PINNER WOOD SCHOOL

BREACH MANAGEMENT PLAN

Approval Authority:	
Effective From:	November 2021
Date Ratified by GB:	
Next Review Date:	November 2023

Breach Management Plan

The management response to any reported data security breach will involve the following four elements.

1. Containment and Recovery
   Data security breaches will require an initial response to investigate and contain the situation. It will also require a recovery plan which will include, where necessary, damage limitation. The recovery plan will need to involve input from our data protection staff, IT, HR and in some cases external suppliers.

2. Assessing the Risks
   Some data security breaches will not lead to risks beyond possible inconvenience, e.g. where a laptop is irreparably damaged but the files were backed up and can be recovered. While this type of incident can still have significant consequences the risks are very different from those posed by theft of parent/student data, where by someone may use this to commit identity fraud. Before deciding what steps are necessary further to immediate containment, assess the risks which may be associated with the breach. One of the most important is an assessment of potential adverse consequences for the individual/s, how serious or substantial these are and how likely are they to happen.

3. Notification
   Informing people and organisations that we have experienced a data security breach can be an important element in our breach management strategy. However, informing people about a breach is not an end in itself. Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints

4. Evaluation
   It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of our response to it. Clearly, if the breach was caused, even in part, by systemic and ongoing problems, then simply containing the breach and continuing 'business as usual' is not acceptable; similarly, if our response was hampered by inadequate policies or a lack of a clear allocation of responsibility then it is important to review and update these policies and lines responsibility in the light of experience. Existing procedures could lead to another breach and we will need to identify where improvements can be made.

Each of these four elements will need to be conducted in accordance with the checklist for Data Security Breaches. An activity log recording the timeline of the incident management should also be completed.

Checklist for Data Security Breaches

Step	Action	Notes
A	**Containment and Recovery:**	**To contain any breach, to limit further damage as far as possible and to seek to recover any lost data.**
1	DPO along with relevant members of staff to ascertain the severity of the breach and determine if any personal data is involved.	**See Evaluation of Incident Security**
2	DPO to investigate breach and speak with person who identified breach and record the breach on GDPRiS	To oversee full investigation and produce report. Ensure DPO has appropriate resources including sufficient time and authority.
3	Identify the cause of the breach and whether the breach has been contained? Ensure that any possibility of further data loss is removed or mitigated as far as possible	Establish what steps can or need to be taken to contain the breach from further data loss. Contact all relevant departments who may be able to assist in this process. This may involve actions such as taking systems offline or restricting access to systems to a very small number of staff until more is known about the incident.
4	Determine whether anything can be done to recover any losses and limit any damage that may be caused	E.g. physical recovery of data/equipment, or where data corrupted, through use of back-ups.
5	Where appropriate, the DPO or nominee to inform the police	E.g. stolen property, fraudulent activity, offence under Computer Misuse Act.
6	Ensure all key actions and decisions are logged and recorded on the timeline.	**See Evaluation of Incident Security**

B	**Assessing the Risks**	**To identify and assess the ongoing risks that may be associated with the breach.**
8	What type and volume of data is involved?	Data Classification/volume of individual data etc
9	How sensitive is the data?	Sensitive personal data? By virtue of definition within Data Protection Act (e.g. health record) or sensitive because of what might happen if misused (banking details).
10	What has happened to the data?	E.g. if data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk.
11	If the data was lost/stolen, were there any protections in place to prevent access/misuse?	E.g. encryption of data/device.
12	If the data was damaged/corrupted /lost, were there protections in place to mitigate the impact of the loss?	E.g. back-up tapes/copies.

