Thurlstone Primary School

Data Breach Policy

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 Data Protection Lead (DPL) in school.

- The DPL will investigate the report, and determine whether a breach has occurred.
- The DPL will contact the DPO to 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

A decision will be made by the DPO on whether the breach should be classed as a 'contained' or 'controlled breach or whether the ICO should be informed.

If data has been breached, but it has no direct impact on the data freedoms of a subject, the school can define this as a 'contained' breach.

If the school has asked parents/carers to register with a third party services e.g. catering system were data has been breached, the school will work with the company to support parents/carers.

- The DPL will alert the Headteacher to evaluate the impact of the breach on the
- school.
- The DPL/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 DPL/DPO will assess the potential consequences, based on how serious they are,
- and how likely they are to happen
- The DPL/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 DPL 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 in a secure filing cabinet in the school office, electronic copies may be stored
- with the DPO and Business Manager.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page
- of the ICO website (https://ico.org.uk/for-organisations/report-a-breach/) within 72
- hours. As required, the DPL/DPO will set out:
    - o 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 DPL/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 DPL/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 DPL/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 DPL will liaise with the data subject to help them notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
- The DPL/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 in either a secure filing cabinet in the school folder or on an electronic folder on the school network.

The DPL (and in some circumstances, 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.

The important aspect of a data breach is to understand the 'lessons learned' and the school may wish to review its procedures after the breach. In addition, staff may need further training to avoid any further breaches.

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.

Specific Actions Needed After a Data Breach

NB This list is not exhaustive and schools may want to add further information.

- Consultation with IT technical support to ensure that software is updated (patched) to minimise a breach.
- Password to be changed and the school to follow guidance from the National Cyber

Security Centre

- To ensure that staff use BCC on emails that include multiple recipients
- For staff to use the encryption service on the email platform that the school uses.
- The school to review the use of removeable media and ensure that it is encrypted. It
- is recommended that the school moves away from the use of removable media and
- uses cloud based platforms e.g. One Drive/G Drive.
- All mobile technology e.g. Ipads has security measures in place.
- All staff follow a clear desk policy.
- All sensitive data that is transported out of school is locked in car boots and in secure
- places in staff homes.
- Staff to read the relevant Data Privacy Impact Assessments