DATA PROTECTION BREACH & NON COMPLIANCE PROCEDURE

Author:	Governance and Compliance Manager
Approval needed by:	Chief Executive
Consultation required	Data Protection Officer
Adopted (date):	13th March 2019
Date of review and updated:	25th June 2021
Date of next review:	As and when necessary

Data Protection Breach & Non Compliance Procedure

All staff, local governors and trustees must be aware of what to do in the event of a Data Protection Act (DPA) / UK General Data Protection Regulations (UK GDPR) breach.

The 'Data Breach Flowchart' outlines the process and should be considered alongside this policy (see annex 1).

The 'Data Breach Form' must be completed and updated as the process progresses. (see annex 2).

Most breaches, aside from cyber-criminal attacks, occur as a result of human error. They are not malicious in origin and if quickly reported are often manageable.

Everyone needs to understand that if a breach occurs it must be swiftly reported.

What is a breach?

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

Examples of breaches are:-

- Information being posted to an incorrect address which results in an unintended recipient reading that information
- Loss of mobile or portable data device, unencrypted mobile phone, USB memory stick or similar
- Sending an email with personal data to the wrong person
- Dropping or leaving documents containing personal data in a public place
- Personal data being left unattended at a printer enabling unauthorised persons to read that information
- Not securing documents containing personal data (at home or work) when left unattended
- Anything that enables an unauthorised individual access to our buildings or computer systems
- Discussing personal data with someone not entitled to it, either by phone or in person. How can you be sure they are entitled to that information?
- Deliberately accessing, or attempting to access or use personal data beyond the requirements of an individual's job role e.g. for personal, commercial or political use. This action may constitute a criminal offence under the Computer Misuse Act as well as the Data Protection Act.
- Opening a malicious email attachment or clicking on a link from an external or unfamiliar source, which leads to our equipment (and subsequently our

records) being subjected to a virus or malicious attack, which results in unauthorised access to, loss, destruction or damage to personal data.

What to do?

Being open about the possible breach and explaining what has been lost or potentially accessed is an important element of working with the Information Commissioners Office (ICO) and to mitigate the impact. Covering up a breach is never acceptable and may be a criminal, civil or disciplinary matter.

Each academy has appointed a lead for data protection. All breaches must be immediately reported to the academy lead. The academy lead will be responsible for completing the breach notification form and maintaining a breach register. The academy lead will report the breach to the Data Protection Officer (DPO) and the Governance and Compliance Manager immediately. This is essential.

If the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach, notification to those people will be done in a coordinated manner with support from the DPO.

Actions and changes to procedures, additional training or other measures may be required to be implemented and reviewed.

A breach report will be made by the DPO within 72 hours of becoming aware of the breach.

It may not be possible to investigate the breach fully within the 72-hour timeframe. Information about further investigations will be shared with the ICO with support from the DPO.

Procedure – Breach notification data controller to data subject

For every breach the academy (with guidance from the DPO) will consider notification to the data subject or subjects as part of the process. If the breach is likely to be high risk they will be notified as soon as possible and kept informed of actions and outcomes.

The breach and process will be described in clear and plain language.

If the breach affects a high volume of data subjects and personal data records, the most effective form of notification will be used and discussed with the Data Controller with support from the DPO.

Advice will be taken from the ICO about how to manage communication with data subjects if appropriate.

A post breach action plan will be put into place and reviewed.

Evidence Collection

It may be necessary to collect information about how an information security breach or unauthorised release of data occurred. This evidence gathering process may be used as an internal process (which can include disciplinary proceedings), it may be a source of information for the ICO, and it could also be used within criminal or civil proceedings.

