DATA BREACH MANAGEMENT PROCEDURE

Approved and signed by the Board of Trustees

09.02.23

DUE FOR RENEWAL: JAN 25

NOVEMBER 2020

CHANGES

November 2020	Policy implemented
October 2021	Policy updated to reflect initial actions
January 2023	Policy reviewed, no changes made

CONTENTS

1.IDENTIFYING A BREACH

1.1 Identification

If any member of staff finds or has reported to them an actual breach or 'near miss' breach of personal data they must complete the Trust's 'Data Breach Report – Initial Details Form'.

Please refer to the Data Breach Management Policy for the definition of what is considered a breach to see if this procedure needs to be followed.

If you have identified a cyber-attack please refer to the Local Authority guidance on how to deal with this and refer to the DPO for support in completing the actions.

1.2 How were we notified?

In order to take appropriate actions we need to establish how we were notified e.g.:

- Staff member
- Partner
- Parent/carer or pupil of the school
- Member of the Public
  - Escalate to Data Protection Officer
  - Do we need to put a communication together for the press?
  - Are they taking further action?
- News article
  - Escalate to Data Protection Officer / Chief Executive Officer / Board of Trustees
  - Prepare a communications statement for the press
- Other
  - Please contact Data Protection Officer for advice

1.3 Initial Actions

In order to minimise the loss of personal data and to protect personal data from further loss immediate action must be taken.

The staff member must complete the 'Initial actions' outlined at the start of the 'Data Breach Report – Initial Details' form. These are:

1. If possible, recover the data / document as soon as possible
2. Stop further data loss (see Part 2.0 Containment below) however, DO NOT delete any emails until the DPO has reviewed the breach
3. Consult with the Chief Executive Officer
4. Report the incident

* The report must be submitted to the Data Protection Officer's (DPO) at the latest by close of business on the day of identification, if the breach was identified before 1pm, or by 12pm the following day for breaches identified after 1pm. Breaches that need to be reported to the Information Commissioner must be notified to them within 72 hours therefore the 'Initial Details' form should be submitted to the DPO sooner than the times specified if possible.

** In the case of electronic breaches the schools IT department must also be notified.

2. CONTAINMENT

Upon receipt of the notification, the DPO will take all reasonable steps, not already undertaken, to contain and minimise the impact of the breach:

- Is the breach paper or electronic?
  - Paper
    - Recover the document

        - Identify how the breach occurred
    - Post
        - Do we need to stop any further post going out?
    - By Hand
        - Is this an isolated incident?
    - Other
        - Please contact Data Protection Officer for advice
            - Identify whether anyone else may have been affected
    - Recover the documents

- Electronic
    - Email
        - Can the email be recalled?
            - Emails can only be recalled if the recipients are internal
        - Can the recipient delete the email?
            - Both from inbox and deleted items
        - Ask the recipient to confirm they have complied with the request to delete?

    - Removable media
        - Was the media encrypted?
        - Has the data been copied?
        - Has the data been passed onto a 3rd party?
        - Can the media be recovered?

    - Portable devices (laptops/tablets)
        - Was the device encrypted?
        - Was the device password protected?
        - Has the data been copied?
        - Has the data been passed onto a 3rd party?
        - Can the device be recovered?
    - Other
        - Please contact Data Protection Officer for advice

* The DPO will carry out an internet search to check that the information has not been made public; if it has been request that the information is removed from the website and deleted.

3. ASSESSMENT

The DPO will:

- Identify the type of data
- Identify the sensitivity of data
- Identify number of people affected
- Provide a description of the likely consequences of the personal data breach
- Identify any measures needed to help those affected
- Identify the cause of breach
- Analyst the breach to determine what the impact will be. This will be an assessment of the impact on the data subject of the particular aspect of the breach.
- Complete the digital Data Breach Investigation Report.

* Staff will cooperate fully during the assessment process.

4. NOTIFICATION

The DPO, in agreement with the schools Chief Executive Officer will:

- Create a communication plan to include:

- ❖ Details of who needs to be contacted
- ❖ Nature of communication
- ❖ Further requirements to manage any other contact
    - Trust contact point / DPO
    - Other short term contact points for any people that are affected (where loss affects numerous subjects).

- Send notification to any partners affected, e.g. Social Care team.
- Where applicable notify the ICO via the report a breach' page of the ICO website within 72 hours of being notified of the breach. If all 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.

5. REMEDIATION

- The DPO will identify any mitigation that prevents a recurrence.
- The Chief Executive Officer will implement any agreed mitigating actions.
    - ❖ This will include any process changes, quality assurance checks or technical controls.

6. MONTORING

6.1 Logging

The breach will be logged on the central logging database by the Data Protection Officer.

6.2 Monitoring

The DPO will review actions to:

- Ensure that they have been implemented
- Test that the risk has been minimised/eliminated

6.3 Reporting

A copy of the Data Breach Investigation Report will be provided to the Trust for the attention of the Chief Executive Officer.

A report of breaches will be provided to the Chief Executive Officer on a termly basis.

7. CLOSURE

The Data Protection Officer will confirm that the incident is closed once satisfied with the remediation plan and that any information required for external organisations such as the ICO is provided.

APPENDIX A: Data Breach Report – Initial Details Form

DATA BREACH REPORT – INITIAL DETAILS FORM

This report template is to be used when a data breach occurs or is suspected to have occurred. Please complete the form, (however do not send any sensitive details, all that is needed is that breach has occurred).

For immediate advice contact Alison Nettleship, Chief Executive Officer.

Initial actions:

1. If possible, recover the data / document as soon as possible
2. Stop further data loss
3. Consult with the Chief Executive Officer
4. Report the incident

Date/time of incident	
Please detail the relevant parties involved?	
Author of this incident report (job title and name)	
Author email address	
How many persons were affected? **If the exact number is not known please give an approximate number**	

Incident details	
Summary of affected data	
Data sensitivity	
Actions taken	

Signed by:

Author……...

Chief Executive Officer……..

Data Protection Officer……..