Data Incident and Breach Policy and Procedure

B – School Administration Policies & Procedures

Key author	Director of Finance & Operations
Audience	Employees; Parents
Approval body	Data Protection Committee
Approval frequency	3 Yearly
Last approved	December 2024
Date of next review	December 2027
Published	ClassLink; Portal; BSAK Website
Linked policies	Data Protection Policy

Contents

Document Control 2

Contents 3

Guidance on use 4

Data Incident and Breach Policy 5
- Introduction 5
- Definitions 5
- School Incident & Breach Team 6
- General Policy 6

Data Incident and Breach Response Procedure 7
- Introduction 7
- Definitions 7
- Procedure 8
  - Step 1: Reporting of Incident (Background) 8
  - Step 2: Containment 9
  - Step 3: Incident Assessment 10
  - Step 4: Reporting 12
  - Step 5: Accountability and Response 13

Data Security Incident and Breach Procedure Appendix 15
- Meeting agenda 15

Data Incident and Breach Policy

Introduction

This Data Incident and Breach Policy ("Policy") sets out how The British School Al Khubairat ("BSAK", "we", "our", "us") will respond to any data security incidents and breaches.

This Policy applies to all personal data we process regardless of the media on which that data is stored or whether it relates to past or present employees, students, parents, or other stakeholders (e.g. members of our Board of Directors).

This Policy applies to all staff at The British School Al Khubairat .

In accordance with our Data Protection Policy, we commit to utilising this Policy to ensure the correct and lawful treatment of personal data and to protecting the confidentiality and integrity of personal data. In accordance with the Federal Decree-Law No. 45 of 2021 regarding personal data protection (PDPL), we will use this Policy to ensure that when a data security incident is reported, we will quickly establish whether a personal data breach has occurred and, if so, use the Incident & Breach Policy & Procedure to take steps to address it. s The Data Protection Management Team is responsible for approving this Policy. Our Data Protection Management Committee is responsible for reviewing this Policy on a regular basis. You can contact our Data Protection Management Team by emailing dataprotection@britishschool.sch.ae if you have any questions or concerns.

Definitions

Breach can be broadly defined as a data security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed. This can include if someone accesses the data or passes it on without proper authorisation, or if the data is made temporarily unavailable, for example, when it has been encrypted by ransomware.

Data Security Incident means an event that compromises the integrity, confidentiality, or availability of an information asset. Data Incidents are situations which, upon further analysis, might be deemed by The Director of Finance & Operations to be a Data Breach (if the incident affects the confidentiality, integrity or availability of personal data) or might not. In short, every breach will necessarily involve a Data Security Incident, but not every Data Security Incident will result in a Breach.

Employee means a prospective, current, or former employee, contractor or volunteer.

Near Miss means any Data Security Incident which did not result in a Breach.

School Incident & Breach Team

Name	Role
Brunella Koutsileos	Director of Finance & Operations
Abdulkadir Hassan	Head of Compliance
Mark Leppard	Headmaster
Stephanie Jerron-Quarshie	Head of Communications
Paula Bentley	Compliance & Admin Coordinator

The Director of Finance & Operations is responsible for identifying and managing the school's response to data security incidents. A team, with the appropriate skills and organisational oversight, will be appointed to coordinate the school's response to a data security incident, and review those incidents that have taken place for lessons learnt.

General Policy

Employees are required to report all data incidents. Even if the Employee was not directly involved in the loss or disclosure, that Employee is obliged to report the matter immediately.

Upon reporting of a data incident, the Director of Finance & Operations shall follow the Breach Incident and Breach Response Procedure, which is hereby incorporated by reference.

The Director of Finance & Operations shall keep the Board of Governors updated on the status of all reported incidents and breaches under investigation. The determination regarding whether a particular incident or breach is considered closed (for reporting purposes) rests with The Board of Governors.
The Director of Finance & Operations is responsible for ensuring that the Incident Report Log, which is a catalogue of all reported incidents, is maintained and is up-to-date. This Log shall be reviewed regularly by the Director of Finance & Operations to ensure that we learn lessons from every incident by implementing appropriate measures to improve the operation of our data protection programme.

