Data Breach Policy

Expanse Learning Group

November 2022

Author:	Scott Roberts	Version	6	Review Date:	Nov-2023

1. Scope

This policy applies to all staff at Expanse Learning and its purpose is to provide guidance in the event of a data breach within the company.

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

2. On finding a breach

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

3. Role of Data Protection Officer (DPO)

The name and contact details of the DPO:

Scott Roberts
Head of shared Services
T: 01942 877715
M: 07921888300
E: scott.roberts@expansegroup.co.uk

The DPO will:

- alert the CEO and the chair of governors
- 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).*
- assess the potential consequences, based on how serious they are, and how likely they are to happen
- work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis.
- 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.*
- 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 DatabridgeMIS (Restricted Access)
- 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*
- 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 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 Expanse Learning OneDrive Folder (Controlled access).*
    - *The DPO and CEO will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible*

4. 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.

5. 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 recall it
- In any cases where the recall is unsuccessful, the DPO 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
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A Company laptop containing non-encrypted sensitive personal data being stolen, lost or hacked

6. Monitoring arrangements

This policy will be reviewed every 12 months but can be revised as needed.

Impact of non-compliance

Staff:	Disciplinary action, prosecution
Student:	Not applicable
Legislation/organisational:	Reputational damage, litigation, statutory and non-regulated compliance. prosecution
Compliance lead:	Shared Services
Policy Reference:	ELGR-POL-DAMA-0005
Version:	6
Agreed policy location:	DatabridgeMIS
Review Schedule:	12 Months
Does the policy require Governor approval?	No

Approval

Prepared by	***Approved by***	***Counter Signatory***
Scott Roberts (Assoc. CIPD)	Tony Brown	Richard King
01/11/2022	01/11/2022	01/11/2022
		
Head of Shared Services	CEO	Director of Schools, Pre 16 Education

Version Control

Version	***Date***	***Revision***	***Review Date***
1	04/01/2018	First Issue	03/01/2019
2	04/02/2019	Transferred to new policy template	04/02/2020
3	01/09/2019	Policy review and transfer onto new template	31/08/2020
4	01/09/2020	Reviewed	31/08/2021
5	01/09/2021	Policy Reviewed	31/08/2022
6	01/11/2022	Policy Reviewed and DPO updated	31/10/2023