PERSONAL DATA BREACH NOTIFICATION PROCEDURE

1. Scope

This procedure applies in the event of a personal data breach under Article 33 of the GDPR – *Notification of a personal data breach to the supervisory authority* – and Article 34 – *Communication of a personal data breach to the data subject*.

The GDPR draws a distinction between a 'data controller' and a 'data processor' in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. Each organisation should establish whether it is the data controller, or a data processor for the same data processing activity; or whether it is a joint controller.

2. Responsibility

2.1 All users (whether Employees/Staff, contractors or temporary Employees/Staff and third party users) of Luminate Education Group are required to be aware of, and to follow this procedure in the event of a personal data breach.

2.2 All Employees/Staff, contractors or temporary personnel are responsible for reporting any personal data breach to the Data Protection Officer /GDPR Owner.

3. Procedure – Breach notification data processor to data controller

3.1 Luminate Education Group reports any personal data breach or security incident to the data controller without undue delay where required.

3.2 NOTE: The data processing contract between the controller and the processor should have all the contact details and relevant procedures for making contact regarding data breaches

3.3 The breach notification is made by email or telephone.

3.4 A confirmation of receipt of this information is made by email or telephone.

4. Procedure – Breach notification data controller to supervisory authority

4.1 Luminate Education Group determines if the supervisory authority needs to be notified in the event of a breach.

4.2 Luminate Education Group assesses 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 reviewing or conducting the data protection breach against supervisory authority reporting matrix available on the ICO website. Self-assessment for data breaches | ICO

4.3 If you experience a personal data breach you need to consider whether this poses a risk to people. You need to consider the likelihood and severity of the risk to people's rights and freedoms, following the breach. When you've made this assessment, if it's likely there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report. **You do not need to report every breach to the ICO.**

4.4 There are legitimate reasons why a personal data breach might **not** need to be reported to the UK **Information Commissioner's Office (ICO)**.

The key test is whether the breach is **unlikely to result in a risk to the rights and freedoms of individuals**. If there is no likely risk, reporting to the ICO is generally not required, although the breach should still be documented.

Common reasons for not reporting include:

No personal data was actually exposed
For example, a system malfunction occurred, but no personal data was accessed, disclosed, altered, or lost.

The data was adequately protected
For example, a lost laptop contained strong encryption and there is no evidence the encryption was compromised.

The data was recovered before anyone could access it
For example, an email sent to the wrong recipient was recalled or securely deleted immediately before being viewed.

The recipient was authorised and trusted

For example, data was sent to the wrong person within the organisation, but they were already authorised to access the information or confirmed secure deletion.

The information was not sensitive and presents little risk
For example, limited contact details were disclosed with no realistic possibility of fraud, identity theft, discrimination, financial loss, or distress.

The breach was contained immediately
The organisation can demonstrate that effective action prevented any likely harm to affected individuals.

The data was already publicly available
In some circumstances, disclosure of information already lawfully in the public domain may not create additional risk.

Even when a breach is not reported, organisations should:

Record what happened.
Assess the risk.
Document why they concluded that reporting was unnecessary.
Retain evidence supporting that decision.

The ICO expects organisations to be able to justify their decision later if questioned.

4.5 If a risk to data subject(s) is likely, Luminate Education Group reports the personal data breach to the supervisory authority without undue delay, and not later than 72 hours.

4.6 If the data breach notification to the supervisory authority is not made within 72 hour's Luminate Education Group's Data Protection Officer / GDPR Owner submits it electronically with a justification for the delay.

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

4.8 The following information needs to be provided to the supervisory authority (GDPR REC 4.5): (Internal Breach Register and Notification Form)

4.8.1 A description of the nature of the breach.
4.8.2 The categories of personal data affected.
4.8.3 Approximate number of data subjects affected.
4.8.4 Approximate number of personal data records affected.
4.8.5 Name and contact details of the Data Protection Officer / GDPR Owner.
4.8.6 Consequences of the breach.
4.8.7 Any measures taken to address the breach.
4.8.8 Any information relating to the data breach.

4.9 In the event the supervisory authority assigns a specific contact in relation to a breach, these details are recorded in the Internal Breach Register GDPR REC 4.5.

4.10 The breach notification is made by email or telephone.

4.11 A confirmation of receipt of this information is made by email or telephone.

5. Procedure – Breach notification data controller to data subject

5.1 If the personal data breach is likely to result in high risk to the rights and freedoms of the data subject, Luminate Education Group notifies those/the data subjects affected immediately by using this form/in accordance with the Data Protection Officer / GDPR Owner recommendations.

5.2 The notification to the data subject describes the breach in clear and plain language, in addition to information specified in clauses 4.4 to 4.6 above.

5.3 Luminate Education Group takes measures to render the personal data unusable to any person who is not authorised to access it using software encryption. Egress System

5.4 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.

5.5 If the breach affects a high volume of data subjects and personal data records, Luminate Education Group will make a decision based on assessment of the amount of effort involved in notifying each data subject individually, and whether it will hinder Luminate Education Groups ability to appropriately provide the notification within the specified time frame. In such a scenario a public communication or similar measure will inform those affected in an equally effective manner.

5.6 If Luminate Education Group has not notified the data subject(s), and the supervisory authority considers the likelihood of a data breach will result in high risk, Luminate Education Group will communicate the data breach to the data subject

5.7 Luminate Education Group documents any personal data breach(es), incorporating the facts relating to the personal data breach, its effects and the remedial action(s) taken.

Document owner and approver

The Luminate Director of IT is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the GDPR.

A current version of this document is available to all members of the Luminate Education Group.

This procedure is issued on a version controlled basis.

Change History Record

Issue	Description of Change	Date of Policy
1.0	Initial issue	29/10/2017
1.1	Annual Review	01/12/2018
1.2	Annual Review – Responsibilities updated	17/10/2019
1.3	Annual Review – Luminate Education Group	14/11/2020
1.4	Annual Review	06/10/2021
1.5	Review and update	03/11/2022
1.6	Yearly review – no changes	03/11/2022
1.7	Annual review – added 5.3 Egress	14/10/2024
1.8	Annual Review – Added section 4.4 on the reasons and examples of when not to report a breach to the ICO.	25/06/2026