Data Security Breach Incident Management Policy

Review Date: May 2022
Review Committee: Personnel/Student Care and Discipline Committee
Final Approval: Full Governors

Context

The Core Values of the Academy which relate specifically to this policy state that we are working together to form relationships based on

- **Truth** - everyone is required to be honest and to communicate in a positive manner
- **Responsibility** - everyone is expected to understand the consequences of their actions
- **Justice** - everyone in entitled to be treated fairly and to promote the self-esteem of others

Such values contribute to our common purpose of "Striving for high quality education with a strong Christian ethos", and underpin, recording and data practices within the Academy.

Data Protection

Any personal data processed in the delivery of this policy will be processed in accordance with the school Data Protection policy.

Background

Data security breaches are increasingly common occurrences whether these are caused through human error or via malicious intent. As technology trends change and the creation of data and information grows, there are more emerging ways by which data can be breached. The academy needs to have in place a robust and systematic process for responding to any reported data security breach, to ensure it can act responsibly, protect its information assets and minimise the impact to any data subjects as far as practically a possible.

Aim

The aim of this policy is to standardise the academy response to any reported data breach incident, and ensure that such breaches are appropriately logged and managed in accordance with best practice guidelines.

By adopting a standardised consistent approach to all reported incidents, the academy will ensure that:

- incidents are reported in a timely manner and can be properly investigated
- incidents are handled by appropriately authorised and skilled personnel
- appropriate levels of academy management and directors (if applicable) are involved in response management
- incidents are recorded and documented
- the impact of the incidents are understood and action is taken to prevent further damage
- evidence is gathered, recorded and maintained in a form that will withstand internal and external scrutiny
- external bodies or data subjects are informed as required
- the incidents are dealt with in a timely manner and normal operations restored
- the incidents are reviewed to identify improvements in policies and procedures.

Definition

A data security breach is considered to be "any loss of, or unauthorised access to, academy data". Examples of data security breaches may include:

- Loss or theft of hard copy data or electronic equipment on which data is stored
- Unauthorised access to confidential or highly confidential data
- Equipment failure
- Human error for example incorrectly addressed emails
- Unforeseen circumstances such as a fire or flood
- Hacking/Phishing attack
- 'Blagging' offences where information is obtained by deceit

For the purposes of this policy data security breaches include both confirmed and suspected incidents.

Scope
This policy applies to all academy information, regardless of format, and is applicable to all staff, students, visitors, contractors and data processors acting on behalf of the academy.

Responsibilities
Information users
All information users are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.
Heads of Faculty/Department
Heads of Faculty or Departments are responsible for ensuring that staff in their area act in compliance with this policy and assist with investigations as required.
Data Protection Officer
The Data Protection Officer will be responsible for overseeing the management of the breach in accordance with the Data Breach Management Plan and advising the Head Teacher. Suitable delegation may be appropriate in some circumstances.
Head Teacher
The Head teacher will implement the Data Breach Management Plan, working with the Data Protection Officer and other individuals as necessary.

Data Classification
Data security breaches will vary in impact and risk depending on the content and the quantity of the data involved, therefore it is important that the academy is able to quickly identify the classification of the data and respond to all reported incidents in a timely and thorough manner.

All reported incidents will need to include the appropriate data classification in order for assessment of risk to be conducted. Data classification referred to in this policy means the following approved categories:
Public Data
Information intended for public use, or information which can be made public without any negative impact for the academy.
Internal Data:
Information regarding the day-to-day business and academic operations of the academy. Primarily for staff and student use, though some information may be useful to third parties who work with the academy.
Confidential Data:
Information of a more sensitive and or personal nature required for the business and academic operations of the academy, representing basic intellectual capital and knowledge. Access should be limited to only those people that need to know as part of their role within the academy.
Highly confidential Data:
Information that, if released, will cause significant damage to the individual or academy's business activities or reputation, or would lead to breach of the UK GDPR and the Data Protection Act 2018. Access to this information must be highly restricted.

Data Security Breach Reporting
Confirmed or suspected data security breaches should be reported promptly to the Data Protection Officer (DPOService@Schoolpeople.co.uk). The report should include full and accurate details of the incident including who is reporting the incident and what classification of data is involved. Where possible section 1 of the incident report form should be completed as part of the reporting process by the person initially reporting the incident. See **Appendix 1.**
Once a data breach has been reported the DPO will assess the severity of any personal data breach based on the number of data subjects involved, the data involved and the risks to the rights and freedoms of the data subject as a result of that breach All data security breaches will be centrally logged by the Data Protection Officer or delegated person to ensure appropriate oversight in the types and frequency of confirmed incidents for management and reporting purposes. The Data Protection Officer will be responsible for reporting appropriate breaches to the Information Commissioners Office (ICO).

Data Breach Management Plan
The management response to any reported data security breach will involve the following four elements. See **Appendix 2** for the checklist.

