Fairfield School
Embracing Uniqueness

Data Breach Response Policy and Procedure

Nov 2020

Version	1.0
Date Approved by Governors:	10th Nov 2020
Review date:	10th Nov 2022
Version History	

Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out below.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately complete Appendix 1 and notify the DPO
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the headteacher, Business Manager and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation

- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way) in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the school's computer system.

- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- *If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error*
- *Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error*
- *If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it*
- *In any cases where the recall is unsuccessful, the Sender will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way*
- *The Sender will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request and advise the DPO of the fact*
- *The ICT representative or DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted*

***Other types of breach that you might want to consider could include**:*

- *Details of pupil premium interventions for named children being published on the school website*
- *Non-anonymised pupil exam results or staff pay information being shared with governors*
- *A school laptop containing non-encrypted sensitive personal data being stolen or hacked*
- *The school's parent payment provider being hacked, and parents' financial details stolen*

Consequences of Failing to Report a Breach

Failing to notify a breach when required to do so can result in a significant fine up to 10 million euros or 2 per cent of your global turnover. The fine can be combined the ICO's other corrective powers under Article 58, a sample of which are as follows:

a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;
b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;
c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;
d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;
e) to order the controller to communicate a personal data breach to the data subject;
f) to impose a temporary or definitive limitation including a ban on processing;

NB: This list is not exhaustive

So, it's important that staff follow the breach-reporting process in place within this policy and to ensure we recognise, detect via our IT provider and can notify a breach, on time; and to provide the necessary details. We shall use the ICO breach reporting form for this purpose as follows https://ico.org.uk/media/for-organisations/documents/2614197/personal-data-breach-report-form-web-20190124.doc .

It is imperative that, where staff feel a breach has occurred, they report this to the DPO, Head or the Business Manager at the earliest opportunity.

This policy will be reviewed on a bi-annual basis.

Adopted by Governors on [Insert Date]

Review date [Insert Date]

Signed

Date

Appendix 1 – Data Breach Report Form

Data Breach Report Form		
This form should be completed as soon as a data breach has been discovered. Please complete sections 1 -7 with as much information as possible and pass the form on to the School Business Manager or Headteacher immediately. The breach will be recorded on the School's Breach Register and the DPO informed so that an investigation can be carried out		
	Report by:	
	Date	
1	Nature of breach e.g. theft/disclosed in error/technical problem	
2	Description of how breach occurred:	
3	When was the breach reported and how did you become aware?	
4	Full description of all personal data involved	
5	Number of individuals affected? Have all individuals affected been informed	
6	What immediate remedial action was taken:	
7	Has the data been retrieved or deleted? If yes – date and time:	
8	Any Procedure changes needed to reduce risks of future data loss	

9	Conclusion	