13	How many individuals' personal data are affected by breach?	
14	Who are the individuals whose data has been compromised?	Students, Parents, Staff, or suppliers?
15	What could the data tell a third party about the individual? Could it be misused?	Consider this regardless of what has happened to the data. Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined
16	Is there actual/potential harm that could come to any individuals?	E.g. are there risks to: • physical safety; • emotional wellbeing; • reputation; • finances; • identify (theft/fraud from release of non-public identifiers); • or a combination of these and other private aspects of their life?
17	Are there wider consequences to consider?	E.g. a risk to public health or loss of public confidence in an important service we provide?
18	Are there others who might advise on risks/courses of action?	E.g. If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.

C	Notification	Notification is to enable individuals who may have been affected to take steps to protect themselves or allow the regulatory bodies to perform their functions.
19	Are there any legal, contractual or regulatory requirements to notify?	E.g.: terms of funding; contractual obligations
20	Can notification help the school meet its security obligations under the seventh data protection principle?	E.g. prevent any unauthorised access, use or damage to the information or loss of it.
21	Can notification help the individual?	Could individuals act on the information provided to mitigate risks (e.g. by changing a password or monitoring their account)?
22	If a large number of people are affected, or there are very serious consequences, inform the Information Commissioner's Office.	DPO
23	Consider the dangers of 'over notifying'.	Not every incident will warrant notification "and notifying all staff of an issue affecting only 20 may well cause disproportionate enquiries and work".

24	Consider whom to notify, what you will tell them and how you will communicate the message.	• There are a number of different ways to notify those affected so consider using the most appropriate one. Always bear in mind the security of the medium as well as the urgency of the situation. • Include a description of how and when the breach occurred and what data was involved. Include details of what has already been done to respond to the risks posed by the breach. • When notifying individuals give specific and clear advice on the steps they can take to protect themselves and also what the institution is willing to do to help them. • Provide a way in which they can contact the DPO directly
25	Consult the ICO guidance on when and how to notify it about breaches.	See Data Security Breach Policy
26	Consider, as necessary, the need to notify any third parties who can assist in helping or mitigating the impact on individuals.	E.g. police, insurers, professional bodies, funders, trade unions, website/system owners, bank/credit card companies.

D	Evaluation and Response	To evaluate the effectiveness of the Schools response to the breach.
27	Establish where any present or future risks lie.	
28	Consider the data and contexts involved.	E.g. what data is held, its extent, sensitivity, where and how it is stored, how long it is kept.
29	Consider and identify any weak points in existing security measures and procedures.	E.g. in relation to methods of storage and/or transmission, use of storage devices, levels of access, systems/network protections.
30	Consider and identify any weak points in levels of security awareness/training.	Fill any gaps through training or tailored advice.
31	Report on findings and implement recommendations.	Report to relevant people

Evaluation of Incident Severity

The severity of the incident will be assessed by the DPO along with others as required. Assessment would be made based upon the following criteria:

High Criticality: Major Incident	**Contact:**
• Highly Confidential/Confidential Data • Breach involves personal data • External third party data involved • Significant or irreversible consequences • Likely media coverage • Immediate response required regardless of whether it is contained or not • Requires significant response	DPO • Heather Richardson Other relevant contacts • Headteacher – Sarah Marriott • IT Lead – Greg Williams • IT – Dan Leigh • HR - EPM • Contact external parties as required ie police/ICO/individuals impacted
Moderate Criticality: Serious Incident	**Contact:**
• Confidential Data • Not contained within the School • Breach involves personal data • Significant inconvenience will be experienced by individuals impacted • Incident may not yet be contained	DPO • Heather Richardson Other relevant contacts • Headteacher – Sarah Marriott • IT Lead – Greg Williams • IT – Dan Leigh • HR - EPM • Contact external parties as required ie police/ICO/individuals impacted
Low Criticality: Minor Incident	**Contact:**
• Internal or Confidential Data • Small number of individuals involved • Risk to School low • Inconvenience may be suffered by individuals impacted • Loss of data is contained/encrypted	DPO • Heather Richardson Other relevant contacts • Headteacher – Sarah Marriott • IT Lead – Greg Williams • IT – Dan Leigh • HR - EPM