Data Incident and Breach Response Procedure

Introduction

This Data Incident and Breach Procedure ("Procedure") sets out how The British School Al Khubairat ("BSAK", "we", "our", "us") will report, assess and manage a personal data breach, or suspected personal data breach/incident. It is crucial that all stakeholders read and understand their roles within this Procedure, as it is how The British School Al Khubairat will ensure compliance with the regulatory requirements.

The Data Management Team is responsible for approving this Procedure.

This Procedure applies to all personal data we process regardless of the media on which that data is stored or whether it relates to past or present employees, students, parents, internal stakeholders (e.g. members of our Board of Directors), or other individuals.

This Procedure applies to all Employees at The British School Al Khubairat.

In accordance with our Data Protection Policy and the Data Incident and Breach Policy, we commit to utilising this Procedure to ensure the correct and lawful treatment of personal data and to protecting the confidentiality and integrity of personal data.

Our Data Management Team is responsible for overseeing this Procedure. You can contact our Data Management Team by emailing dataprotection@britishschool.sch.ae

Definitions

Breach can be broadly defined as a data security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed. This can include if someone accesses the data or passes it on without proper authorisation, or if the data is made temporarily unavailable, for example, when it has been encrypted by ransomware.

Data Security Incident means an event that compromises the integrity, confidentiality, or availability of an information asset. Data Incidents are situations which, upon further analysis, might be deemed by the Data Management Team to be a Data Breach (if the incident affects the confidentiality, integrity or availability of personal data) or might not. In short, every breach will necessarily be a Data Security Incident, but not every Data Security Incident will result in a Breach. Data Security Incident shall also be referred to herein as a "Security Incident."

Security Event means any reported or identified suspected Data Security Incident/Breach.

Procedure

Our Data Incident and Breach Procedure has five parts:

- Step 1: Reporting of Incident (Background)
- Step 2: Containment
- Step 3: Incident Assessment
- Step 4: Reporting
- Step 5: Accountability and Response

Step 1: Reporting of Incident (Background)
Employees are required to report all Security Events within a reasonable time frame after becoming aware of the data incident. When in doubt about whether a particular situation may represent a security incident/breach or not, Employees are encouraged to report. Reporting shall consist of an email to dataprotection@britishschool.sch.ae.

All reports of Data Incidents shall include the following information to the fullest extent possible:

- Name and phone number (for follow-up) of reporting staff member
- Brief description of what is factually known about the incident
- Did the security event occur while the school was in control of the data in question and/or did the breach involve a data processor/service provider
- Country in which the security event took place (e.g. if the security event took place at a data processor who processes data in a different country)?
- Does the security event involve paper and/or electronic information?
- When did the reporting staff member first learn about the security event (data and time)?
- How did the reporting staff member become aware of the security event?
- If applicable, what information systems are potentially affected/implicated?
- When (date and time) did the security event occur/start?
- Is the security event ongoing or has the threat been mitigated?
- What data has been affected (e.g. health information, disciplinary details etc)?
- Are the availability, confidentiality or integrity of any personal data affected?
- How many individuals have been impacted?
- How many data records were involved?
- Any actions that have been taken so far?

When new security events are reported, the Director of Finance & Operations] shall keep accurate notes regarding the reported incident within the Incident Report Log ("Log"). The 9ine App's Breach Incident Management module can facilitate this process. Log entries shall include identifying what (if any) actions have been taken thus far, by whom, and the exact time and date of the incident and when it was reported

Before progressing to the next step, the Director of Finance & Operations shall determine whether they should continue investigating the Security Event or, on the other hand, close it, if the report appears to be erroneous, false, and/or unsubstantiated.

Step 2: Containment
For those reported Security Events which appear as though they may be credible, the Director of Finance & Operations shall conduct a root cause analysis to determine whether the root cause(s) of the threat posed by the reported incident has been contained.

If the Director of Finance & Operations discerns during the course of that root cause analysis that the threat is ongoing, they will take steps to limit the impact, for example working with relevant stakeholders to:

- Secure or disconnect affected systems;
- Secure affected records or documentation;
- Halt affected business processes;
- Pause any processes that may rely on exposed information;
- Change passwords on all affected systems and applications;
- Install additional security scans for malware; and
- Implement new security measures.

