Data Breach Policy

Ratified by Governors: November 2018

CONTENTS:

1.0 INTRODUCTION

1.1 The Data Protection Act 2018 (DPA) is based around six principles of 'good information handling'. These give people specific rights in relation to their personal information and place certain obligations on organisations that are responsible for processing it. An overview of the main provisions of DPA can be found in The Guide to Data Protection: https://ico.org.uk/for-organisations/guide-to-data-protection

1.2 Occasionally things will go wrong and mistakes will be made. It is vital that as a School, we can identify, evaluate contain data breaches as soon as they occur.

1.3 Identifying data breaches quickly and effectively to limit any impact on our students is critical. Equally we need to understand where there are areas of weakness within our operating processes and continuously improve to reduce the risk of significant control failures leading to data breaches.

1.4 This policy meets the guidance provided by the ICO on data security breach management.

2.0 AIMS AND OBJECTIVES

This policy sets out:

- Policy statement on data breaches
- Definitions
- Reporting responsibilities

2.1. This policy aims to ensure that adequate controls are in place so that:

- Data breaches are identified, and action is taken quickly. Actions should be proportionate, consistent and transparent
- An assessment is completed to ensure that any major data breaches are reported to the Senior Management Team (SMT), Data Protection Officer (DPO) / Education Authority and the ICO appropriately
- All data breaches and near misses are recorded and regularly reported
- Lessons are learnt to ensure similar mistakes are not repeated and appropriate control mechanisms are put in place.

3.0 POLICY STATEMENT

3.1 This policy is in place to raise awareness of data breach cases. To ensure that all staff can identify a case and understand the steps required for dealing with them.

3.2 This policy identifies inherent risk of a data breach and/or near-miss, which will ensure that appropriate Senior Management and DPO are informed, able to manage actions relating to any real or potential serious data breach and be in a position to report to the ICO and affected individuals as appropriate.

4.0 DEFINITIONS

What is a data breach?

4.1 According to the ICO, organisations which process personal data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data.

4.2 A data breach is “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”.

4.3 A personal data breach may mean that someone outside the school gets unauthorised access to personal and/or special category (sensitive) data. But a personal data breach can also occur if there is unauthorised access within the school for example an employee accidentally or deliberately alters or deletes personal data.

4.4 A data security breach can happen for many 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
- Offences where information is obtained by deceiving the organisation who holds it.

4.5 Human error is the most common cause of data breaches. This can happen for many reasons:

- Theft or loss of paperwork
- Data posted to incorrect recipient
- Data sent by email to incorrect recipient
- Failure to redact personal/sensitive data.

4.6 A near miss is an event that does not result in a data breach, but which had the potential to do so. Examples of such events might include data that was misplaced but found quickly internally or data that was sent out but was identified and returned.

4.7 The School is committed to identifying weaknesses in our operational procedures. We will record all near misses, in order to understand patterns, learn lessons and implement improvements.

5.0 TRAINING

5.1 Training and guidance will be provided to all staff on data protection regulations.
5.2 Training will be provided to all new employees including temporary and contracted staff.

6.0 IDENTIFICATION

6.1 Data breaches or near misses may be identified as part of everyday business. They may be identified by the reception at the first point of contact; by a parent or pupil making us aware; by a third party like the local authority making us aware or via individual meetings.
6.2 Where a data breach is identified the Principal or designated deputy or Chair of BoG will inform the Data Protection Officer / Education Authority immediately. The individual concerned (with support from the Data Protection Officer) will investigate the to determine the next step.
6.3 The controls in place will be reviewed or consideration given to introducing them. It will be considered if this was an exceptional case that could not have reasonably been avoided, or does action need to be taken to avoid a recurrence.
6.4 Dependent on the level of risk identified, the DPO and School will take additional advice from the ICO.
6.5 All incidents will be reported to the Data Protection Officer / Education Authority.
6.6 With support from the DPO, the School will take appropriate steps to ascertain full details of the breach, determine whether the breach is still occurring, recover any losses and limit the damage.

Steps might include:

- Attempting to recover any lost equipment or personal information.
- Contact with C2k if appropriate if an IT based breach and on advice from EA.
- Contact with Office Staff and Communications Officers within the Education Authority on seek advice from EA in the case of a potential enquiry.
- If an inappropriate enquiry is received staff should attempt to obtain the enquirer's name/contact details and confirm that they will ring the enquirer back.
- The risk owner organising, with the approval of the Senior Management Team, for a school-wide email to be sent.
- If bank details have been lost / stolen consider contacting banks directly for advice on preventing fraudulent use.
- If the data breach includes any entry codes or passwords then these codes must be changed immediately, and C2K and members of staff informed.

