EBOR ACADEMY TRUST

Policy Number

19A

Statutory
General Data Protection Regulation (GDPR) Data Breach Management Policy

Signed: ______________________________

Dated: May 2018

Review Period: Annually (By DPO)

Review Date: May 2019

Last updated: May 2018

1. 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. Ebor Academy Trust needs to have in place a robust and systematic process for responding to any reported data security breach, to ensure it can act responsibly and protect its information assets as far as possible.

2. Aim

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

By adopting a standardised consistent approach to all reported incidents, it aims to ensure that:

- incidents are reported instantly so they can be properly investigated
- incidents are handled by appropriately authorised and skilled personnel
- appropriate levels of Trust management are involved in responding to the breach
- 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 within the ICO recommended time frames (72 hours) so normal operations can be restored
- the incidents are reviewed to identify improvements in policies and procedures

3. Definition

A data security breach is considered to be "any loss of, or unauthorised access to, Trusts' data". Examples of data security breaches may include but are not limited to:

- Loss or theft of data or equipment on which data is stored
- Unauthorised access to confidential Trust Data
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceit

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

4. Scope

This policy applies to all Ebor Academy Trust information, regardless of format, and is applicable to all staff, students, visitors, contractors and data processors acting within or on behalf of the Trust. Staff should be aware of the policy as part of the induction process.

5. Responsibilities

5.1 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.

5.2 SLT
SLT are responsible for ensuring that staff are act in compliance with this policy and assist with investigations as required.

5.3 Data Protection Officer
The Data Protection Officer (DPO) will be responsible for overseeing management of the breach in accordance with the Data Breach Management Plan. Suitable delegation may be appropriate in some circumstances.

5.4 Contact Details
The Ebor Academy Trust DPO can be contacted by phone on 01904 553404 or email: dpo@ebor.academy.

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 Trust is able to quickly identify the classification of the data and respond to all reported incidents in a thorough manner, within the time frame given by the ICO.

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 Trust Data Categories:

6.1 Public Data:
Information intended for public use, or information which can be made public without any negative impact for the Trust.

6.2 Internal Data:
Information regarding the day-to-day business and academic operations of the Trust. Primarily for staff and student use, though some information may be useful to third parties who work with the Trust.

6.3 Confidential Data:
Information of a more sensitive nature for the business and academic operations of the Trust. Access should be limited to only those people that need to know as part of their role within the Trust.

6.4 Highly confidential Data:
Information that, if released, will cause significant damage to the Trust's business activities or reputation, or would lead to breach of the Data Protection Act. Access to this information should be highly restricted.

6. Data Security Breach Reporting

Confirmed or suspected data security breaches should be reported immediately to the Data Protection Officer by phone on 01904 553404 or email: dpo@ebor.academy.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 the incident report form should be completed as part of the reporting process. See Appendix 1. Upon request from the DPO, reporting individuals may be asked for additional information to support an investigation. Once a data breach has been reported, an initial assessment will be made to establish the severity of the breach. See Appendix 2.

All data security breaches will be centrally logged and monitored by the DPO.

7. Data Breach Management Plan

The management response to any reported data security breach will involve the following four elements. See Appendix 3 for suggested 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 4.

8. 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.

9. Review

The Ebor Academy Trustees will monitor the effectiveness of this policy and carry out regular reviews of all reported breaches.

Appendix 1: Incident Report Form

Time and Date breach was identified	
Description of the Data Breach	
Who is reporting the breach: Name/Post/School	
Contact details: Telephone/Email	
Classification of data breached (in accordance with Trusts Security Policy) i. Public Data ii. Internal Data iii. Confidential Data iv. Highly confidential Data	
Volume of data involved	
Confirmed or suspected breach?	
Is the breach contained or ongoing?	
If ongoing what actions are being taken to recover the data	
Who has been informed of the breach	
Any other relevant information	

Email form to the DPO and advise that a Data Security Breach report form is being sent.

Received by:	
Date/Time:	

Appendix 2: Evaluation of Incident Severity

The severity of the incident will be assessed by the DPO. Assessment would be made based upon the following criteria:

High Criticality: Major Incident Contact:	**Contact:**
● 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	DPO Other relevant contacts ● CEO ● SLT ● Chair of Trustees ● Board of Trustees ● Legal Services
Moderate Criticality: Serious Incident Contact:	**Contact:**
● 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	DPO Other relevant contacts: ● CEO ● SLT ● Chair of Trustees ● Board of Trustees ● Legal Services
Low Criticality: Minor Incident Contact:	**Contact:**
● Internal or Confidential Data ● Small number of individuals involved ● Risk to Trust low ● Inconvenience may be suffered by individuals impacted ● Loss of data is contained/encrypted ● Incident can be responded to during working hours Example: Email sent to wrong recipient ● Loss of encrypted mobile device	DPO Other relevant contacts: ● SLT ● CEO

Appendix 3: Data Breach Checklists

Step	Action	Notes
A	**Containment and Recovery**	**To contain any breach, to limit further damage as far as possible and to seek recovery any lost data.**
1	SLT to ascertain the severity of the breach and determine if any personal data is involved. Contact DPO.	**See Appendix 2**
2	SLT to investigate and forward a copy of the data breach report.	To oversee full investigation and produce report. Ensure assigned person 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, DPO 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.	

B	**Assessment of Risks**	**To identify and assess the ongoing risks that may be associated with the breach.**
7	What type and volume of data is involved?	Data Classification/volume of individual data etc
8	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).
9	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.
10	If the data was lost/stolen, were there any protections in place to prevent access/misuse?	E.g. encryption of data/device.
11	If the data was damaged/corrupted /lost, were there protections in place to mitigate the impact of the loss?	E.g. backup tapes/copies
12	How many individuals' personal data are affected by breach?	
13	Who are the individuals whose data has been compromised?	Students, applicants, staff, customers, clients or suppliers?
14	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.
15	Is there actual/potential harm that could come to any individuals?	E.g. are there risks to: physical safety; emotional wellbeing; reputation; finances; identity (theft/fraud from release of non-public identifiers); or a combination of these and other private aspects of their life?
16	Are there wider consequences to consider?	E.g. a risk to public health or loss of public confidence in an important service we provide?
17	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.**
18	Are there any legal, contractual or regulatory requirements to notify?	E.g.: terms of funding; contractual obligations
19	Can notification help the Trust meet its security obligations.	E.g. prevent any unauthorised access, use or damage to the information or loss of it.
20	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)?
21	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 DPO.
22	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".
23	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).
24	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
25	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 Trusts response to the breach.**
26	Establish where any present or future risks lie.	
27	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
28	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.
29	Consider and identify any weak points in levels of security awareness/training.	Fill any gaps through training or tailored advice.
30	Report on findings and implement recommendations.	Report to Information Management and Security Board.

Appendix 4: Timeline of Incident Management

Date	Time	Activity	Decision	Authority