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 personal data breach or suspected personal data breach takes place.

The purpose of this procedure is to ensure that:

- personal data breaches are identified and reported promptly;
- breaches are contained and the risk of harm to individuals is minimised;
- the School assesses the risk to the rights and freedoms of individuals;
- reportable breaches are notified to the Information Commissioner's Office (ICO) within the required timescale;
- individuals are informed where a breach is likely to result in a high risk to their rights and freedoms;
- all personal data breaches are documented, including those that do not require notification to the ICO; and
- lessons are learned and appropriate measures are implemented to prevent recurrence.

A personal data breach can include a breach of confidentiality, integrity or availability. It is not limited to the theft or loss of personal data. Examples include sending information to the wrong person, unauthorised access, accidental disclosure, loss of availability, cyber-attacks and inappropriate disposal of records.

1. Legal Context

Parkgate Primary School will comply with the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 in relation to personal data breaches.

1.1 In the case of a personal data breach, the School, as data controller, shall notify the ICO without undue delay and, where feasible, not later than 72 hours after becoming aware of the breach, where the breach is likely to result in a risk to the rights and freedoms of individuals. The 72-hour period runs from the time the School becomes aware that a personal data breach has occurred, rather than necessarily from the time the incident itself occurred. If notification to the ICO is not made within 72 hours, the School must provide reasons for the delay.

1.2 Where a processor becomes aware of a personal data breach affecting information processed on behalf of the School, the processor must notify the School without undue delay. Contracts with processors should contain appropriate requirements for breach notification and cooperation in accordance with Article 28 UK GDPR.

1.3 A notification to the ICO should include, where available: (a) a description of the nature of the personal data breach, including, where possible, the categories and approximate number of individuals concerned and the categories and approximate number of personal data records concerned; (b) the name and contact details of the School's Data Protection Officer or other appropriate contact point; (c) a description of the likely consequences of the personal data breach; and (d) a description of the measures taken or proposed to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

1.4 Where it is not possible to provide all information at the same time, the information may be provided to the ICO in phases without undue further delay. The School must not delay a reportable notification simply because the investigation is not yet complete.

1.5 The School shall document all personal data breaches, whether or not notification to the ICO is required. The breach record should include the facts surrounding the breach, when the School became aware of it, the categories of personal data involved, the individuals affected or potentially affected, the number of individuals and records involved where known, the likely consequences, the risk assessment, containment and remedial action, whether the ICO was notified and, if not, the reason, whether affected individuals were notified and, if not, the reason, and lessons learned and actions taken to prevent recurrence.

2. Types of Breach

2.1 Personal data breaches can be caused by a number of factors. Examples include:

- Loss or theft of pupil, staff, governor or other personal data;
- Loss or theft of equipment on which personal data is stored;

- Personal data sent to the wrong recipient;
- Unauthorised access to personal data;
- Inappropriate access controls;
- Accidental disclosure of personal data;
- Unauthorised alteration of personal data;
- Loss of availability of personal data;
- Equipment or system failure;
- Poor data destruction or disposal procedures;
- Human error;
- Phishing, malware, ransomware or other cyber-attacks;
- Hacking or other unauthorised access;
- Inappropriate sharing of information;
- Failure to apply appropriate security measures;
- Personal data left unsecured or accessible to unauthorised people; and
- Breaches involving a third-party processor or service provider.

A suspected breach must be reported even where it is not yet clear whether personal data has actually been accessed, lost, disclosed, altered or destroyed.

3. Managing a Data Breach

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

3.1 Immediate reporting

The person who discovers or receives a report of a suspected breach must inform the Head Teacher, the School's Data Protection Lead or the School's Data Protection Officer (DPO) as soon as possible. If the breach occurs or is discovered outside normal working hours, this should be reported as soon as reasonably practicable. Staff should not delay reporting because they are uncertain whether an incident constitutes a personal data breach. The incident should be recorded using the attached Breach Reporting Form. Where necessary, the DPO or designated person should record the exact date and time when the School became aware of the breach, as this is relevant to the 72-hour reporting period.

3.2 Containment

The DPO or designated person must establish whether the breach is still occurring. If so, immediate steps must be taken to contain the breach and minimise its effect. Depending on the circumstances, this may include shutting down or isolating a system; disabling user accounts; changing passwords; recalling or securing documents; asking an unintended recipient to delete or return information; remotely wiping lost or stolen equipment where appropriate; blocking unauthorised access; contacting the School's IT support; preserving relevant evidence; and taking urgent steps to protect affected individuals. Containment should be carried out carefully so that important evidence is not unnecessarily destroyed.

3.3 Escalation

The DPO must inform the Head Teacher and, where appropriate, the Chair of Governors as soon as possible where the breach is considered serious, involves a significant risk to individuals, involves safeguarding concerns, involves suspected criminal activity, or may attract significant regulatory or public interest. As the registered data controller, the School remains responsible for determining and implementing the appropriate response. Where a breach involves safeguarding concerns, the School's safeguarding procedures must also be followed.

3.4 Police and other bodies

The DPO must consider whether the Police or another relevant organisation needs to be informed. Police involvement may be appropriate where illegal activity is known or suspected, including theft, fraud, malicious hacking, blackmail, deliberate unauthorised access or other criminal activity. The School should obtain appropriate legal, safeguarding, cyber-security, insurance or other professional advice where necessary. The School must also consider whether any contractual, regulatory or other reporting obligations apply.