The Director of Finance & Operations will also establish whether there is anything the school can do to recover any losses, e.g. physical recovery of data etc.

Step 3: Incident Assessment
Within 7 days of the Security Event being reported, after ensuring that the threat has been mitigated (as much as possible), the Director of Finance & Operations will conduct an assessment of the reported Security Event by establishing if a Breach or Security Incident has taken place using the 9ine App Incident Management module. If, in the course of that assessment, the Director of Finance & Operations determines that:

- a reported/identified security event does not represent a data incident, then it shall be logged in accordance with the "Data Breach Response" section of the Information Security Policy as a "near miss." If the Breach Response Team identifies any steps necessary to mitigate any threats, then those steps shall be completed and recorded in the log as well; or
- a data incident did occur (or is still occuring) but it did not (or does not) involve any personal data, then we shall handle the incident in accordance with the process outlined in the "Incident Management Process" subsection of the "Data Breach Response" section of the Information Security Policy; or
- a data incident had occurred (or is occuring) which affected the confidentiality, integrity or availability of personal data by involving the loss, destruction, corruption or unlawful disclosure or access of personal data, then the incident shall be classified as a data breach and handled in accordance with the process outlined below. After handling the breach in accordance with the process below, we shall then follow the "Incident Management Process" subsection of the "Data Breach Response" section of the Information Security Policy.

Regardless as to the classification above, the Director of Finance & Operations shall identify in the 9ine App whether the Security Event involved any personal data that is/was under the

control of a third party (e.g. when the personal data is being stored by a processor or joint controller). If the incident occurred while the data was under the control of a third party, the Director of Finance & Operations will review the contract of the third party to determine the next course of action with that third party in accordance with this Procedure and the Data Security Incident and Breach Policy.

For all incidents and breaches, if related to a breach of an information system, the Director of Finance & Operations shall assess and log:

- The type of information security incident which led to the breach (phishing, malware, password attack, zero-day exploit or denial of service)
- Which information systems were affected (application services, authentication services, internet access, file services, servers, storage, wireless services)
- Which information services were affected (access control, CCTV, email, finance, intranet, management or student information system, organisation website, printing, remote access)
- Whether a service desk ticket has been created to address the root cause and ensure that the breach is not ongoing
- What evidence can be provided to support the investigation of the incident

If the Director of Finance & Operations determines that a breach occurred, it shall then assess and log:

- What types personal data is involved in the breach (e.g. phone numbers, names, photographs, etc.);
- The cause of the breach;
- The extent of the breach (i.e., how many individuals are affected);
- The potential harm to affected individuals caused by the breach;
- Whether the breach is still ongoing;
- Were vulnerable individuals affected (e.g., children or an individual who is unable to act on their own behalf for mental or physical reasons); and
- How the breach can be contained (including identification of which internal/external stakeholders need to be engaged, if any)
- any special category data is involved
- the number and type (e.g. students, parents) of data subjects impacted as well as the number of personal data records.
- if applicable, whether the school's records of processing involves a relevant processing activity
- Whether the school was acting as a controller or processor of the data in question

For breaches, following an analysis of those issues, the Director of Finance & Operations will investigate several risk considerations:

- whether the nature, sensitive or volume of personal data affected could lead to any of the following damages for the data subject(s): damage or distress, reputational damage, financial loss, economic disadvantage, social disadvantage, confidentiality, identity theft.

- whether the identification of individuals through exposure of their personal data could lead to any of the following damages for the data subjects: damage or distress, reputational damage, financial loss, economic disadvantage, social disadvantage, confidentiality, identity theft.
- whether the characteristics of the individual(s) affected by the breach lead to any of the following damages to those data subjects: damage or distress, reputational damage, financial loss, economic disadvantage, social disadvantage, confidentiality, identity theft.
- whether the number of individuals affected by the breach lead to any of the following damages to those data subjects: damage or distress, reputational damage, financial loss, economic disadvantage, social disadvantage, confidentiality, identity theft.

