EBOR ACADEMY TRUST

Policy Number

19a

Data Breach Management Policy

Approved By:	Ebor Academy Trust Board of Trustees
Approval Date:	November 2021
Review Period:	2 Years (subject to legislative/regulatory changes)
Review Date:	November 2023

Author:	Clare Walters Director of Risk, Governance & Compliance
Date Created/updated:	*October 2021*
Version Number:	*2*

Contents:

1. Introduction

1.1. Ebor Academy Trust holds, processes, and shares personal data, a valuable asset that needs to be suitably protected. Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security. Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance, and/or financial costs.

2. Purpose

2.1. Ebor Academy Trust is obliged under the Data Protection Act 2018 to have in place an institutional framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility. This Policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across the Trust.

2.2. Article 33 of the UK GDPR requires data controllers to report breaches of personal data to the Information Commissioner's Officer, and sometimes the affected data subject(s), within 72 hours of discovery if the incident is likely to result in a risk to the rights and freedoms of the data subject(s). Therefore it is vital that the Trust has a robust system in place to manage, contain, and report such incidents.

3. Scope

3.1. This Policy relates to all personal and special category data held or processed by Ebor Academy Trust in all forms including, but not limited to:

a) Hard copy or documents printed or written on paper;
b) Information or data stored electronically, including scanned images;
c) Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;
d) Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;
e) Information stored on portable computing devices including mobile phones, tablets, cameras and laptops;
f) Speech, voice recordings and verbal communications, including voicemail;
g) Published web content, for example intranet and internet;
h) Photographs and other digital images.

3.2. This Policy applies to all staff, unpaid, employed or contracted including Trustees, Governors and pupils. This includes temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of the Trust and its Schools. The objective of this Policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

4. Definition/Type of Breach

4.1. For the purpose of this Policy, data security breaches include both confirmed and suspected incidents. An incident in the context of this Policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately and has caused or has the potential to cause damage to the School's information assets and/or reputation.

4.2. An incident includes but is not restricted to, the following:

a) Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad/tablet device, or paper record)
b) Equipment theft or failure
c) Unauthorised use of, access to or modification of data or information systems
d) Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
e) Unauthorised disclosure of sensitive/confidential data
f) Website defacement
g) Hacking attack
h) Unforeseen circumstances such as a fire or flood
i) Human error
j) 'Blagging' offences where information is obtained by deceiving the organisation who hold it.

5. Reporting an Incident

5.1. Any individual who accesses, uses or manages the School information is responsible for reporting a data breach or information security incidents immediately to the Data Controller (school head teacher of trust CST function head) and the trust Data Protection officer (dpo@ebor.academy). If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

5.2. The report should be made using the report template in Appendix A to include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. These forms are available from the G Suite templates drive or via google form link by emailing the Trust DPO (dpo@ebor.academy)

5.3. All staff should be aware that any significant breach of the UK GDPR & Data Protection Act (when enforced) may result in the School's Disciplinary Procedures being instigated.

6. Containment of Recovery

6.1. The Data Controller (Headteacher/CST function head) 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. The Headteacher / function head will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause. The Headteacher/function head will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate. Advice from experts across the Trust may be sought in resolving the incident promptly. The Headteacher/function head will

determine the suitable course of action to be taken to ensure a resolution to the incident.

7. Investigation and Risk Assessment

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

7.2. The investigation will need to take into account the following:

a) The type of data involved
b) The protections are in place (e.g. encryptions)
c) What has happened to the data, has it been lost or stolen
d) Its sensitivity
e) Whether the data could be put to any illegal or inappropriate use
f) Who the individuals are, number of individuals and the potential effects on those data subject(s)
g) Whether there are wider consequences to the breach

7.3. The Trust DPO will assess the data protection risks and assign a severity rating according to the identified risks and mitigations. The severity ratings can be found in Appendix One of this document. Red incidents will be reported to the Audit and Risk Assurance Committee.

8. Notification

8.1. The Headteacher/CST function head and Data Protection Officer will determine who needs to be notified of the breach.

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

a) Whether there are any legal/contractual notification requirements;
b) Whether notification would assist the individual affected – could they act on the information to mitigate risk?
c) Whether notification would help prevent the unauthorised or unlawful use of personal data?
d) Would notification help the School meet its obligations under the seventh data protection principle;
e) If a large number of people are affected, or there are very serious consequences, whether the Information Commissioner's Office (ICO) should be notified within 72 hours of the reported breach. The ICO will only be notified if personal data is involved. Guidance on when and how to notify ICO is available from their website at: https://ico.org.uk/for-organisations/report-a-breach/
f) The dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work.

8.3. Notification to the individuals whose personal data has been affected by the incident 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.

8.4. The Headteacher/CST function head must consider notifying third parties such as the police, insurers, bank or credit card companies, and trade unions. 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. The Headteacher/function head will consider whether the Board of Trustees should be informed, if a press release is to be issued and to be ready to handle any incoming press enquiries. All actions must be recorded as part of the investigation by the Data Protection Officer.

