Appendix 1

The Eliot Bank and Gordonbrock Schools Federation

Data Breach Process

Overview

Any school that process personal data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data. Many organisations take the view that one of those measures might be the adoption of a policy on dealing with a data security breach.

This guidance sets some of the things a school needs to consider in the event of a security breach. It is not intended as a comprehensive guide as all breaches are different, however it should assist schools in deciding on an appropriate course of action if a beach occurs.

This guidance is applicable to all aspects of the school's information, whether held in paper or electronic format.

What the guidance covers

This document describes the standard process for handling data/information security breaches involving The Eliot Bank and Gordonbrock Schools Federation data.

This guidance covers the procedures for identifying, reporting and responding to a data breach/security incident.

(See below the Breach Report Form for Schools - Template to log a breach)

What is a data breach?

Personal Identifiable Information is exposed, shared or unauthorised or inappropriate processing that results in its data / security being compromised. The extent of damage caused will be determined by the volume, sensitivity and exposure of the information.

Examples of common breaches are listed below:

Example of typical breaches	Breach examples, but not limited to

Human Error	• Unauthorised disclosures • Inappropriate sharing • Data Input errors • Non-secure disposal of hardware or paperwork • Loss in transit/post • Failed to follow a policy
Technical	• Data Corruption • Malware Corrupt • Code Hacking • Inappropriate access controls allowing unauthorised use
Physical	• Loss in transit/post • Unescorted visitors in secure areas • Break-ins to sites • Thefts from secure sites • Theft from unsecured vehicles/premises

A data security breach can happen for a number of reasons:

• Loss or theft of data or equipment on which data is stored
• Inappropriate access controls allowing unauthorised use
• Equipment failure
• Human error
• Unforeseen circumstances such as a fire or flood
• Hacking attack
• 'Blagging' offences where information is obtained by deceiving the school who holds it

However the breach has occurred, there are four important elements to any breach management plan:

1. Containment and recovery
2. Assessment of ongoing risk
3. Notification of breach
4. Evaluation and response

1. Containment and recovery

Data security breaches will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation. This may involve input from specialists across the school such as IT, HR, legal and your data protection advisers.

Consider the following:

- Decide on who should take the lead on investigating the breach and ensure they have the appropriate resources.

- Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. This could be isolating or closing a compromised section of the network, finding a lost piece of equipment or simply changing the access codes at the front door.

- Do everything that is in your power to recover any losses and limit the damage the breach can cause. As well as the physical recovery of equipment/documentation, this could involve the use of back up tapes to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.

- Where appropriate, inform the police.

2. Assessing the risks

Some data security breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. An example might be where a laptop is irreparably damaged but its files were backed up and can be recovered, albeit at some cost to the business. While these types of incidents can still have significant consequences the risks are very different from those posed by, for example, the theft of a customer database, the data on which may be used to commit identity fraud. Before deciding on what steps are necessary further to immediate containment, assess the risks which may be associated with the breach. Perhaps most important is an assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen.

The following points steps should be followed;

- What type of data is involved?

- How sensitive is it? Remember that some data is sensitive because of its very personal nature (health records) while other data types are sensitive because of what might happen if it is misused (students' grades)

- If data has been lost or stolen, are there any protections in place such as encryption?

- What has happened to the data? 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

- Regardless of what has happened to the data, what could the data tell a third party about the individual? 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

- How many individuals' personal data are affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment

- Who are the individuals whose data has been breached? Whether they are staff, students, parents, clients or suppliers, for example, will to some extent determine the level of risk posed by the breach and, therefore, your actions in attempting to mitigate those risks

- What harm can come to those individuals? 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 a risk to public health or loss of public confidence in the image of your school?

- If individuals' bank details for services they pay in regards to their children (schools meals, trips, etc.) have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.

3. Notification of breaches

Informing people and organisations that you have experienced a data security breach can be an important element in your breach policy and management.

However, informing people about a breach is not an end in itself. Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves, or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.

Checking process:

- Are there any legal or contractual requirements? Schools have an obligation to notify the Information Commissioner in certain circumstances, in other areas sector specific rules may lead you towards issuing a notification.

- Obtain advice and guidance from your Data Protection Officer in regards to a breach of personal/personal sensitive information.

- Can notification help you meet your security obligations with regard to the seventh data protection principle?

- Can notification help the individual? Bearing in mind the potential effects of the breach, could individuals act on the information you provide to mitigate risks, for example for staff to notify their bank of any data loss?

- If a large number of people are affected, or there are very serious consequences, you should consider whether you need to inform the Information Commissioners Office (ICO), this will depend on the severity of the breach/security incident..

- Consider how notification can be made appropriate for particular groups of individuals, for example, if you are notifying children or vulnerable adults.

- Have you considered the dangers of 'over notifying'. Not every incident will warrant notification and notifying 800 parents based on an issue affecting only 50 children may well cause disproportionate enquiries and work.

