breaches may lead to possible inconvenience to those who need the data to do their job, such as the loss of, or inappropriate alteration of a telephone list. These should be dealt with internally but not reported to the ICO.

High These are risks which may have adverse effects on individuals such as emotional distress and physical or material damage. They may include:

- loss of control over personal data;
- discrimination;
- identity theft or fraud;
- financial loss;
- damage to reputation; and
- significant economic or social disadvantage.

These must be reported to the ICO

Further information

- Information Commissioner's Office (www.ico.org.uk)

Associated Policies and Procedures

- 1.2 : Safeguarding Children and Child Protection
- 5.3 : Data Protection
- 5.4 : Data Subject Access Requests

Version Number	Author	Purpose of change	Date
1.0	NP and HS	Updating policies	23.01.2023
2.0	KC	Reviewed and formatted: • further clarification about breaches; • inclusion of "Associated Policies and Procedures" section	26.02.2024 Committee Meeting

[3] These are examples taken from the ICO website. It is likely that guidance will become clearer over time.

Data Breach Recording Form

Date and time breach occurred	
Date and time breach discovered	
Breach reported by	
Description of breach	
Details of IT systems/software involved	
Other Information	

Form completed by: _____

Date: _____

Signed: _____

Data Risk Assessment Form

Nature of data involved:			
Number of individuals affected		Security mechanisms in place (eg. passwords, encryption etc).	

Nature of risk (X)	
Inconvenience	Financial Loss
Loss of control over personal data	Personal Security
Discrimination	Emotional distress
Identity theft or fraud	Other

Overall Severity of risk	**Overall likelihood of risk**
Negligible	Low
	Medium
	High
Low	Low
	Medium
	High
Medium	Low
	Medium
	High
High	Low
	Medium
	High

Reporting Requirement			
ICO	Yes/No	Individual	Yes/No
Processor/s	Yes/No	Controller/s	Yes/No

Form completed by: _____

Date: _____

Signed: _____

Data Breach Review Form

Nature of Data Breach	
Date of Data Breach	
Recommended actions to reduce risk of future breaches and minimise their impact	
Recommended changes to existing processes	
Recommended changes to security controls	
New training needs	
Financial implications	
Other notes	