9. Evaluation and Response

9.1. Once the initial incident is contained, the investigating 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. 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.

9.2. The review will consider:

a) Where and how personal data is held and where and how it is stored
b) Where the biggest risks lie, and will identify any further potential weak points within its existing measures
c) Whether methods of transmission are secure; sharing minimum amount of data necessary
d) Identifying weak points within existing security measures
e) Staff awareness
f) Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security
g) If deemed necessary recommend any changes to systems, policies and procedures

Data Breach Incident Reporting Form

Section 1: Notification of Data Security Breach	*To be completed by person reporting incident*	
Date of the incident:		
Approximate time of the incident:		
Data Processor involved (School Name / Central Service Team Function):		
Name of the person reporting the breach:		
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:		
Brief description of any immediate action taken at the time of discovery:		
Type of Breach	Personal Information Accessed by unauthorised third party	
	Personal Information sent to an incorrect recipient	
	IT equipment loss/theft	
	Accidental sharing of personal information by data controller	
	Deliberate sharing of personal information by data controller	
	Alteration of personal information without permission	
	Loss of availability of personal data	

Categories of Data Subjects affected:	
Number of Records involved	
Contact Details of the person reporting	

For Use by the Data Controller (Headteacher / Function Head) and Data Protection Officer		
Reviewed By DPO (Date)		
Details of IT systems , equipment and records involved in breach		
What is the nature of the information involved		
How much data has been lost?		
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the School or third parties?		
How many data subjects are affected		
Details of information loss:		
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		
Severity (See appendix 2 Breach Reporting Policy)	**White**	
	Green	
	Amber	
	Red (Reportable to the Audit & Risk Committee)	

Action taken by responsible officer/s:		
Was incident reported to Police?		
Reported to other internal stakeholders (details, dates):		
ICO Notified	**NO**	
	YES	
If yes, notification date:		
Details of notification to data subjects		
Notification to other external regulator / stakeholder		

Severity Ratings For Information Security Incidents Rating	Incident Threshold	Recommended Actions
WHITE **Information Security Event**	No breach of confidentiality, integrity, or availability has taken place but there is a failure of the implemented safeguards that could lead to a breach in the future. *Examples* A post-it note containing a user name and password to a School database is found attached to a keyboard. A key safe, containing keys to filing cabinets, has been found unlocked and unsupervised.	Logged on the trust register of incidents Responsible officer(s) spoken to by management and reminded of data protection responsibilities.
GREEN **Minimal Impact Incident**	The School's security measures have failed and have consequently resulted in a breach of confidentiality, integrity, or availability. Incident has been contained within the organisation (or trusted partner organisation). The information does not contain any special category data or any data that would be considered to be sensitive. The actual or potential detriment to individuals is virtually non-existent. *Examples* An email, containing details of a service user's address or contact details, is sent to an incorrect recipient within the School. A document containing the only record of pupil's contact details have been destroyed in error.	Responsible officer(s) spoken to by management and reminded of data protection responsibilities. If repeated offence management to consider HR action. Logged on the trust register of incidents Investigation to be conducted by Information Data Protection Officer

AMBER **Moderate Impact Incident**	The School's security measures have failed and have consequently resulted in a breach of confidentiality, integrity, or availability. The information has left school control. Confidential Data Not contained within Trust Breach involves personal data of more than 100 individuals Significant inconvenience will be experienced by individuals impacted Incident may not yet be contained Incident does not require immediate response Incident response may require notification to Trusts senior managers The information does not contain special category data or data that is considered to be sensitive but may contain data that should have been confidential to the School.	Notify: Data Protection Officer CEO SLT Responsible officer(s) asked to re-sit Data Protection e-learning. Management to consider HR action. Consider utilising key messages to remind all staff of certain data protection best practice. Investigation report to be conducted by Information Data Protection Officer

RED Serious Impact Incident	The School's security measures have failed and have consequently resulted in a breach of confidentiality, integrity, or availability. Highly Confidential/Confidential Data Personal data breach involves > 1000 individuals 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 beyond normal operating procedures The information has left school control. The information contains special category data or data that is considered to be sensitive in nature and/or affects a large number of individuals. The incident has or is likely to infringe on the rights and freedoms of an individual and has a likely potential to cause detriment (emotional, financial, or physical damage) to individuals. Examples A file, containing safeguarding and health data, is left unsupervised in a vehicle which is subsequently stolen and the data has been lost to persons unknown. A spreadsheet containing the SEN information for all the School's pupils has been mistakenly sent to a member of the public.	Logged on Trust Breach register Notify: Data Protection Officer CEO SLT Chair of Trustees Board of Trustees Legal Services Consider forming an incident strategy conference Consider reporting to the Information Commissioner's Office Consider informing affected individual(s) Consider informing the police or other law enforcement agencies. Where appropriate the Data Protection Officer to conduct incident investigation with assistance (where and if required) from internal audit and counter fraud colleagues. Management to consider (potentially immediate) HR action.