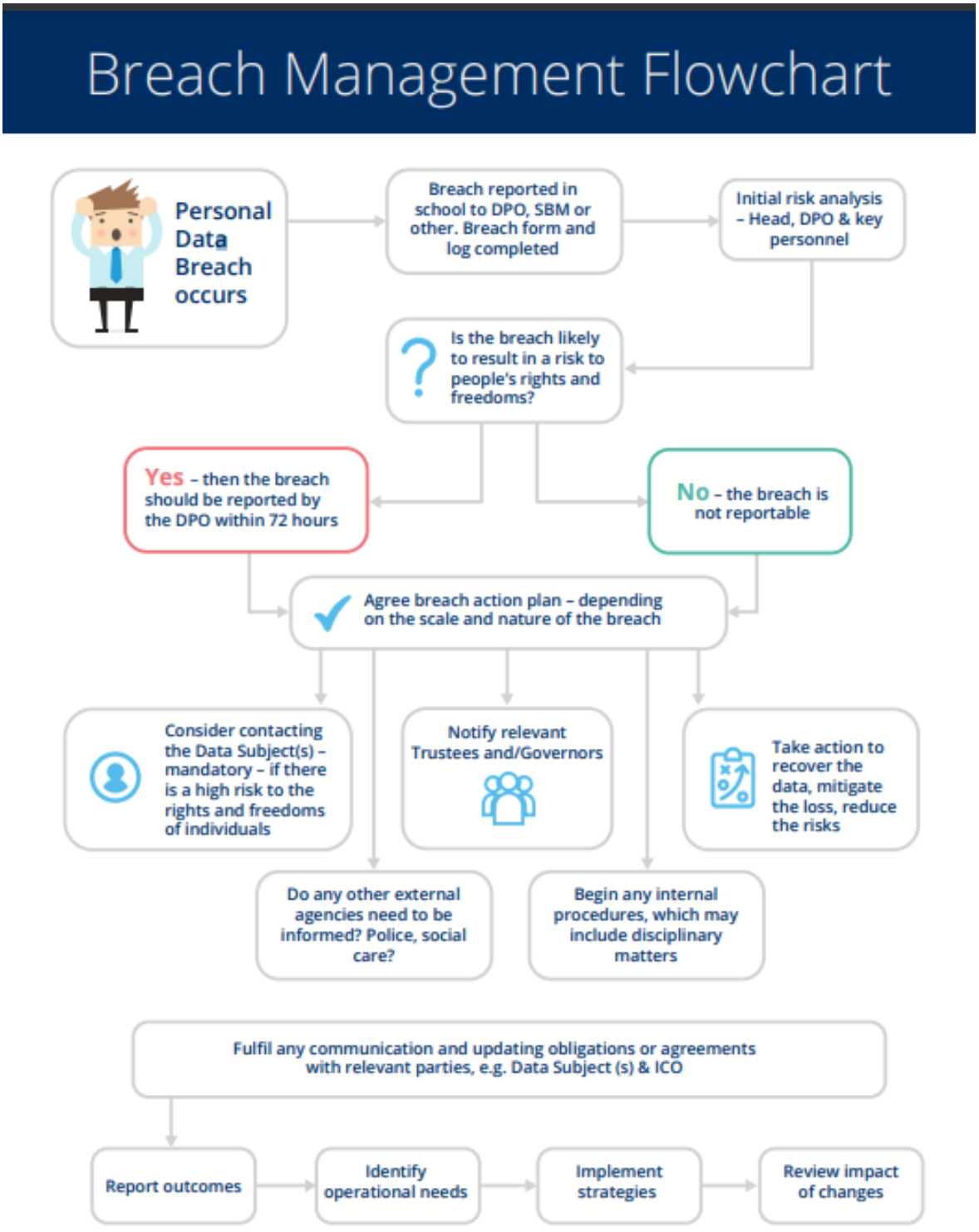
This process will be conducted by a suitable member of staff, which may be the academy lead for data protection, Governance and Compliance Manager or the DPO, but will be determined depending on the nature of the breach.

Guidance may be required from external legal providers and police may be involved to determine the best way to secure evidence.

A record of what evidence has been gathered, stored and secured must be available as a separate log (see example below). Files and hardware must be securely stored, possibly in a designated offsite facility.

Date	Evidence Description	Secure storage location & confirmed date	School Officer (whoever gathered the evidence)

Annex 1 – Data Breach Flowchart



Annex 2

Data Breach Reporting Form

School	
Date	
Reporter name and role	

Part A: Breach Information

When did the breach occur (or become known)?	
Description of Breach. **This must include the type of information that was lost, e.g. name, address, medical information, NI numbers**	
Which staff member was involved in the breach?	
Has the staff member had Data Protection Training within the last 2 years?	
Who was the breach reported to?	
When was the DPO notified?	
Date Reported:	
Time Reported:	
Initial Actions:	

Part B: Breach Risk Assessment

What type of data is involved:	Hard Copy: Electronic Data:
Is the data categorised as 'sensitive' within one of the following categories:	Racial or ethnic origin: Political opinions: Religious or philosophical beliefs: Trade union membership: Data concerning health or sex life and sexual orientation: Genetic data: Biometric data:
How was the data secured originally?	
How did the breach occur?	
What information was disclosed?	
Whose data has been breached?	
What risks could this pose? Be specific about this situation. If the risk is minimal, explain why.	
Are there wider consequences for the data subjects or school to consider e.g. reputational, loss of confidence?	
How many people might be affected by the breach? Either directly or indirectly.	

Part C – Cyber Breaches

Is this a cyber breach?	Yes/No If 'No' move to Section D
Has the confidentiality, integrity and/or availability of the system been affected. If so which and why	
What is the impact on the organization?	
What is the expected recovery time?	
Are any other IT systems/providers affected? If so, who and how?	

Part D: Breach Notification

Is the breach to be reported to the ICO? With reasons for decision	Yes/No Reasons
Date ICO notified	
Time ICO notified	
Reported by	
Method used to notify ICO	
ICO Reference No.	
Governors' Notified? Yes or No – reasons for decision at this point	
Notes:	
Is the data subject to be notified? Yes / No with reasons	Yes/No Reasons
Date and method data subject notified	
Notified by	

Response	

Part D: Breach Action Plan

Has the data been recovered? **Is it likely to be recovered?** **What steps were taken to recover the data?**	Yes/No Reasons
Who has been involved in the data recovery/breach management process?	
Do any other agencies need to be involved? If so, why?(e.g. police and social care)	
What will be done to prevent another breach	
Any training needs identified? For individuals and for whole staff?	

This page is blank