- You also need to consider who to notify, what you are going to tell them and how you are going to communicate the message. This will depend to a large extent on the nature of the breach but the following points may be relevant to your decision:

    i. Make sure you notify the appropriate regulatory body. A sector specific regulator may require you to notify them of any type of breach but there is a breach notification duty to notify the ICO – not all breaches will have to be notified to the ICO, but all where the individual is likely to suffer some form of damage (i.e. confidentiality breach, identity theft) Failure to report a breach within 72 hours when required to do so could result in a fine, as well as a fine for the breach itself.

ii. 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.

iii. Your notification should at the very least include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to respond to the risks posed by the breach.

iv. When notifying individuals give specific and clear advice on the steps they can take to protect themselves and also what you are willing to do to help them.

v. Provide the contact details for the Data Protection Officer to the ICO to ask for further information or to ask questions about what has occurred.

When notifying the ICO you should also include details of the security measures in place such as encryption and, where appropriate, details of the security procedures you had in place at the time the breach occurred.

(See below the ICO Data Protection Breach Notification Form)

You should also inform the ICO if the media are aware of the breach so that they can manage any increase in enquiries from the public. If there is a need to inform the media, it is useful to inform them whether you have contacted the ICO and what action is being taken. The ICO will not normally tell the media or other third parties about a breach notified to them, but they may advise you to do so.

The ICO has produced guidance for organisations on the information we expect to receive as part of a breach notification and on what organisations can expect from them on receipt of their notification. This guidance is available on the ICO website:

https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/

Comment [MB1]: Check for new address when available

You might also need to consider notifying third parties such as the police, insurers, professional bodies, bank or credit card companies who can assist in reducing the risk of financial loss to individuals, and trade unions.

4. Evaluation, response and action planning to prevent future incidents

It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of your response to it. Clearly, if the breach was caused, even in part, by systemic and ongoing problems, then simply containing the breach and continuing 'business as usual' is not acceptable; similarly, if your response was hampered by inadequate policies or a lack of a clear allocation of responsibility then it is important to review and update these policies and lines responsibility in the light of experience.

You may find that existing procedures could lead to another breach and you will need to identify where improvements can be made.

The following points will assist you:

- Make sure you know what personal data is held and where and how it is stored. Dealing with a data security breach is much easier if you know which data is involved.
- Establish where the biggest risks lie. For example, how much sensitive personal data do you hold? Is this data store in one location?

- Risks will arise when sharing with or disclosing to others. Do you have sharing agreements in place? You should make sure not only that the method of transmission is secure but also that you only share or disclose the minimum amount of data necessary. By doing this, even if a breach occurs, the risks are reduced.

- Identify weak points in your existing security measures such as the use of portable storage devices or access to public networks.

- Monitor staff awareness of security issues and look to fill any gaps through the tailored advice and training the school receives as part of the Information & Data Protection Service Level Agreement with Lewisham Council.

- Consider discussions such as 'what if' scenarios – this would highlight risks and weaknesses as well as giving staff at different levels the opportunity to suggest solutions.

- If your school already has a Business Continuity Plan for dealing with serious incidents, consider implementing a similar plan for data security breaches.

- It is recommended that at the very least, you identify an individual/s responsible for reacting to reported breaches of security.

5. Internal reporting

Staff should report any known or suspected data breach or security incident to the Data Protection Officer, Head Teacher or Deputy Head immediately. Senior School Staff can contact the Data Protection Officer for advice and guidance with any breach of personal / special categories of data.

Depending on the seriousness of the data breach, the ICO may need to be notified, as per point 3 above. This will be decided once the initial risk assessment has been completed by The Eliot Bank and Gordonbrock Schools Federation senior management.

(See below Breach Report Form for Schools)

As part of the containment and recovery process the school must:

- Do everything in your power to recover any losses and limit the damage the breach can cause

- Carry out the risk assessment and advise your Head Teacher or Deputy Head of the next steps. The risk assessment will be carried out in accordance with guidance issued by the ICO.

- The Federation Business Manager / the SAO or a member of their team will (if needed) input procedures to mitigate the risk of any further information loss

- Record all correspondence for a data breach (see the School's Breach Report template)

- If appropriate, inform the police

The data protection adviser is available to provide advice and guidance to the school as and when required from 9am-5pm Monday to Friday, by phone on **020 8314 8183** or **07825762328** or e-mail Schoolsdpa@lewisham.gov.uk

6. Breach Report & Breach Notification forms

Please find attached the Breach Report Form for Schools – template (to log and investigate a breach) and the ICO Data Protection Breach Notificatuion.


Breach Report Form for Schools- templat


ICO Data Protection Breach Notification

7. What happens if this policy is breached?

Failure to adhere to this policy, could lead to a breach of the data protection act and, ultimately, to disciplinary action.

8. Review

This policy is part of our data protection policy, which will be reviewed annually or sooner, if changes have to be made.

9. Policy Authorisation

Name/Role	Date	Version
Data Protection Adviser for Schools	2016	V 1
Gemma Varela & Samuel Akeredolu Data Protection Advisers for Council & Schools	13/03/2017	V 2
Brendan Myles Data Protection Officer for Lewisham Council & Schools	19/03/2018	V 3