St. Paulinus Catholic Primary School

"Inspiring all to live, learn and love in the light of Jesus."
(I am the light of the world; whoever follows me will never walk in darkness but will have the light of life." *cf* John 8:12)

GDPR - Data Protection 'Data Breach Procedure'

Responsible Governor Committee: Health and Safety

Version control

Version number	Date	Revisions made	By who?	Approval date
V01	06/07/2020	G.Duarte – DPO	E.Sinclair	
V01.1	19/9/2021	None made	G.Duarte	

GDPO
Data Protection - Data Breach Procedure

Covering both Data Protection Act 1998 and GDPR which replaces the DP Act 1998 on 25 May 2018

School Mission

"Inspiring all to live, learn and love in the light of Jesus"

The governors and staff of St. Paulinus School commit themselves to live as a community with Christ at its centre, characterised by living Gospel values within the Catholic Church. They commit themselves to provide the best possible education for each child in school and according to their needs and affirming their achievements.

Purposes

There are four main purposes to this policy:

- To establish an entitlement for all pupils
- To establish expectations for teachers of this subject
- To promote continuity and coherence across the school
- To state the school's approaches to this subject and to promote understanding of the curriculum.

Policy Statement

St. Paulinus Catholic Primary School holds large amounts of personal and sensitive data.
Every care is taken to protect personal data and to avoid a data protection breach. In the unlikely event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This breach procedure applies to all personal and sensitive data held by St. Paulinus Catholic Primary School. This procedure applies to all school staff including governing bodies, referred to herein after as 'staff'.

Purpose

This breach procedure sets out the course of action to be followed by all staff at St. Paulinus Catholic Primary School if a data protection breach takes place.

Names persons

Headteacher: Miss S.Hayes
Data Protection Officer: Miss G.Duarte

Legal Context

- **The Data Protection Act 1998** makes provision for the regulation of the processing (use) of information relating to individuals, including the obtaining, holding, use or disclosure of such information. Principle 7 of the Act states that organisations which process personal data must take:

  "appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".

- **Article 33 of the General Data Protection Regulations**

Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

   (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

   (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

   (c) describe the likely consequences of the personal data breach;

   (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Types of Breach

Data protection breaches could be caused by a number of factors. Some examples are:

- Loss or theft of pupil, staff or governing body data and/ or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment Failure;
- Poor data destruction procedures;
- Human Error;
- Cyber-attack, including 'phishing' or 'whaling';
- Hacking;
- 'Blagging' offences where information is obtained by deception;
- Unforeseen circumstances such as fire or flood.

Immediate Containment/Recovery

In the event that the School identifies or is notified of a personal data breach, the following steps should followed:

1. The person who discovers/receives a report of a breach must inform the Head Teacher or, in their absence, either the Deputy Head Teacher or the Data Protection Officer (DPO). If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

2. The Head Teacher / DPO must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT technician.

3. The Head Teacher / DPO must inform the Chair of Governors as soon as possible. As a registered Data Controller, it is the school's responsibility to take the appropriate action and conduct any investigation.

   However, should the Head Teacher/DPO require any expert guidance and assistance; they can contact the Information Governance Team at Kirklees Council. The Information Governance Team can be contacted either via telephone on 01484 221000 or by email **excluding any person identifiable data** to information.governance@kirklees.gov.uk

4. The Head Teacher / DPO must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from the school may wish to obtain advice from its legal support.

5. The Head Teacher / DPO must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

   a. Attempting to recover lost equipment.

   b. Contacting the relevant Council Departments, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or

individuals concerned. Consideration should be given to a global email to all school staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual making the enquiry back.

Whatever the outcome of the call, it should be reported immediately to the Head Teacher/ DPO.

c. Contacting the Council's Marketing and Communications Department so that they can be prepared to handle any press enquiries. The Council's Press Office can be contacted by telephone on 01484 221000 or via email **excluding any person identifiable data**

d. The use of back-ups to restore lost/damaged/stolen data.

e. If bank details have been lost / stolen, consider contacting banks directly for advice on preventing fraudulent use.

f. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

Investigation

In most cases, the next stage would be for the Head Teacher / DPO to fully investigate the breach. The Head Teacher / DPO should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data;
- Its sensitivity;
- What protections are in place (eg encryption);
- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What types of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach, such as harm to self, or finances, property or possessions.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office (ICO). A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The Head Teacher/DPO should, after seeking expert or legal advice, decide whether anyone is notified of

the breach. In the case of significant breaches, the ICO must be notified within 72 hours of the breach under the GDPR. Every incident should be considered on a case by case basis.

When notifying individuals, give specific and clear advice on what they can do to protect themselves and what the School is able to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the School's Complaints Procedure). The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach

Review and Evaluation

Once the initial aftermath of the breach is over, the Head Teacher/DPO should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next available Senior Management Team and Full Governors meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources or Internal Audit for advice and guidance.

This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance. Consideration should be given to reviewing this breach procedure whenever the data protection policy is reviewed.

Implementation

The Head Teacher/DPO should ensure that staff are aware of the school's Data Protection policy and its requirements, including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the School's Data Protection policy and associated procedures, they should discuss this with their line manager, DPO or the Head Teacher.

Further Information

ICO website: https://ico.org.uk/for-organisations/report-a-breach/

Policy Monitoring and Review

This policy will be reviewed following the 3-year Policy Review Cycle of the school or when there are significant changes to the curriculum that warrant it. It may also be reviewed earlier should it no longer comply with school practice or the legal requirements of schools.