

## **Data Breach and Cyber Incident Procedure**

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

The 'Data Breach Flowchart' (Appendix 3) outlines the process. The 'Data Breach Form' will be completed and updated as the process progresses via the school GDPR Lead (details below). In the event of a cyber-criminal attack, you should inform your Cyber Security Lead who will complete an incident log and follow the correct procedures.

Most breaches, aside from cyber-criminal 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 School GDPR Lead and Trust Governance Manager as soon as possible, this is essential. The Trust Governance Manager will liaise with the DPO and report any breaches to them.

**Any cyber-criminal attacks will need to be reported to the school's Cyber Security Lead, details below. They will then inform the Managed Service Provider, AIT.**

Trust Governance Manager: Danielle Benyon-Payne, [admin@oaktrust.org](mailto:admin@oaktrust.org) T: 0116 303 3721

#### GDPR Leads

School	Name	Office hours	Out of hours
Brookside Primary School	Richard Skelton	0116 271 3680 / 201	07951498804
Manor High School	Bukie Ayo Bello Out of hours / Alison Dawes	0116 272 9799 / 799	07900922501
Overdale Infant School	Jenny Robinson	0116 2882724 / 415	07769654636
Overdale Junior School	Ravinder Kooner Out of hours: Sarah Cooke	0116 288 3736	07795573048
Woodland Grange Primary	Annette Howard / James Parker	0116 2720401 / 501	07482316089

#### Cyber Security Leads

Brookside Primary School	Richard Skelton	0116 271 3680 / 201	07951498804
Manor High School	Alison Dawes	0116 272 9799 / 799	07900922501
Overdale Infant School	Jenny Robinson	0116 2882724 / 415	07769654636

Overdale Junior School	Sarah Cooke	<a href="tel:01162883736">0116 288 3736</a> /402	07795573048
Woodland Grange Primary	Annette Howard / James Parker	0116 2720401 / 501	07482316089

What happens next?

The breach notification form will be completed by the Trust Governance manager, 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.

In the event of a cyber incident, the insurance company will also be notified (appendix 4).

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 Trust Governance 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 Trust staff, which may be the Governance Manager, Managed Service Provider (for a cyber-attack) 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.