7.0 INVESTIGATION

7.1 If a data breach is identified then a formal investigation will be commenced by the Principal and / or Designated Governor, who will determine the seriousness of the breach and the risks arising from it. Specifically, this will identify:

- Whose information was involved in the breach
- What went wrong
- The potential effect on the data subject(s)
- What immediate steps are required to remedy the situation
- What lessons have been learnt to avoid a repeat incident.

7.2 The investigation and subsequent report will consider:

- The type of information lost
- Its sensitivity
- How many individuals are affected by the breach?
- What protections are in place (e.g. encryption)?
- What happened to the information?
- Whether the information could be put to any illegal or inappropriate use
- What could the information tell a third party about the individual?
- How many people are affected?
- What types of people have been affected (the students, parents, staff etc)?
- Whether those affected have any special needs/vulnerabilities.

NOTE*: Actions to contain and recover data as well as mitigate any risk should be taken immediately. The investigation is to ensure that the case is being managed and any improvement actions agreed are implemented. The investigation should be proportionate to the breach identified and risk of harm.*

7.3 The initial investigation should be completed urgently and wherever possible within 24 hours of the breach being discovered / reported. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved

7.4 However, some level of investigation might be required to carry out the Risk Assessment and determine the most appropriate route of escalation. If, once identified, risk of a data breach is contained and does not pose immediate further threat to the school and/or students, timeframes for official escalation/notification can be extended to allow for a more thorough investigation. Extensions must be agreed at each stage and noted in the report.

7.5 As an investigation proceeds the risk may change and the reporting requirements should be amended in line with the change in risk. For example, a case identified as a significant risk initially may increase to a major risk and therefore should be escalated to the ICO

7.6 Advice, input and support can be sought from your Data Protection Officer as required.

8.0 INFORMING AFFECTED INDIVIDUALS

8.1 The ICO requires us to inform those affected where there is a significant breach of personal and sensitive data and the risk of harm to those individuals is high.
8.2 Clearly if there was a high risk of further harm the school would have an obligation to disclose the breach to each individual affected. However, this has to be balanced against the risk of causing further distress and anxiety to the families by informing them about the breach.
8.3 The ICO guidance states that “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.”
8.4 Only the data breach owner and DPO can decide whether to advise affected individuals of a data breach and therefore the reasons for deciding to do this should be clearly set out in the investigation report and discussed with the data breach owner and other involved parties before affected parties are informed.
8.5 Further advice and guidance on whether to disclose to individuals should be sought from the DPO and ICO to help determine the significance and risk of the breach.

9.0 REVIEW

9.1 A review of any data breaches and near misses should be completed and will form part of the investigation process.
9.2 Subsequent action plans should clearly outline the lessons learnt and controls agreed to reduce the risk of a further reoccurrence, a lead member of staff and a completion date.

10.0 PERFORMANCE MONITORING AND RESPONSIBILITIES

An investigation should be completed within 10 working days of the data breach being identified.
10.1 Where a major risk has been identified:

- An interim report should be presented to the Governors a minimum within 10 working days even when the case cannot be concluded within this timescale
- Further reports should be presented to Governors at least every 10 working days until the case is concluded.
-

11.0 DATA BREACH LOG

11.1 All data breaches, including near misses, will be recorded on the Data Breach Log.

12.0 GUIDANCE FOR STAFF AND GOVENORS

12.1 Sensitive or personal information and data should not be removed from the school site. However, the school acknowledges that some staff may need to transport data between the school campuses and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings or are on school visits with pupils.

The following guidelines are in place for Staff and Governors in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off the school site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances.

- Hard copy data, records, and personal information are stored out of sight and in a locked cupboard. The only exception to this is medical information that may require immediate access during the school day. This will be stored securely in each child's classroom.

- Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.

- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.

- If information is being viewed on an electronic device, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers / non-password protected electronic devices.

- If it is necessary to transport data away from the school, it should be downloaded onto a USB stick. The data should not be transferred from this stick onto any home or public computers. Work should be edited from the USB and saved onto the USB only.

- USB sticks that staff use must be password protected.

13.0 RELATED DOCUMENTS

- Data Protection Policy