Data Breach Procedure

Review Date: **01/08/2023**

Next Review Date: **August 2024**

Signed: ***Changing Education Group***

Consultants: ***RiskEvolves***

Policy title:	Data Breach Procedure

Issue date:	August 2023	Review date:	August 2024

Version:	1.0	Issued by:	Helen Barge

Scope:	

Associated documentation:	Information Security and Privacy Policy Data Breach Register, Data Privacy Policy
Appendices:	None
Approved by:	Managing Director
Date:	June 2022

Review and consultation process:	Annual review as part of CE & IASME Process. Additional reviews to be undertaken in the event of changes to legislations and as part of ISO9001 etc.
Responsibility for Implementation & Training:	Day to day responsibility for implementation: Managing Director Day to day responsibility for training: Managing Director

Revisions:		
Date:	Author:	Description:
16th August 2020	Helen Barge	Initial Version
1st June 2022	Rachel Fuller	Second Version

Distribution	Document to be stored on Changing Education Google Drive. Access to be provided via email to all employees and contractors. If you have any suggested changes to this document, then please notify the Managing Director at info@changingeducation.co.uk Any copies that are printed will be deemed to be invalid within 24 hours of printing.

1. Purpose

Changing Education have this procedure is in place to provide a standardised response to any reported data breach incident and ensure that data breaches are appropriately logged and managed in accordance with the law and best practice.

2. Scope

This procedure applies in the event of a personal data breach and applies to all Changing Education Employees or Contractors at all times and whether located within the physical offices or not.

The document applies to all information we hold and all information technology systems utilised by us.

3. Responsibility

All Employees or Contractors and third parties working for or on behalf of us are required to be aware of, and to follow this procedure in the event of a personal data breach.

All employees or Contractors are responsible for reporting any personal data breach to the Data Protection Officer who's contact details are as follows:

Name: Stephen Hackney
Telephone: 01625 827309
Email: s.hackney@changingeducation.co.uk

4. Definition

The GDPR defines a "personal data breach" in Article 4(12) as: "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". Examples include:

- Loss or theft of data or equipment (paper records, digital records and IT devices)
- Access by an unauthorised third party (including physical intrusion of the premises)
- Sending personal data to an incorrect recipient
- Alteration of personal data without permission
- Loss of availability of personal data such as equipment failure
- Unforeseen circumstances such as a fire or flood
- Hacking attack eg. ransomware or phishing attack
- 'Blagging' offences where information is obtained by deceit for the purposes of this procedure data security breaches include both confirmed and suspected incidents.

If you suspect a data breach or are unsure whether the incident which has occurred constitutes a data breach, please refer the matter to the Data Protection Officer for consideration

5. Reporting an incident

Any individual who accesses, uses or manages information within our business is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer.

If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

The report will include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, the nature of the information, and how many individuals are involved.

6. Next Steps

The Data Protection Officer will firstly determine if the breach is still occurring.

- **In progress :** If an event is in progress, the appropriate steps will be taken immediately to minimise the effect of the breach.

- **Occurred :** If an event has been deemed to have occurred in the past, the appropriate steps will be taken immediately to understand the time and impact of the event, numbers of records impacted etc,

- **Near Miss :** If an occur may have occurred or has the potential to occur in the future, then this should be reported to the Data Protection Officer.

In all instances, an entry must be made in the data breach register (see below).

An initial assessment will be made by the Data Protection Officer in liaison with relevant persons (which may include IT services, insurance providers etc) to establish the severity of the breach and who will take the lead investigating the breach (this will depend on the nature of the breach).

An investigation will be undertaken immediately and wherever possible within 24 hours of the breach being discovered/reported.

The Data Protection Officer will investigate the risks associated with the breach, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur using a risk matrix - see Appendix 1

The Data Protection Officer will then establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

The Data Protection Officer will identify who may need to be notified. The relevant procedures from those identified below will then be followed. Every incident will be assessed on a case by case basis.

7. Procedure – Breach notification where Changing Education act as a data processor for another data controller

Changing Education must report any personal data breach or security incident to the Data Controller without undue delay and within 72 hours as a maximum. These contact details are recorded in the Data Breach Register.

Changing Education provides the Controller with details of the breach.

The breach notification should be made by the Data Protection Officer by email and phone call to a named representative in the Controller's organisation.

A confirmation of receipt of this information should be requested. The Data Controller should confirm this in writing by email to the info@changingeducation.co.uk email address.

8. Procedure – Breach notification data controller to supervisory authority

The Data Protection Officer will determine if the supervisory authority (the Information Commissioner's Office (ICO) need to be notified in the event of a breach and reasons noted in the Data Breach Register

If the breach affects individuals in different EU countries, the ICO may not be the lead supervisory authority. The Data Protection Officer will also need to establish which European data protection agency would be the lead supervisory authority for the processing activities that have been subject to the breach.

We will assess whether the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach, by conducting an investigation and/or an impact assessment – See appendix 1. If we decide that we do not need to report the breach to the ICO we will justify and document our decision in the Data Breach Register

If a risk to data subject(s) is likely, the Data Protection Officer will report the personal data breach to the ICO without undue delay, and not later than 72 hours after becoming aware of it.

If the data breach notification to the ICO is not made within 72 hours, the Data Protection Officer will submit notification electronically with a justification for the delay.

If it is not possible to provide all of the necessary information at the same time we will provide the information in phases without undue further delay.