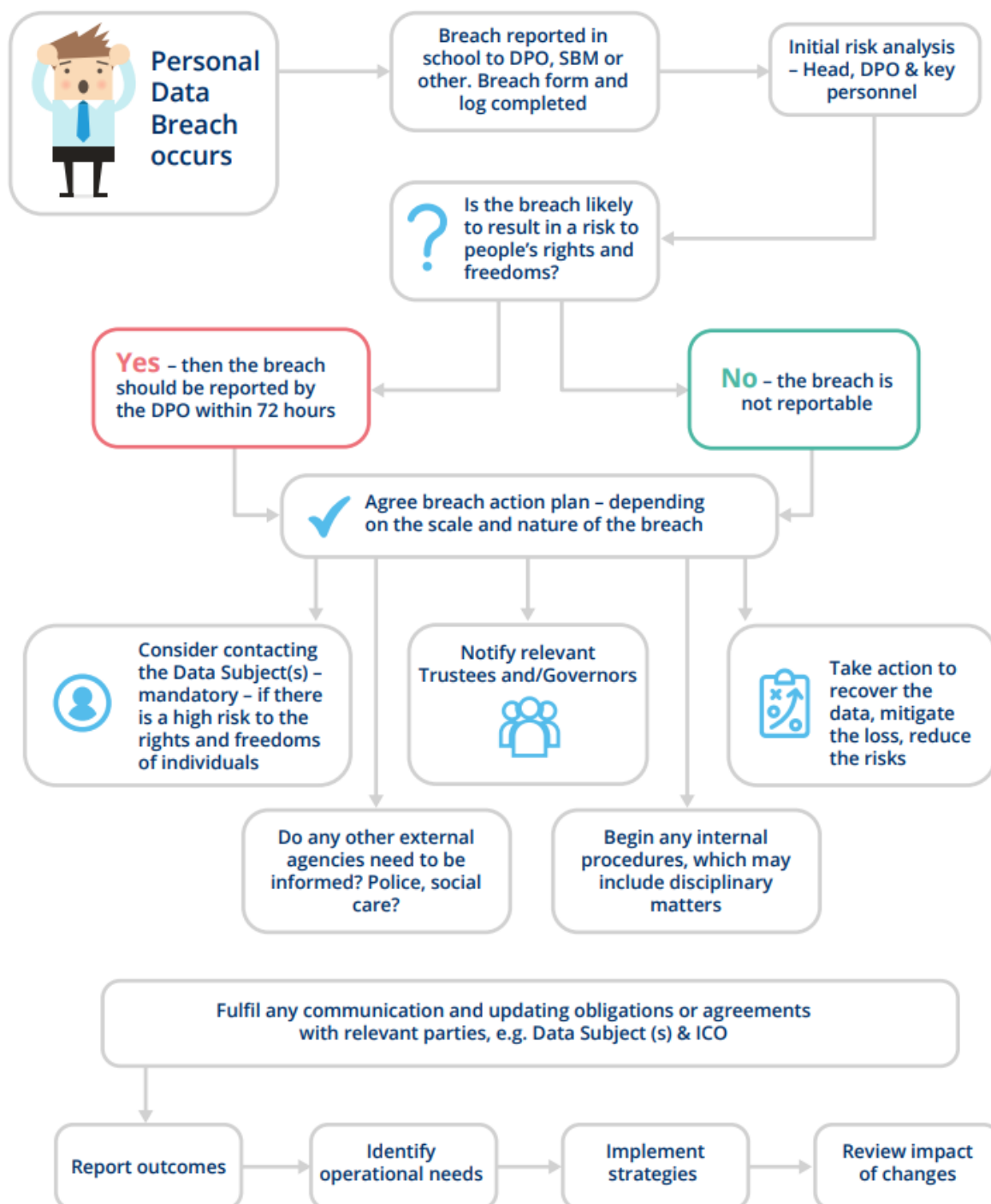
A record of what evidence has been gathered, stored and secured must be available as a separate log. Files and hardware must be securely stored, possibly in a designated offsite facility.

## Appendix 1 – Data Breach Reporting form

Please send any information regarding a data breach to [admin@oaktrust.org](mailto:admin@oaktrust.org) in the following format:

[illegible]

## Appendix 2: Data Breach Flow Chart




## Appendix 4: Insurance requirements in cyber incident



# Are you experiencing a cyber incident?


*Our in-house team is ready to help you, 24 hours a day, 365 days a year*



### Phone

USA (local): 1-844-677-4155	Australia (local): 1800 803 202
UK (local): 0800 975 3034	Rest of World: +44 (0) 208 798 3134
Canada (local): 1-800-607-1355	

OR



### CFC app

- ☒ **Download**  
Get our free incident response app at time of policy purchase
- ☒ **Register**  
Sign up by entering your policy number when prompted
- ☒ **Report**  
It takes just a few short clicks through the app


OR



### Online

Notify a claim at  
[www.cfcunderwriting.com/claims](http://www.cfcunderwriting.com/claims)

OR



### Email

Send your details to  
[cyberclaims@cfcunderwriting.com](mailto:cyberclaims@cfcunderwriting.com)

### How it works

- 1 Get in touch**

Reach out to us right away and provide us with your company name, phone number, policy number, and brief description of the incident.
- 2 Immediate response**

You'll immediately be assigned an experienced cyber claims specialist to guide you through the incident.
- 3 Proactive management**

We'll support you through the entire lifecycle of your claim, getting you back up and running as quickly as possible.

CFC Underwriting Limited is authorised and regulated by the Financial Conduct Authority FRN: 312848. Registered in England and Wales RN: 3302887  
Registered Office: 85 Gracechurch Street, London EC3V 0AA VAT Number: 133541330