3.5 Risk assessment and notification

The DPO, or another person formally authorised by the School, must assess the risk to the rights and freedoms of the individuals affected or potentially affected. The assessment should consider the nature of the personal data; sensitivity; special category or other particularly sensitive information; whether children or vulnerable individuals are involved; number of individuals and records; who may have received or obtained the information; encryption or other protection; whether information was accessed, copied, disclosed, altered or lost; potential consequences; likelihood; and measures taken to reduce the risk. The School must consider both the severity of potential consequences and the likelihood of those consequences occurring.

3.6 ICO notification

The ICO must be notified where the breach is likely to result in a risk to the rights and freedoms of individuals. Where notification is required, it must be made without undue delay and, where feasible, within 72 hours of the School becoming aware of the breach. The School should not wait for the investigation to be fully completed before making a report.

3.7 Notification to affected individuals

Where the breach is likely to result in a high risk to the rights and freedoms of individuals, the School must inform the affected individuals without undue delay, subject to any applicable legal exception. The communication should be clear and in plain language and explain what happened, what personal data was involved, likely consequences, measures taken, what individuals can do to protect themselves, and who they can contact. A decision not to notify individuals must be documented, together with the reasons.

3.8 Recovery and mitigation

The DPO must take appropriate steps to recover any losses and limit the damage. Depending on the circumstances, steps may include attempting to recover lost equipment; asking an unintended recipient to securely delete or return information; contacting relevant organisations where necessary; using backups to restore lost or damaged data; contacting banks or other financial organisations where financial information has been compromised; changing passwords, access codes, encryption keys or other credentials; securing or isolating affected systems; arranging specialist technical or cyber-security support; and providing advice and support to affected individuals where appropriate.

4. Investigation Process

4.1 Investigation

In most cases, the DPO or designated investigator will investigate the breach. The investigation should establish, as far as reasonably possible:

- whose data was involved;
- what personal data was involved;
- the sensitivity of the information;
- whether special category or other sensitive information was involved;
- how the breach occurred;
- when it occurred;
- when the School became aware of it;
- what has happened to the data;
- whether the data has been accessed, copied, disclosed, altered, lost or destroyed;
- whether the data could be put to illegal or inappropriate use;
- what technical and organisational protections were in place;
- how many individuals are affected;
- what type of individuals are affected;
- whether children or vulnerable individuals are affected;
- the likely consequences for affected individuals; and
- whether there are wider consequences for the School.

4.2 A clear record must be made of the nature of the breach and the actions taken to contain, investigate and mitigate it. The risk assessment and the reasoning behind the ICO and individual notification decisions must also be recorded.

4.3 The investigation should be completed as a matter of urgency. Where an ICO notification is required, the School must not delay notification while waiting for the investigation to be completed. Further information can be provided to the ICO once it becomes available.

4.4 A more detailed review of the causes of the breach and recommendations for future improvements should be undertaken once the immediate incident has been resolved.

5. Notification

5.1 Some people or agencies may need to be notified as part of the initial containment or investigation. Depending on the circumstances, this may include the Head Teacher; DPO/Data Protection Lead; Chair of Governors; IT support or cyber-security provider; Police; safeguarding personnel; relevant Council services; insurers; affected individuals; parents/carers where appropriate; the ICO; and other relevant regulators or professional bodies.

5.2 The DPO should determine whether notification to the ICO is required following a documented risk assessment. The ICO must be notified without undue delay and, where feasible, within 72 hours where the breach is likely to result in a risk to individuals' rights and freedoms. The School should report early and provide further information later where the full circumstances are not yet known. Every incident must be considered on a case-by-case basis.

5.3 Where affected individuals are notified, the School should provide specific and clear advice on what happened, what personal data was involved, likely consequences, what the School has done to contain and mitigate the breach, what the individual can do to protect themselves, and who they can contact. Individuals should be given the opportunity to raise a complaint through the School's Complaints Procedure. The decision to notify, or not to notify, affected individuals must be recorded together with the reasons.

6. Review and Evaluation

6.1 Once the immediate aftermath of the breach is over, the DPO should review the cause of the breach; how it was detected; how quickly it was reported; the effectiveness of containment; the quality of the risk assessment; whether notification decisions were made appropriately; the effectiveness of communication; the effectiveness of existing technical and organisational measures; and whether further action is required.

6.2 Significant breaches and the lessons arising from them should be reported to the next available Senior Management Team and/or Full Governors meeting, where appropriate. Personal information about affected individuals should only be shared with governors or senior staff where necessary and appropriate.

6.3 If systemic or ongoing problems are identified, an action plan must be drawn up to address them. Actions should have named owners and, where appropriate, target completion dates.

6.4 If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources or the appropriate professional adviser for advice and guidance. Any disciplinary process should be conducted separately from the data breach investigation where appropriate.

6.5 This breach procedure should be reviewed following a significant breach; relevant legislative or regulatory changes; significant changes to ICO guidance; changes to the School's systems or processing activities; and at the School's normal policy review interval.

7. Implementation

7.1 The DPO/Data Protection Lead should ensure that staff are aware of the School's Data Protection Policy and its requirements, including this breach procedure. Staff should understand that suspected breaches must be reported promptly and that they should not attempt to conceal or delay reporting an incident.

7.2 If staff have any queries in relation to the School's Data Protection Policy or associated procedures, they should discuss these with their line manager, DPO/Data Protection Lead or Head Teacher.

Breach Reporting Form

General Details

Incident Summary:	
When did the incident occur?	
Date identified?	
Was the School notified by 3rd 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	• To be reviewed • Advice issued • Governor assessment required • Referred to ICO • DPO Notice Issued • Closed
Admin – Classification	• 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	• 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

	• Other • System / Application Failure • Unauthorised Access
Admin – Incident Cause	• 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:	