CHAILEY SCHOOL

Data Breach Management Procedures

Date of Governing Body's Approval: 27th January 2021

Chair of Governors:

Head Teacher:

Date Due for Review: December 2022 (biennial review)

Data Breach Management Procedures
Chailey School

1. Raising an incident:

- If you become aware of a personal data breach you should immediately notify either Glen Mayhew, Data Manager or in his absence Janine Slade, School Business Manager;

- The Data Manager or School Business Manager should then refer any data breaches to the DPO – Roger Simmonds (rsimmondsltd@gmail.com) as soon as they happen so that they can make an assessment of whether they need reporting to the Information Commissioner's Office (ICO). Please refer to Appendix A Data Breach Report Form.

- Failure to report breaches that need to be reported to the ICO within 72 hours constitutes a breach so it is very important that the appropriate escalation point is made aware of breaches as soon as they happen.

Crucial basic information to report;

- What's happened?
- Details of the type of personal or sensitive information that has been or has the potential to be compromised
- An overview of how the incident has been dealt with so far

2. Containment and Recovery:

- Decide who should take the lead on investigating the breach and ensure they have the appropriate resources.
- Establish containment actions that can take place and enact them if possible – e.g. find a lost piece of equipment/data, change the access code to a door or close an affected section of a network.
- Establish whether there is anything you can do to recover any losses/damage from a breach – i.e. back up database to store lost data.
- Where appropriate, inform the police.

3. Assessment of impact and ongoing risks:

- Following the immediate containment of a breach, the risks associated should be assessed in order to identify an appropriate response.
- All breaches must be managed according to their risk.
- Questions to consider when assessing level of risk; *Nature of the breach? Category and amount of individuals effected? What are the potential*

adverse consequences? How likely are these? What could the data tell a 3rd party, what harm could this cause?

4. Notification of breach:

- Consideration is required as to whether any individuals or organisations should be notified of a breach. Notification should have a clear purpose;
- As detailed in the tab before, individuals at 'high risk' due to a breach need to be informed in order to take steps to protect themselves.
- Remember you must report a breach in which it is likely to result in a risk to the rights and freedoms of individual(s), to the ICO within 72 hours (please refer to the 'GDPR obligations' tab for more detail).

5. Evaluation and response:

It is important to evaluate the effectiveness of the response to the incident. If the breach was caused, even in part, by inadequate policies or a lack of a clear allocation of responsibility for example, then it is important to review and take remedial action.

6. Finally, ensure you document personal data breaches:

The GDPR states that you should ensure all personal data breaches are recorded, regardless of whether they have been sent to the ICO, etc.

You need to document the details of the breach, its effects and any remedial action taken as this is part of your overall obligation to comply with the accountability principle of the GDPR.

Appendix A

Data Breach Report Form		
Name of School:	Chailey School	
Name and contact details of DPO:		
Date:		
Reported by (name):		
Date of breach/incident:		
Type of breach/incident		e.g. lost or stolen paperwork/disclosed in error/technical security failing/unauthorised access/ lost or stolen hardware etc.
Description of incident		
Remedial Action taken		
Data Subject(s) notified? (provide date)		
DPO notified? (provide date)		
Reported to ICO? (provide date)		
Additional Information		