Based on the results of those determinations, theDirector of Finance & Operations will then establish the overall level of risk present in the Breach by considering the likelihood and severity of the risk to people's rights and freedoms.

If the Director of Finance & Operations determines that the Breach is unlikely to pose a risk to individuals' rights and freedoms, the Director of Finance & Operations shall record in the 9ine App that Breach as a Non-Reportable Breach. TheDirector of Finance & Operations shall then continue to Step 5 of this Procedure.

For a Breach which is determined to pose a risk to individuals' rights and freedoms, the Director of Finance & Operations shall record that Breach within the 9ine App as a Reportable Breach and make a determination as to whether the risk posed to individuals is low or high.

For reportable breaches, the Director of Finance & Operations will schedule a data incident investigation meeting within 72 Hours. This meeting shall include the following key stakeholders: The Data Management Team. The objective of this meeting is to define the incident, establish a plan to manage the impact as soon as possible (within 72 hours) and confirm any required communication. (See Appendix for data incident investigation meeting agenda)

Step 4: Reporting

If the Breach is determined to be reportable in accordance with Step 3 (above), the Director of Finance & Operations shall, no later than 72 hours after the incident is first identified, notify the relevant supervisory authority/data protection authority/regulator and fill out the relevant forms supplied by that agency.

The following information must be provided to the regulator/supervisory authority:

- The categories and approximate number of individuals concerned;
- The categories and approximate number of personal data records concerned;
- The name and contact details of the Data Protection Officer (if necessary) or another contact point;

- Description of the breach;
- Description of the measures taken; and
- Any other available information at the time of notice.]

The above information will need to be tailored to your jurisdiction's requirements

Where all of the information set out in above is not known within 72 hours of discovering the incident, a preliminary report must be made to the supervisory authority/regulator/data protection authority, with additional information provided as it is learned.

Where the Director of Finance & Operations determines that a high risk to data subjects exists, the Data Management Team is responsible for notifying each individual that has been affected by the breach with the following information :

- A description of the breach;
- Likely consequences of the breach;
- Measures taken or proposed to be taken by the controller to address the breach;
- The name and contact details of the Data Protection Team or Director of Finance & Operations
- Advice to individuals to protect themselves from possible adverse consequences of the breach, such as by resetting passwords or monitoring credit scores.]

Communication to individuals affected should be transparent, such as:

- Email;
- Written communications.
- Voice communication

Where direct contact would involve a disproportionate effort, alternative methods of contacting individuals include:

- Website notification and advertisements in print media.

Step 5: Accountability and Response
After completing any necessary containment steps (identified in Step 2) have been implemented to stop any ongoing threat(s) and contacting any appropriate parties (as determined in Step 4) have been notified, the Director of Finance & Operations shall:

- Record all relevant information regarding the breach within the 9ine App including:
    - A summary of the incident
    - Proposed actions to be undertaken in response (specifically identifying who will be completing the actions and by when each action will be completed)
        - For reportable breaches, the proposed actions should include a recovery plan consisting of mitigating actions for each risk.

- An identification of the assessment decision (near miss, non-reportable incident, reportable incident)
- Any lessons learned

Data Security Incident and Breach Procedure Appendix A

Meeting agenda

The meeting should be structured around the following agenda. Each key point should be addressed and notes taken in minutes.

- Description of what has happened:
  - Details of the date, time and location of the incident
  - Nature of breach (Theft, accidental loss, inappropriate disclosure, procedural failure etc.)
  - Outline of the security protections (encryption, backup, physical security) that were in place and reasons why they failed in this case
- The scope and scale of the breach e.g:
  - Data subjects involved (Staff, students, parents)
  - The number of records involved
  - The format of the records (paper or digital)
  - The type of records/data involved
  - The potential risks to the rights and freedoms of natural persons
- Actions taken so far
  - Containment & recovery actions
  - Who has been formally and informally notified
- Required actions to mitigate the identified risks and the provision of 'necessary' resources to contain and manage the breach including:
  - HR
  - IT
  - Cyber Security
  - Data Protection Lead
- Communications plan
- Summary of actions with timescales & ownership
- Next meeting