Forward Education Trust Guidance on Breach Management

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

- On finding or causing a breach, or a potential breach, the staff must immediately notify the Data Protection Officer via email at DPO@fet.ac and also enquiry@fet.ac. The relevant data protection contact from the school concerned should also be copied into this email, unless the disclosure is potentially a confidential whistleblowing matter;
- The DPO, in conjunction with relevant staff will investigate the alleged data breach, and determine whether a breach has occurred.
- To decide whether a breach has occurred, 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 relevant Headteacher and the CEO of the Trust.
- The school, supported by 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 in conjunction with the CEO and Trust team will determine 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 breach should be reported to 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 will be stored in as part of the relevant IAR and risk register.
  - Where the ICO must be notified, the DPO will do this 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 in conjunction with the relevant school 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 school/Trust 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 and school 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 each base school's data audit spreadsheet.

- In the case of a reportable breach, the DPO and relevant Headteacher and CEO will review what has happened and how it can be stopped from happening again. This will happen as soon as reasonably possible. In these circumstances, the Headteacher will be responsible for sharing this information to the CEO, so that lessons can be learnt and appropriate interventions or training put in place.

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 alert the Headteacher at their school and notify the DPO as soon as they become aware of the error.
- The member of staff or Headteacher will contact the relevant unauthorised individuals who received the email, explaining 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
- Members of staff who receive personal data sent in error must alert the sender as soon as they become aware of the error
- The school will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- Where relevant, the 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

Lessons Learned and follow up actions

The DPO will work with the relevant school and Trust staff to ensure lessons learned from breaches and near misses affecting the Trust are shared appropriately.

The DPO will ensure training and guidance to staff is adjusted to account for risks that have been realised as breaches or near misses.