DATA SECURITY INCIDENT / BREACH POLICY AND PROCEDURE

1. Introduction

1.1. Manchester High School for Girls (the 'School') collects, holds, processes, and shares personal data, a valuable asset that needs to be suitably protected.

1.2. Every care is taken to protect personal data from incidents (either accidental or deliberate) to avoid a data protection breach that could compromise security.

1.3. Compromise of information, confidentiality, integrity, or availability may result in harm to individuals, reputational damage, detrimental effect on service provision, legislative non-compliance, and/or financial costs.

2. Purpose

2.1 This document describes how the School identifies and responds to a security incident or personal data breach.

2.2 It provides a structure for investigating and reporting security incidents and personal data breaches and for considering what action is necessary to secure personal data and prevent further breaches.

3. Fair Blame Principle

3.1 All employees have an important role to play in identifying, assessing and managing risk. To support employees in this role a Fair Blame Principle is promoted to encourage a culture of openness and willingness to admit mistakes. All employees must report any situation where things have or could have gone wrong. Balanced in this approach is the provision of information and support for employees through any such situation. At the heart of this principle is the desire to learn from events and situations in order to improve management processes on a continuous basis.

3.2 Provided that the full facts are told, no disciplinary action is taken because of an information security or personal data breach investigation, **unless** it is found that the employee acted:

- illegally - against the law (e.g. selling personal data or theft of equipment); or
- maliciously - intending to cause harm (e.g. deliberately releasing confidential information);
- deliberately, in contravention of school policies
  or
- recklessly - deliberately taking an unjustifiable risk where the employee either knew of the risk or deliberately closed their mind to its existence e.g. working while under the influence of alcohol or repeatedly making the same careless mistake.

4. Policy Statement

4.1 This document is made available to all employees via the staff intranet.

4.2 All employees must report all security incidents and personal data breaches to the School's Privacy and Compliance Officer (PCO) as soon as they become aware of them, or as soon as they suspect them.

4.3 The School logs all security incidents and personal data breaches and investigates each breach without delay.

4.4 Appropriate remedial action is taken as soon as possible to isolate and contain any breach, evaluate and minimise its impact, and to recover from the effects of the breach.

4.5 "Near misses" are investigated and recorded in the same manner as security incidents and data protection breaches.

4.6 Our procedures include allocated responsibilities, decision-making criteria and timescales for notifying data subjects, the supervisory authority, other regulatory authorities, the media or the police about a personal data breach as appropriate.

4.7 All staff are reminded of their obligations, with respect to data protection, in an INSET session at the start of the academic year.

5. Definitions

5.1 A 'security incident' means a suspected, attempted, successful, or imminent threat of unauthorised access, use, disclosure, breach, modification, or destruction of information; interference with information technology operations; or significant violation of responsible use policy. It includes any event that leads an employee or other worker to be concerned that a personal data breach has occurred, might have occurred or might be about to occur.

5.2 A 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. This includes breaches that are the result of both accidental and deliberate causes. It includes, but is not restricted to, the following:

- Loss or theft of confidential or sensitive data or equipment on which such data are stored (e.g. loss of laptop, iPad/tablet device, mobile device or paper records);
- Equipment theft or failure;
- Unauthorised use of, access to, or modification of, data or information systems;
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s);
- Unauthorised disclosure of sensitive/confidential data;
- Website defacement;
- Hacking attack;
- Unforeseen circumstances such as a fire or flood; leading to unavailability of systems processing personal data;
- Human error;
- Offences where information is obtained by deception;
- Sharing personal data without a data sharing agreement;
- Processing data by a processor without a legally binding contract in place.

6. Scope

6.1 This procedure applies in the event of a security incident or personal data breach.

6.2 For the purpose of this policy, data security breaches include both confirmed and suspected incidents.

7. Roles and Responsibilities

7.1 The PCO is responsible for

- Ensuring that all employees are trained in their responsibilities concerning security incidents and data breaches;
- Responding to all reported security incidents and data breaches;
- Performing an initial assessment to establish the severity of a security incident or personal data breach and for appointing a Lead Investigation Officer (LIO).

7.2 The LIO is responsible for investigating the security incident or personal data breach and taking the appropriate action.

7.3 The PCO is responsible for reviewing systems and procedures following a personal data breach and recommending corrective action.

7.4 **All employees** are responsible for ensuring that they report a security incident or personal data breach to the PCO immediately it is discovered or suspected.

7.5 Governors have the responsibility of ensuring that the policy is implemented and may request to see the annual records of data breaches that are recorded.

8. Reporting an incident

8.1 Any individual who accesses, uses or manages the School's information must report a security incident or personal data breach to the PCO immediately it is discovered or suspected by completing section 1 of the Security Incident /Breach Report Form (see Appendix 1) and sending the form to the PCO by emailing privacy@mhsg.manchester.sch.uk.

8.2 The employee must ask for an acknowledgement by email to ensure the notification has been received. If no acknowledgement is received within 8 hours it may mean that the PCO is unavailable and the employee should contact the Head Mistress.

9. Containment and recovery

9.1 The PCO will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

9.2 An initial assessment will be made by the PCO in liaison with other relevant staff to establish the severity of the breach and who will take the lead investigating the breach, as the LIO (this will depend on the nature of the breach; in some cases it could be the PCO). In cases involving personal data stored digitally the PCO will liaise with the Director of Digital Solutions.

