Data Breach Procedure

Introduction

1. Spurgeon's College collects, holds, processes and shares large amounts of personal data and has a legal obligation to ensure that it is kept secure and appropriately protected.

2. In line with our Data Protection Policy, all staff have a duty to protect the personal data they possess from loss or unauthorised destruction, alteration, disclosure or access, whether due to human error or malicious intent.

3. In some circumstances, the College has a legal responsibility to report personal data breaches to the Information Commissioners Office (ICO) within 72 hours of the time the breach occurred.

Purpose

4. The purpose of this procedure is to ensure that:

   - personal data breaches are detected, reported, categorised and monitored consistently
   - incidents are assessed and responded to appropriately without undue delay
   - decisive action is taken to reduce the impact of a breach
   - improvements are implemented and communicated to prevent recurrence or future incidents
   - certain personal data breaches are reported to the Information Commissioner's Office (ICO) within 72 hours, where required.

5. This document sets out the procedure to be followed to ensure a consistent and effective approach in managing personal data security breaches across the College.

Scope

6. This procedure applies to all staff, students, partner organisations and staff, suppliers, contractors, consultants, representatives and agents that work for or process, access, use or manage personal data on behalf of the College.

7. This procedure relates to all personal and special category ('sensitive') information handled, stored, processed or shared by the College whether organised and stored in physical or IT- based record systems.

Definition

8. A data security breach is any loss of or unauthorised access to, College data, normally involving personal or confidential information.

9. A personal data breach means ***'a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.***

10. A personal data breach in the context of this procedure is an event or action that has affected the confidentiality, integrity or availability of personal data, either accidentally or deliberately, that results in its security being compromised, and has caused or has the potential to cause damage to the College and/or the individuals to whom the information relates to.

11. For the purpose of this procedure a data security breach includes both confirmed and suspected breaches.

12. A data breach incident includes but is not limited to:

- Devices containing personal data being lost or stolen (e.g. laptop, USB stick, iPad/tablet device or paper record)
- Access by an unauthorised third party (including hacking and viruses) or unlawful disclosure of personal data to a third party (e.g. deliberate leaking of information)
- Unauthorised publication of personal data on a website or social media site
- Deliberate or accidental action (or inaction) by a data controller or processor
- Sending personal data to an incorrect recipient
- Alteration of personal data without permission
- Loss of availability of personal data
- Data input error / human error
- Software malfunctions leading to personal data loss
- Damage or loss of personal data from fire, flood or other physical damage
- Non-secure disposal of hardware or paperwork containing personal data
- Inappropriate access/sharing allowing unauthorised use of, access to or modification of data or information systems
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it.

Reporting an incident

13. As soon as a data security breach has been detected or is suspected, any student, staff, contractor, partnership organisation, partner staff or individual that processes, accesses, uses or manages personal data on behalf of the

College is responsible for reporting the incident/breach immediately or within 24 hours to the Data Protection Officer (or their nominated deputy).

14. If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

15. A current 'Data Breach Report Form' should be completed as part of the reporting process. The report will include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, the nature of the information and how many individuals are involved.

16. Throughout the breach management process records should be kept of what action has been taken, when and by whom. A current 'Data Breach Activity Log' should be used for this purpose.

17. All records must be kept for 5 years in accordance with the College Records Retention schedule.

Containment and Recovery

18. The Data Protection Officer will investigate the breach in liaison with other appropriate staff.

19. They will determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

20. An initial assessment will be made to establish the severity of the breach, who will take the lead as designated Investigating Officer to investigate the breach (this will depend on the nature of the breach) and determine the suitable course of action to be taken to ensure a resolution to the incident.

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

22. Advice from experts across the College and with external third parties may be sought in resolving the incident promptly.

23. See *Appendix 1* for detailed guidance on steps to be taken.

Investigation and Assessing the Risks

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

25. The Investigating Officer will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how likely they are to happen and how serious or substantial they are.

26. The level of risk associated with a breach can vary depending on the type of data and its sensitivity. The investigation will need to consider the following:

    - What type of data is involved?

- What was the volume of data involved and the number of data subjects affected?
- Who are the individuals whose data has been breached?
- How sensitive is the data?
- Where data has been lost or stolen are there any protections in place such as encryption or backup copies?
- What has happened to the data? Has it been lost or stolen?
- What could the data tell a third party about the individual?
- Could the data be put to any illegal or inappropriate use?
- Could it be used for purposes which are harmful to the individuals to whom the data relates?
- Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider, such as loss of public confidence?
- Are there others who can advise on risks or actions? e.g. contact bank for advice on how they can help prevent bank details being used fraudulently.

27. See *Appendix 2* for guidance on assessing risks.

Notification of Breaches

28. The Investigating Officer in consultation with the Data Protection Officer and Director of Operations will determine who needs to be notified of the breach.

29. Every incident will be assessed on a case by case basis. Not every incident warrants notification and over notification may cause disproportionate enquiries and work e.g. notifying all students of an issue when only some are affected.

30. The following will need to be considered:

    - Are there any legal/contractual notification requirements?
    - Can notification help the individual? Could they take steps to act on the information to protect themselves?
    - Would notification help prevent the unauthorised or unlawful use of personal data?
    - Can notification help the College meet its obligations under the data protection principles?
    - Are a large number of people affected? Are there serious consequences?
    - Should the ICO be notified of the personal data breach?

31. The ICO must be notified where there is likely to be a risk to people's rights and freedoms. For example, may result in discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to a natural person.

