



Athena Learning Trust

Trust-wide

Data Breach Procedure

Review

Reviewed on: 31st October 2022

Reviewed by: Board

Review Period: 3 years





ATHENA
LEARNING TRUST

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

Judicium Consulting Limited is the Data Protection Officer (DPO). Their role is to oversee and monitor the role of the trust's data protection procedures and to ensure they are compliant with UK GDPR and DPA 2018. The DPO can be contacted by email:

dataservices@judicium.com

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.
- 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 CEO/school principal and the chair of trustees/local governing board.
- 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 how serious they are, and how likely they are to happen
- 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
 - 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



ATHENA LEARNING TRUST

- If it is 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 in the Data Breach Log on the trust's network.
- 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 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. 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 will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - Facts, cause and 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 the Data Breach Log on the trust's network.



- The DPO and CEO/school principal will meet, as soon as reasonably possible, to review what happened and how it can be stopped from happening again. The trust will take action to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. The trust will review the effectiveness of these actions and amend them as necessary after any data breach.

Actions to minimise the impact of data breaches

We set out below the steps we might take to try to mitigate the impact of different types of data breach if they were to 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.

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 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 ICT department to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence).
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to 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 endeavour to obtain 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.
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any of its local safeguarding partners.

Other potential data breaches are outlined below and will be dealt with in line with the trust's policy:

- Details of pupil premium interventions for named children being published on the school website.
- Non-anonymised pupil exam results or staff pay information being shared with governors.
- 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.
- Hardcopy reports sent to the wrong pupils or families.