# Data Protection Breach & Non Compliance Procedure

All staff, governors and trustees must be aware of what to do in the event of a DPA / UK GDPR breach.

The ‘Data Breach Flowchart’ (Appendix 1) outlines the process.

The ‘Data Breach Form’ (Appendix 2) must be completed and updated as the process progresses.

Most breaches, aside from cybercriminal attacks, occur because 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, unauthorised 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 school 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 school’s equipment (and subsequently its 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 ICO and to mitigate the impact. Covering up a breach is never acceptable and may be a criminal, civil or disciplinary matter.

Report the breach to the Data Controller, Data Protection Compliance Manager and DPO as soon as possible, this is essential. Complete the Data Breach form (Appendix 2).

Data Controller: Head teacher at the school within which the Breach has taken place. Data Protection Compliance Manager: Danielle Benyon-Payne, [admin@oaktrust.org](mailto:admin@oaktrust.org) DPO: John Walker: [john@jawalker.co.uk](mailto:john@jawalker.co.uk)

**What happens next?**

The breach notification form will be completed and the breach register updated.

Advice will be sought from the DPO. Consideration is given about how to effectively manage the breach, who to inform and how to proceed.

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 co-ordinated manner with support from the DPO.

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

The breach report will be 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 school 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 Data Protection Compliance Manager and 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, it could also be used within criminal or civil proceedings.

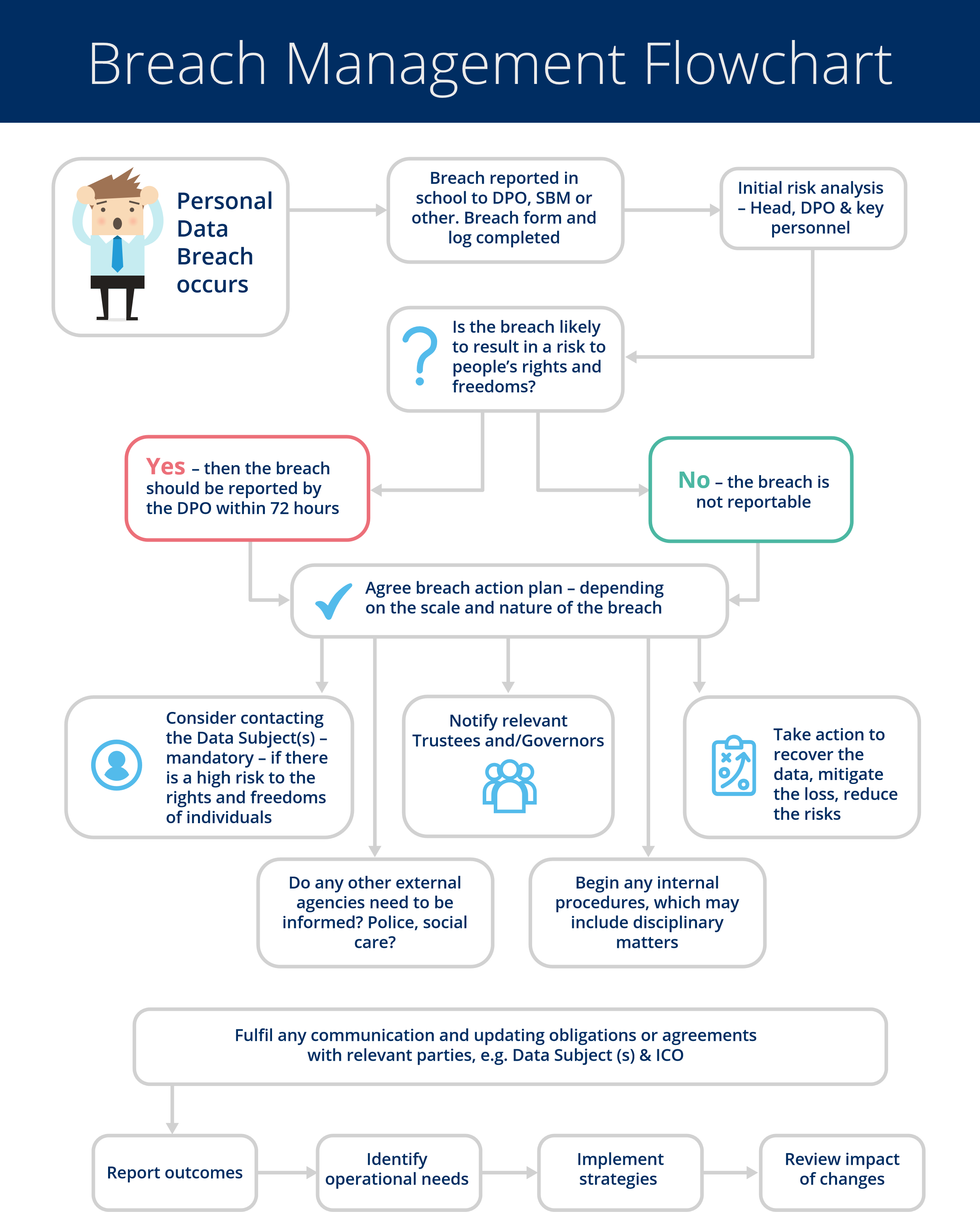
This process will be conducted by a suitable member of school staff, which may be the Data Management Compliance Officer or Data Protection Officer, but will be determined depending on the nature of the breach.

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. Files and hardware must be securely stored, possibly in a designated offsite facility.

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Evidence Description | Secure storage  location & confirmed date | School Officer |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Appendix 1





**www.jawalker.co.uk john@jawalker.co.uk 0333 772 9763**

Appendix 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:** |  |

**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:** |  |
| **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 E: 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?** |  |

# Appendix 3

# Template email to parents re email data breach

Dear Parent/Carer,

I am writing to apologise for the recent email where addresses were shared. This was an error. I hope that this has not caused any distress or anxiety. I am asking that you make sure that you delete the email with the addresses.

(IF APPLICABLE)

I attach the same documents to this email for ease. Please respond by XXXXX

The matter has been reported to our Data Protection Officer and advice has been taken.

There will be further staff training about the issue to prevent a repeat of this type of incident.

If you have any additional concerns, please do not hesitate to contact me to discuss.

Kind regards,