The following information needs to be provided to the supervisory authority:

- A description of the nature of the breach.
- The categories of personal data affected.
- Name and contact details of the Data Protection Officer
- Likely consequences of the breach.
- Any measures taken to address the breach.
- Any information relating to the data breach.
- Approximate number of data subjects affected.
- Approximate number of personal data records affected.

The breach notification should be made via telephone - **ICO: 0303 123 1113.** Alternatively, the Data Protection Officer may choose to report it online if they are still investigating and will be able to provide more information at a later date or if they are confident that the breach has been dealt with appropriately.

In the event the ICO assigns a specific contact in relation to a breach, these details are recorded in the Data Breach Register.

9. Procedure – Breach notification data controller to data subject

If the personal data breach is likely to result in high risk to the rights and freedoms of the data subject, Changing Education will notify those/the data subjects affected without undue delay and in accordance with Data Protection Officers' recommendation. This will be considered using the Data Breach Flowchart – see Appendix 2

A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. In any event the Data Protection Officer will document their decision-making process.

We will describe the breach in clear and plain language, in addition to information to assist the data subject. For example, if the event is a as result of an email hack then we will advise data subjects by email or letter.

The data controller takes subsequent measures to ensure that any risks to the rights and freedoms of the data subjects are no longer likely to occur.

If the breach affects a high volume of data subjects and personal data records, we will make a decision based on assessment of the amount of effort involved in notifying each data subject individually, and whether it will hinder our ability to appropriately provide the notification within the specified time frame. In such a scenario a public communication or similar measure informs those affected in an equally effective manner and will be considered by the DPO who's decision will be final.

If we have not notified the data subject(s), and the supervisory authority considers the likelihood of a data breach will result in high risk, Changing Education will communicate the data breach to the data subject by telephone or email.

We will document any personal data breach(es) within the Data Breach Register, incorporating the facts relating to the personal data breach, its effects and the remedial action(s) taken.

10. Documentation requirements

Data Breach Register: there is an obligation for us to document each incident "comprising the facts relating to the personal data breach, its effects and the remedial action taken".

Significant Event Report: we will utilise our Corrective Action report template. The purpose of this document is to understand the root cause of the incident, to capture the corrective actions and to identify any lessons learned to prevent the incident from occurring in the future.

11. Evaluation

Once the initial incident is contained, the Data Protection Officer will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken. This will be summarised in the Corrective Action Template.

Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

The review will consider various points, including but not limited to:

- Where and how personal data is held and where and how it is stored
- Where the biggest risks lie, and will identify any further potential weak points within its existing measures
- Whether methods of transmission are secure; sharing minimum amount of data necessary Identifying weak points within existing security measures
- Staff awareness and training
- Supplier involvement

12. Documentation requirements

Data Breach Register: there is an obligation for us to document each incident “comprising the facts relating to the personal data breach, its effects and the remedial action taken”.

Significant Event Report: we will utilise our Corrective Action report template. The purpose of this document is to understand the root cause of the incident, to capture the corrective actions and to identify any lessons learned to prevent the incident from occurring in the future.

13. Evaluation

Once the initial incident is contained, the Data Protection Officer will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken. This will be summarised in the Corrective Action Template.

Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

The review will consider various points, including but not limited to:

- Where and how personal data is held and where and how it is stored
- Where the biggest risks lie, and will identify any further potential weak points within its existing measures
- Whether methods of transmission are secure; sharing minimum amount of data necessary Identifying weak points within existing security measures
- Staff awareness and training
- Supplier involvement

14. Further Information

Further information and advice on this policy can be obtained from the Managing Director at info@changingeducation.co.uk

15. Appendix 1 – Risk matrix

Any incident must be graded according to the significance of the breach and the likelihood of those serious consequences occurring. The incident must be graded according to the impact on the individual or groups of individuals and not the organisation. It is advisable that incidents are reviewed by the Data Protection Officer when determining what the significance and likelihood a data breach will be.

No.	Likelihood	Description
1	Not Occurred	There is absolute certainty that there has been no adverse effect. This should be supported by an audit trail or forensic evidence
2	Not Likely	In cases where there is no evidence or audit trail that can prove that there has been no adverse effect
3	Likely	It is likely that there will be an adverse effect arising from the data breach
4	Highly Likely	There is almost certainty that at some point in the future an adverse effect will happen (eg. data will become available on the dark web, information misused by someone)
5	Occurred	There is a reported occurrence of an adverse effect arising from the breach (eg. unauthorised access to records, loss of credit card data etc

No.	Effect / Impact	Description
1	No adverse effect	There is absolute certainty that no adverse effect can arise from the breach
2	Potentially some minor adverse effect	A minor adverse effect must be selected where there is no absolute certainty but where the impact to the data subject would be minor
3	Potentially adverse effect	This could be the release of information to the general public which includes personal information
4	Potentially pain and suffering / financial loss	Loss of personal information relating to employment eg. personal records, bank information etc.
5	Catastrophic event	Loss of sensitive information (eg. medical data, any information related to children etc).

Risk Matrix

Yellow risks must be reviewed by the Data Protection Officer and potentially reported to the ICO

Red risks must be report to the ICO

All entries must be recorded on the data breach register.

Likelihood that rights of the data subject have been affected	Occurred	5	5	10	15	20	25
	Highly Likely	4	4	8	12	16	20
	Likely	3	3	6	9	12	15
	Not Likely	2	2	4	6	8	10
	Not Occurred	1	1	2	3	4	5
			1	2	3	4	5
			No adverse effect	Minor	Adverse	Serious	Catastrophic
			Severity (Impact)				

16. Appendix 2 – Summary of Procedure