32. The risk to people's rights and freedoms could be physical, material or non-material damage to a person such as loss of control over their personal data or limitation of their rights.

33. If the ICO should be notified, this must be done within 72 hours with details of:

- 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;
- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach;
- details of the security measures and procedures in place at the time the breach occurred;
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

34. If the College decides not to report the breach to the ICO it will need to be able to justify the decision and document it. **Failing to notify a breach when required to do so can result in a significant fine.**

35. If a breach is likely to result in a *high risk* to the rights and freedoms of individuals, those affected must be notified **without undue delay** describing:

- the nature of the personal data breach;
- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects including what action the individual(s) can take to protect themselves.

36. When deciding whether a data breach is high risk the following should be considered:

- Sensitivity of information
- Volume of information
- Likelihood of unauthorised use
- Impact on individual(s)

37. If the College decides not to notify the individuals affected, it will still need to notify the ICO unless it can demonstrate that the breach is unlikely to result in a risk to rights and freedoms.

38. The Investigating Officer and/or Data Protection Officer and Director of Operations must consider notifying third parties such as the police, insurers, professional bodies, bank or credit card companies who can help reduce the

risk of financial loss to individuals. 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.

39. In accordance with the College's Data Sharing Agreement, any actual or suspected personal data breach pertaining to students registered with the University of Manchester, must be notified in writing to the University within 24 hours.

40. The Investigating Officer and/or Data Protection Officer will consider whether a press release or public statement needs to be made and ensure staff are prepared to handle any resulting enquiries.

41. All personal data breaches and actions will be recorded by the Data Protection Officer regardless of whether or not they need to be reported to the ICO.

Evaluation and Response

42. Data protection breach management is a process of continual review. Once the initial incident is contained, the Data Protection Officer 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.

43. 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.

44. The review will consider:
    - Where and how personal data is held/ stored
    - Where the biggest risks lie and identify any further potential weak points within its existing security measures
    - Whether methods of transmission are secure; sharing minimum amount of data necessary
    - Staff awareness.

45. All recommendations will be assigned an owner and timescale for actions to be implemented.

Document control box			
Title	**Data Breach Procedure**		
Date approved	11 February 2019	Implementation date	Feb 2019
Next review date			
Version	2	Supersedes version	1
Approving body		Governors	
Quality Code consulted			
Member of staff responsible		Director of Operations	

Appendix 1: Containment and recovery checklist

	Step	Actions
1	Establish investigating officer/team.	May need to include responsible staff members, IT, Director of Department, Legal etc.
2	Ensure possibility of further data loss is removed or mitigated as far as possible.	Change passwords or access codes
		Isolate or close part of network
		Take down web pages
		Temporarily restrict access to systems/drives/filing systems
		Put in place any additional temporary security measures
3	Determine whether anything can be done to recover any lost data.	Physical recovery of lost data/equipment – conduct search
		Physical recovery of stolen data/equipment – inform police as appropriate
		Use back-ups to recover corrupted or lost electronic data.
		Recall incorrectly sent emails, or contact persons involved asking them to delete the email completely from their systems (including trash) and to confirm that this has been done.
		Retrieve paper document from any unintended recipients.
4	Ensure all key actions and decisions are logged and recorded on the Data Breach Activity Log.	Complete the log at each stage of the process to keep and evidence and audit trail of the breach and remedial action taken. This will help to demonstrate compliance to the ICO.

Appendix 2: Assessment of risks checklist

Please note that the potential effect on risk will depend on the individual circumstances of the breach and must be assessed on a case by case basis.

	Variable	Consideration	Potential effect on risk	Risk Rating if applicable *(No, low, medium,high)*
1.	What volume of personal data is involved?	Are there large amounts of data	The more data about an individual that is released, potentially the higher the risk.	
2.	How many individuals' personal data are affected?	Under 10 11-100 100-1000 1000+	Potentially increased risk as those affected increases.	
3.	What type of personal data is involved?	Is the information already accessible or in the public domain	If the information is in the public domain the risk may be lower.	
4.	How sensitive is the data?	Does it contain special category data such as ethnicity, sexuality etc.	The more sensitive the data the higher the probable risk.	
5.	What has happened to the data?	Lost/Stolen/Damaged Breach is internal or external	If data is stolen then the risk is higher than data that has been damaged. An internal breach may be less risk than an external.	
6.	Who are the individuals whose data has been compromised?	Staff, students, applicants, clients, suppliers	Data breach relating to staff may be less of a risk than that of students or applicants	
7.	If the data was lost or stolen were there any protections in place to prevent misuse?	For example encryption/passwords	Risk reduces with increased protection	
8.	What could the data tell as third party about the individual? Could it be misused?	The loss of apparently trivial information may help a fraudster build up a detailed picture of an individual.	The more 'useful' the data the higher the risk.	
9.	Is there actual/potential harm that could come to any individuals?*****	Are there risks to personal safety, emotional wellbeing, reputation, finances, identify theft, or a combination of these?	The more potential or actual harm the higher the potential risk	
10.	Are there wider consequences to consider?	Risk to public health or loss of confidence in the service provided	The more severe the consequences the higher the potential risk	
11.	Are there others who might advise on risks/courses of action?	Banks to cancel credit cards or actions to reduce risk of fraud from their end.	The more help to prevent misuse the lower the potential risk	

**the ICO must be notified if there is any risk; the individuals must be notified in there is a high risk.*