



Data Breach Procedure for Parkgate Primary School

Purpose

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

1.0 Legal Context

Parkgate Primary School will comply with the requirements of Article 33 of the General Data Protection Regulations in relation to the Notification of a personal data breach to the supervisory authority

- 1.1. In the case of a personal data breach, the controller (the school) 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.
- 1.2. The processor shall notify the controller (the school) without undue delay after becoming aware of a personal data breach.
- 1.3. 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.
- 1.4. 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.
- 1.5. The controller (the school) 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.

2.0 Types of Breach

2.1. Data protection breaches could be caused by a number of factors. A number of examples are shown below:

- 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;
- Hacking.

3.0 Managing a Data Breach

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

- 3.1 The person who discovers/receives a report of a breach must inform the Head Teacher, the schools Data Protection Lead or the School's Data Protection Officer (DPO). If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable. This should be done by completing the attached breach notification form.
- 3.2. The 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.
- 3.3. The DPO must inform the Head/Chair of Governors as soon as possible if the breach is considered of a serious nature. As a registered Data Controller, it is the school's responsibility to take the appropriate action and conduct any investigation.
- 3.4. The 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's legal support should be obtained.
- 3.5 The DPO will take the decision based on the severity of a breach and the likely effect on data subjects as to whether the ICO should be notified (this should occur within 72 hours of the incident being identified) and to whether the data subject should be notified.
- 3.5. The 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 Department, so that they are prepared for any potentially inappropriate enquiries 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. 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 Process

1.0 Investigation

1.1 In most cases, the DPO is to fully investigate the breach. The 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 were in place (e.g. 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 type of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach.

1.2 A clear record should be made of the nature of the breach and the actions taken to mitigate it.

1.3 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.

1.4 A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

2.0 Notification

2.1 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.

2.2 The DPO should decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case by case basis.

2.3 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

3.0 Review and Evaluation

3.1 Once the initial aftermath of the breach is over, the DPO should fully review both the causes of the breach and the effectiveness of the response to it.

3.2 It should be reported to the next available Senior Management Team and Full Governors meeting for discussion.

3.3. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right.

3.4 If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources or Internal Audit for advice and guidance.

3.5 This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

4.0 Implementation

4.1 The /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.

4.2 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.

Breach Reporting Form

General Details

Incident Summary:	
When did the incident occur?	
Date identified?	
Was the School notified by 3 rd party?	Yes/No
Date reported to DPO :	
Reporting Officer:	
Role:	
Contact Number:	

About the Incident

Please describe the incident in as much detail as possible.

a) When did the incident happen?
b) How did the incident happen?
c) If there has been a delay in reporting the incident please explain the reasons for this.
d) What measures were in place to prevent an incident of this nature occurring?

e) Please provide extracts from any policies or procedures considered relevant to this incident, and explain which of these were in existence at the time of this incident. Please provide the dates on which they were implemented.

Personal data placed at risk

f) What personal data has been placed at risk? Please specify if any financial or sensitive personal data (special categories*) has been affected and provide details of the extent.

* Special Categories of Personal data include:

- The racial or ethnic origin of the data subject
- Their political opinions
- Their religious or philosophical beliefs
- Whether they are a member of a trade union
- Their genetic data
- Biometric data used to uniquely identify them
- Their physical or mental health or condition
- Their sex life or sexual orientation

g) How many individuals have been affected and how many data records are involved?

h) Are the affected individuals aware that the incident has occurred?

i) What are the potential consequences and adverse effects on those individuals?

j) Have any affected individuals complained to the school about the incident?

Containment and recovery

k) Has any action been taken to minimise/mitigate the effect on the affected individuals? If so, please provide details.

l) Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.

m) What steps have been taken to prevent a recurrence of this incident?

Miscellaneous

n) Have the police or any other regulatory bodies been informed about this incident?

o) Has there been any media coverage of the incident?

Administration (to be completed by the DPO)

Admin Ref:	
Admin – Incident Status	<ul style="list-style-type: none"> • To be reviewed • Advice issued • Governor assessment required • Referred to ICO • DPO Notice Issued • Closed
Admin – Classification	<ul style="list-style-type: none"> • Non-event • Near Miss • Confirmed Loss • Rights Issue
Admin – Breach Panel Convened	Yes/No
If yes, date convened:	
Admin - Supporting Documents	
Admin – Completed by	
Admin – Incident Classification	<ul style="list-style-type: none"> • 3rd Party Loss • Data sent / given to wrong recipient • Failure to comply with Rights request • Inaccurate Information • Information Obtained by Deception • Information Disclosed without Consent • Information not Encrypted / Secured • Insecure Disposal • Lost in Transit • Loss / Theft of Insecure Records / Equipment

	<ul style="list-style-type: none"> • Other • System / Application Failure • Unauthorised Access
Admin – Incident Cause	<ul style="list-style-type: none"> • Deliberate • Failure to take appropriate steps (to known risk) • Procedural error • Delay in responding • Inadequate policy or procedure • No policy or procedure • Avoidable Error • Criminal activity • Other
Admin – Data Subjects to be notified	Yes/No
If yes, date notified:	
Admin – ICO Notification	Yes/No
If yes, date notified:	
Summary of actions:	
Date Closed:	