DATA BREACH
MANAGEMENT POLICY

Prepared: Sept 2016
Reviewed: May 2018
Approved by: Signed
Governing Body: LUCY PINDAR-BOOTH

Author: Lisa Hughes
Next Review: June 2020
Date: 12/06/2018
The Data Protection Act 1998 (DPA) is based around eight principles of ‘good information handling’. These give people specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it.

Overview
This policy sets out some of the things that the school will consider in the event of a security breach in order that an appropriate course of action is taken. As Longford Park School processes personal data, the school must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data.

Definition
A personal data breach means "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provisions of a public electronic communications service."

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
• Lack of awareness by staff on what information can and cannot be disclosed.
• ‘Blagging’ offences where information is obtained by deceiving the organisation who holds it

Action
When appropriate, we will report the data breach to the ICO within 72 hours. Our procedures are based on guidance on personal data breaches produced by the ICO.

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

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 such as IT, HR and legal and in some cases contact with external stakeholders.

Should a data breach occur at Longford Park School, the staff member or data processor must immediately notify the DPO at the school. The DPO will alert the Headteacher and the chair of governors.

The DPO will:
• Take the lead on investigating the breach, ensuring that appropriate resources are available.
• Decide whether personal data has been accidentally or unlawfully –
  o Lost
  o Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people.

- 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 information or simply removing access rights to a key fob.
- Establish whether there is anything that can be done to recover any losses and limit the damage the breach can cause. As well as the physical recovery of equipment, this could involve the use of backup tapes to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.
- Where appropriate, the DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example the police, insurers, banks or credit card companies.
- Consider notifying the data subject directly affected by the inaccurate disclosure of information concerning them.
- Depending on the severity and/or number of people affected by the data incident, consider informing the ICO.

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. Before deciding on what steps are necessary, the DPO will assess the risks which may be associated with the breach. The DPO will carry out an assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen. To do this, the following points are considered:

- What type of data is involved?
- How sensitive is it?
- If data has been lost or stolen, are there any protections in place?
- What has happened to the data? If data has been stolen, could it be used for purposes which are harmful to the individuals to whom the data relate?
- Regardless of what has happened to the data, what could the data tell a third party about the individual?
- How many individuals’ personal data are affected by the breach?
- Who are the individuals whose data has been breached?
- 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 an important service you provide?

The DPO will assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

3. Notification of breaches

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. When deciding whether a breach requires informing people or organisations, the DPO will consider the following:

- Are there any legal or contractual requirements?
- Can notification help meet the school’s security obligations whereby appropriate technical and organisational measures should be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data?
- 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 by cancelling a credit card or changing a password?
- If a large number of people are affected, or there are very serious consequences, the ICO will be informed.
- How can notification be made appropriate for particular groups of individuals, for example, if you are notifying children or vulnerable adults.

The DPO in conjunction with the Headteacher will consider who to notify, what they will be told and how the message will be communicated. This will depend to a large extent on the nature of the breach but the following points will be considered when making decisions:

- If a data breach occurs, the DPO will inform the Headteacher and Chair or Governors.
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people’s rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
  - Loss of control over their data
  - Discrimination
  - Identify theft or fraud
  - Financial loss
  - Unauthorised reversal of pseudonymisation (for example, key-coding)
  - Damage to reputation
  - Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s) concerned

If it’s likely that there will be a risk to people’s rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the schools electronic folder system.
- Contact will be made with the Information Governance Officer at Trafford Council, depending on the level of the breach to assist the school in its decision to report the incident to the ICO.
Where the ICO must be notified, the DPO will do this via the "report a breach" page of the ICO website within 72 hours. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
  - The categories and approximate number of individuals concerned
  - The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

Data breaches will be recorded in the data breach log (See Appendix 1). regardless of whether it it is reported to the ICO. This record includes:

- Details of what the school has already done to respond to the risks posed by the breach
- Facts and cause
- Effects
- Action taken to contain it and ensure it doesn’t happen again (such as establishing more robust processes or providing further training for individuals).

Records of all breaches will be stored on the schools electronic folder system.

When notifying data subjects, specific and clear advice will be given on the steps they can take to protect themselves and also what the school can do to help them.

If the media become aware of the breach, the ICO will also be notified so that they can support the school in managing enquiries.

4. Evaluation and response

It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of the school’s response to it. Following any breach, the DPO and the headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible. In order to identify where improvements to data protection procedures can be made. The DPO will:

- Review what personal data is held and where and how it is stored.
- Establish where the biggest risks lie and ensure that appropriate measures are in place to minimise the risk of further security breaches.
- Ensure that not only is the method of transmission secure but also that the school only shares or discloses the minimum amount of data necessary. By doing this, even if a breach occurs, the risks are reduced.
- Identify weak points in the 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 training or tailored advice.
- Ensure staff who process personal and sensitive data have been trained appropriately in information security.
Any data security breaches will be recorded in the data security breach log (Appendix 1). The Chair of Governors will be informed of all breaches and the log will be reported to Governors of the Finance & Personnel Committee.

**Actions to minimise the impact of data breaches**
We will take the actions set out in Appendix 2 to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

**Relationship with existing policies**
This policy has been drawn up within the context of:
- Freedom of Information Policy
- Information Security Policy
- Records Management Policy
- Data Protection Policy
- and with other legislation or regulations (including audit, equal opportunities and ethics) affecting the school
Appendix 1 – Personal Data Security Breach Log

Organisation: ______________________ Date: ________________

<table>
<thead>
<tr>
<th>No.</th>
<th>Your Ref</th>
<th>Date of Breach</th>
<th>No People affected</th>
<th>Nature of breach (Choose most relevant)</th>
<th>Description of breach</th>
<th>How you became aware of breach</th>
<th>Description of data</th>
<th>Consequences of breach</th>
<th>All individuals informed?</th>
<th>Remedial action</th>
<th>Other Regulators informed</th>
<th>When did you first notify the ICO of the breach?</th>
<th>Signed by COG &amp; HT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


Appendix 2

Examples of what would be considered a breach and our response -

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the DPO will see support from the school IT support consultant.
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

Personal information disclosed on the school website

- Once report is received that sensitive data has been published the site administrator will be instructed to remove immediately.
- The DPO will report to those individuals or groups affected.
- The DPO will complete an investigation into how the breach happened and will ensure preventative measures are in place to avoid repeated breach.

Breaches made at governor meetings

For example - Non-anonymised pupil exam results or staff pay information being shared

- The DPO will contact all parties that are likely to have been recipients of the disclosure as soon as breach is reported.
- The DPO will receive written responses for all concerned confirming that the data will not be shared, published, saved or replicated in any way.

A school laptop containing non-encrypted sensitive personal data being stolen or hacked

- The DPO will contact the police immediately and receive a crime reference number.
- The DPO will liaise with the school IT consultant as equipment may be traced by GPS or further security activated.
- The DPO will investigate what potential data has been lost and who is affected.

The school’s cashless payment provider being hacked and parents’ financial details stolen

- The DPO will seek information from the provider and determine if reassurances can be made towards future security of information.
- The DPO will work with the provider in contacting all those affected by the breach.