Data Breach Management Policy

Member of staff responsible: Lorraine Shaw
Ratified by Governors:
Review cycle: Annually or as necessary (to reflect best practice and ensure compliance with any changes or amendments to Data Protection legislation)
Next Review date: November 2021

Introduction

This procedure is based on guidance on personal data breaches produced by the ICO and the Article 29 Working Party.

Data Breach Management Procedures

1. On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.

2. 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

3. The DPO will alert the Headteacher and the Chair of Governors if applicable.

4. 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).

5. The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.

6. 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 pseudonymisations (for example, key-coding, however this is not used)
   - 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.

7. 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 filed securely in the GDPR Register. 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

8. 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.

9. 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

10. 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.

11. 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 internal school GDPR Register, and in the school electronic and paper filing systems.

12. The DPO, SBM 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

Bush Hill Park Primary School will take the actions to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. The School will review the effectiveness of these actions and amend them as necessary after any data breach. Such actions include, but are not limited to;

- Anonymising and minimizing data
- Encrypted drives
- Secure access servers
- Strong password setting
- Training and support for staff and governors.
- Encrypted email