A. Containment and Recovery
B. Assessment of Risks
C. Consideration of Further Notification
D. Evaluation and Response

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. See **Appendix 3.**

Authority
Staff, students, contractors, consultants, visitors and guests who act in breach of this policy, or who do not act to implement it, may be subject to disciplinary procedures or other appropriate sanctions.

Review
The Personnel, Student Care and Discipline committee of the governing body will monitor the effectiveness of this policy and carry out regular reviews of all reported breaches.

References
Information Commissioner:
https://ico.org.uk/media/1562/guidance_on_data_security_breach_management.pdf

APPENDIX 1

Data Security Breach Form

Reference Number:

To be completed in all instances of an actual or suspected Personal Data Breach/Data Security Incident.

Please act promptly to report any data breaches. If you discover a data breach, please notify your line manager immediately. Complete section 1 of this form and email it to the Data Protection Officer (dposervice@schoolspeople.co.uk) and the Data Controller's Representative aharwood@bishopstopford.com

Section 1: Notification of Data Security Breach *To be completed by the line manager of the person reporting the incident.*	
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please provide details:	
Has any Special Category Data been placed at risk? If, so please provide details:	
Brief description of any containment action taken at the time of discovery, eg Email recall, computer shut down, etc	

For use by the Data Protection Officer			
Received by:	Dee Whitmore	Date:	
Forwarded by	Arthur Harwood	Email: aharwood@bishopstopford.com Telephone:	
Lead Investigating Officer appointed	Dee Whitmore	Email: DPOService@Schoolspeople.co.uk Telephone: 01773 851 078	

Section 2: Assessment of Severity *To be completed by the Lead Investigation Officer in consultation with the Head of area affected by the breach and if appropriate IT where applicable*	
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of hard copy data involved in the security breach	
Details of Information loss (*loss defined as not recoverable****)***	

How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the Company or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH RISK personal data Special categories personal data (as defined in the Data Protection Legislation) relating to a living, identifiable individual's a) racial or ethnic origin b) political opinions or religious beliefs c) trade union membership e) biometrics (where used for ID purposes) f) health g) sex life or sexual orientation	
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 and visas	
Personal information relating to children and vulnerable adults	
Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed	
Information about individual cases of investigations, discipline or sensitive negotiations which could adversely affect individuals.	

Security information that would compromise the safety of individuals if disclosed.	
Other	

Data Protection Officer and/or Lead Investigation Officer to consider whether it should be escalated to the Governing Body			
Referral decision taken by:		**Referred**	**YES/NO**
Section 3: Action Taken ***To be completed by Data Protection Officer and/or Lead Investigation Officer***			
Incident number		**Completed by**	
Was the incident reported to the Police?	**Yes / NO**	**Date reported**	
Follow up action required/recommended:			
For use of Data Protection Officer and/or Lead Officer:			
Notification to ICO	**YES / NO**	**Date Reported**	
Notification to Data Subjects	**YES / NO**	**Date Reported**	
Details of Notification.			

Notification to other stakeholders	**YES / NO**	**Date Reported**	
Details of Notification			
Evaluation & Response	**Date Reported completed**		

APPENDIX 2

Data Breach Checklists

A. Containment and Recovery
B. Assessment of Risks
C. Consideration of Further Notification
D. Evaluation and Response

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	Data Protection Officer and Head Teacher to ascertain the severity of the breach and determine if any personal data is involved.	**See Appendix 2**
2	Data Protection Officer and Head Teacher to identify Lead Responsible Officer for investigating breach and forward a copy of the data breach report	To oversee full investigation and produce report. Ensure lead has appropriate resources including sufficient time and authority. If personal data has been breached also contact Br-Data-Protection. In the event that the breach is severe, the academy Incident Management Team will be contacted to lead the initial response.
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.
5	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 Lead Responsible Officer or nominee to inform the police.	E.g. stolen property, fraudulent activity, offence under Computer Misuse Act.
5	Ensure all key actions and decisions are logged and recorded on the timeline.	

B	Assessment of 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, applicants, staff, customers, clients 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 fraudster build up a detailed picture of other people.
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	**Consideration of Further 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 academy a 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 (through the Director of Information).	Contact and liaise with the Director of Legal Services or the Governance and Information Compliance Team.
23	Consider the dangers of 'over notifying'.	Not every incident will warrant notification "and notifying a whole 2 million strong customer base of an issue affecting only 2,000 customers 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 us for further information or to ask questions about what has occurred (e.g. a contact name, helpline number or a web page).

25	Consult the ICO guidance on when and how to notify it about breaches.	Where there is little risk that individuals would suffer significant detriment, there is no need to report. There should be a presumption to report to the ICO where a large volume of personal data is concerned and there is a real risk of individuals suffering some harm. Cases must be considered on their own merits and there is no precise rule as to what constitutes a large volume of personal data. Guidance available from http://www.ico.gov.uk/for_organisations/data_protection / the_guide/principle_7.aspx
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 academy's 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 Information Management and Security Board.

APPENDIX 3

Report Form (Proforma) 2

Date	Time	Activity	Decision	Authority