Viking Academy Trust

GDPR Data Breach Procedure

Approved by the Trust: Term 2 2019
Reviewed biennially: Term 2
Last review date: Term 5 2024

Signed: **Chair of Trustees**

The Viking Academy Trust

Empowering Children Through Education: One Childhood One Chance

Schools in the Viking Academy Trust (VAT)

These are:

Chilton Primary School
Ramsgate Arts Primary School
Upton Junior School

This **'Personal Data Breach Policy'** is for all aforementioned schools.

Personal Data Breach Procedure

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

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Data Protection Officer (DPO). The Trust's DPO is **Claire Roby, Central Administration Manager.**

- 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

- The DPO will alert the Executive Headteacher, Head of School and Chair of the Trust Board, Chair of Governors (if school specific breach) and the designated GDPR member of Governance.

- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff member 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, using a checklist (Appendix 1)

- Using all information and the ICO self-assessment tool, 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
- Identity theft or fraud
- 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 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 on SharePoint within the folder called 'GDPR'.
- 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*
- If all of 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 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. The 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 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 Sharepoint's 'GDPR' folder.

The DPO and Executive 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

- 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)

- Sensitive information being disclosed via email (including safeguarding records) **must be encrypted.**
- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the IT department to recall it
- In any cases where the recall is unsuccessful, the DPO/data processor will contact the relevant unauthorised individuals who received the email, explain 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
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- 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

Other types of breach:

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results
- Employees pay information being shared with governors / staff
- Employees bank details shared
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen
- Staff appraisal reports including performance monitoring data eg observation feedback, targets for improvement, informal capability plans

Appendix 1:

GDPR DATA BREACH CASE LOG

Date:

School:

Name & role of staff reporting	
Description of the nature of the breach	
The name and contact details of the data protection officer or another contact point	
A description of the likely consequences of the breach	
A description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects	
Has the ICO been informed?	