9.3 The LIO will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

9.4 The LIO will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.

9.5 The LIO, in liaison with the any other relevant staff will determine the suitable course of action to be taken to ensure a resolution to the incident.

9.6 If the circumstances surrounding a security incident or personal data breach lead the PCO to believe that disciplinary action may be appropriate, the Head Mistress shall be informed immediately and the investigation shall be modified and conducted in accordance with the School's disciplinary procedures.

10. Investigation and risk assessment

10.1 An investigation will be undertaken by the LIO immediately and wherever possible, within 24 hours of the breach being discovered / reported.

10.2 The LIO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

10.3 The investigation will need to take into account the following:

- the type of data involved;
- the sensitivity of the data;
- the protections that are in place (e.g. encryptions);
- what has happened to the data (e.g. has it been lost or stolen;
- whether the data could be put to any illegal or inappropriate use;
- data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s);
- whether there are wider consequences to the breach.

11. Notification

11.1 The LIO and / or the PCO, in consultation with relevant colleagues will establish whether the Information Commissioner's Office (ICO) will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach. The LIO shall submit the breach notification by email and telephone call and request email confirmation of receipt of the notification. If the data breach notification to the ICO is not made within 72 hours, the Lead Investigation Officer shall submit it as soon as possible with a justification for the delay.

11.2 Every incident will be assessed on a case by case basis; however, the following will need to be considered:

- whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms;
- whether notification would assist the individual(s) affected (e.g. could they act on the information to mitigate risks?);
- whether notification would help prevent the unauthorised or unlawful use of personal data;
- whether there are any legal/contractual notification requirements;
- the dangers of over-notifying. Not every incident warrants notification and over-notification may cause disproportionate enquiries and work.

11.3 Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay. Notification will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact the School for further information or to ask questions on what has occurred.

11.4 The LIO and/or the PCO will consider notifying third parties such as the insurers, banks, credit card companies or police. 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.

11.5 The LIO and or the PCO will consider whether the Development and Marketing Director should be

informed to alert them to be ready to handle any incoming press enquiries or to prepare a press release.

11.6 A log will be kept of any personal data breach, regardless of whether notification was required.

11.7 If the LIO decides that the breach does not have to be reported to the ICO, as it is unlikely to adversely affect individuals' rights and freedoms, the justification for the decision will be documented.

12. Evaluation and response

12.1 Once the initial incident is contained, the PCO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

12.2 Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

12.3 The review will consider:

- where and how personal data is held and where and how it is stored;
- where the biggest risks lie including identifying potential gaps or weak points within existing security measures;
- whether methods of transmission are secure; sharing minimum amount of data necessary;
- staff awareness of procedures;

12.4 If deemed necessary, a report recommending any changes to systems, policies and procedures will be considered by the PCO and communicated with the Head Mistress.

13. Policy Review

13.1 This policy will be updated as part of the School's policy review cycle or as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation.

Policy reviewed and updated by the Head Mistress September 2024

Approved by the Governor Academic Development Committee October 2024

APPENDIX 1

Security Incident/Breach Report Form

Upon discovering or suspecting a security incident or data breach you must inform the PCO immediately. You must then complete section 1 of the form below and email it to the PCO at rfairgrieve@mhsg.manchester.sch.uk. You should ask for an acknowledgement by email to ensure it has been received.

Section 1: Notification of Data Breach	**To be completed by person reporting the breach**
Date and time incident was discovered:	
Date(s) and time(s) of incident(s) if different to above:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email and telephone number):	
Brief description of incident and details of information lost/stolen/inadvertently erased etc:	
Has any personal data been placed at risk? If so, provide details:	
Number of Data subjects affected (if known): ie number of persons whose personal data may have been placed at risk	
Brief description of any action taken at the time of discovery:	
For use by the PCO	
Received by:	
Date:	
Forwarded for action to: (Lead Investigation Officer)	
Date:	

Section 2: Assessment of Severity of data breach	**To be completed by the Lead Investigation Officer**
Details of any paper-based personal data lost or compromised in the breach.	
Details of the IT system, equipment, devices, records involved in the breach:	
Details of information loss	
What is the nature of the information lost?	
How much data has been lost? For example, if a laptop has been lost or stolen: how recently was the laptop backed up onto the central IT systems?	
Is the information unique? Will its loss have an adverse operational, financial, legal, liability or reputational consequences for the School?	
How many data subjects are affected? ie number of persons whose personal data may have been placed at risk	
Is the data bound by any security arrangements?	
What is the nature of the sensitivity of the data? Provide details of any types of information that fall into any of the following categories:	
High Risk personal data ➢ **Sensitive personal data** relating to a living, identifiable individual **a)** Racial or ethnic origin **b)** Physical or mental health or condition or sexual health **c)** Commission or alleged commission of any offence, or **d)** Proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings	
➢ Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports or visas	
➢ Personal data relating to children and vulnerable adults	
➢ Detailed profiles of individuals including about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed	

➢ Security information that would compromise the safety of individuals if disclosed	

Section 3: Action taken	**To be completed by the Lead Investigation Officer**
Report received by	
Date:	
Action Taken by responsible officer/s:	
Follow up action required/recommended	
Notification to ICO	Yes/No If yes, notified on: Details: If no, why not?
Notification to data subjects (persons whose personal data has been compromised in the breach)	Yes/No If yes, notified on: Details:
Notification to other external bodies	Yes/No If yes, notified on: Details: