



Personal Data Breach Procedure


for

The ACE Centre Nursery School

This policy was adopted by a meeting of The ACE Centre Nursery School governors:

Held on: 11.05.2022

Date to be reviewed: summer term 2024

Signed:  (Chair of Governors)

Signed:  (Headteacher)

Introduction

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 notify the DPO

Investigation

The DPO will investigate the report to determine whether a breach has occurred. To determine this 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

Responsibilities

- The DPO will alert the Headteacher 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
- The DPO will assess the potential consequences, based on severity and likelihood of occurrence
- The DPO will determine if 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, causing 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

Information Commissioners Office

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 electronically
- If the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through their breach report line (0303 123 1113), 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
 - If this information is not yet known, the DPO will report as much as they can within 72 hours. The report will explain and justify the delay and indicate timescales for the further information.
 - The DPO will submit the remaining information as soon as possible

Risk Assessment

- 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 all individuals in writing whose personal data was breached. This notification will set out:
 - A description, in clear and plain language of the nature of the personal data breach
 - 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 or will be taken to deal with the data breach, mitigating any possible adverse effects on the individual(s) concerned
- The decision to contact individuals will be documented by the DPO
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals (e.g. police, insurers, banks or credit card companies)



Documentation

- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - Facts relating to the breach
 - Effects
 - Action taken to contain it and ensure it does not happen again (e.g. establishing more robust processes or providing further training)
- Records of all breaches will be stored electronically
- 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