PERSONAL DATA BREACH PROCEDURE

This procedure is based on guidance on personal data breaches produced by the Information Commissioners' Office.

1. On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Data Protection Officer (DPO) for the academy. National team members must notify the Director of Governance & HR. It is important that all staff recognise the importance or reporting an actual or suspected breach immediately and that failure to do so may be a disciplinary matter.

2. The DPO will immediately 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 Principal and the Director of Governance & HR on the same day.

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.

5. In discussion with the Director of Governance & HR, the DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.

6. The Director of Governance & HR will decide whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, they 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
    - Identity 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 is likely that there will be a risk to people's rights and freedoms, the Director of Governance & HR must notify the ICO.

7. The Director of Governance & HR 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.

8. Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. The 72 hours includes non working hours, weekends and school holidays so action must be swift. 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 contact person
    - 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

9. If all the above details are not yet known, the Director of Governance & HR will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when further information can be expected. All remaining information must be submitted as soon as possible.

10. In consultation with the Director of Governance & HR 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

11. In consultation with the Director of Governance & HR 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

12. The academy DPO will document each breach, irrespective of whether it is reported to the ICO and forward a copy of this record to the Director of Governance & HR. 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)

13. Records of all breaches will be stored by the DPO.

14. The DPO and Principal will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible and depending on the seriousness of the breach may also include the Director of Governance & HR.

Examples of a data breach

It is important to recognise that personal data may be held electronically or in hard copy and therefore a data breach could range from the loss of a memory stick, a stolen laptop to a file left on a train. As well as accidental breaches, deliberate sharing of personal data with non authorised people or organisations or a cyber attack would also be reportable. Filing cabinets containing personal data left unlocked, altering data, forwarding of data to personal devices or destroying or deleting of data in a non secure way are other examples. This list is not exhaustive and where in doubt guidance should be sought from the DPO or Director of Governance & HR.

Actions to minimise the impact of data breaches

We will also take the necessary steps to minimise the impact of the different data breaches that might occur, 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. All staff and volunteers should follow the requirements of the Trust Data Protection Policy.

DATA BREACH REPORTING FORM (To be completed by the Data Protection Officer)

Academy:

Person reporting:

DPO:

Date and time of suspected/actual breach:

Date and time reported to DPO:

Date and time reported to Principal and Director of Governance & HR:

Report to ICO: YES/NO

Date and time reported to ICO:

Detail of suspected/actual breach (please provide as much detail as possible and continuing on a separate sheet if needed)

Initial investigation report from DPO including potential consequences

Agreed action