

Data Breach Response Plan

Step 1

Report breach to DPO or Headteacher immediately

If you believe a data breach has occured then you must immediately report it to Kate Campbell-Flint or Steve Mills. Possible breaches include:

- Loss or theft of equipment
- Inappropriate access to personal data
- Attack on systems
- Human error

Step 2

Identify the breach

(DPO and/or Headteacher)

Make a record of:

- Date and time suspected breach was discovered.
- Cause and extent of breach.
- Which data is affected?

Step 3

Contain the breach

(DPO and/or Headteacher)

Coordinate immediate action to prevent the breach continuing or recurring. Depending on the breach, this may include contacting incorrect email recipients requesting them to delete emails

Step 4

Assess the risk to stakeholders

(DPO and/or Headteacher)

Collect a list of affected individuals and determine whether the personal information involved in the breach is high risk for those involved.

Step 5

Complete Data Breach log

Use the information gathered to complete the Data Breach Log as soon as possible. This must be reported to the Governing Body and where necessary, the ICO.

Step 6

Report to ICO if necessary - within 72 hours

If the breach is considered high risk then it becomes a Notifiable Breach and must be reported to the ICO within 72 hours. If it is not deemed necessary then a note must be made in the Data Breach Log as to why this is the case.