ACCESS CONTROL PROCEDURE

1 Luminate Education Group controls access to the IT network, business applications and information systems on the basis of business and security requirements.

2 Access control rules and access rights to each application, expressed in standard user profiles, for each user and group of users in each application are managed by the resource owner system administrator to ensure the business requirements are met by the controls.

3 The security requirements and access to each application is determined by the resource owner system administrator who identifies all information related to the application and the risks to that information. Security groups are created in the application.

4 Access to the IT network is managed through an automated request from Human Resources for each new starter to the IT Service Management (Help Desk FRESH System). All basic account information is provided by Human Resources (HR) IT network and email accounts are created by the IT Service Desk team.

5 The access rights to each application take into account:

a) The classification levels of information processed within that application and ensure that there is consistency between the classification levels and access control requirements.

b) General Data Protection Requirements (GDPR) and Data Protection (DPA 1988) and any contractual commitments regarding access to data or services.

c) The 'need to know' principle (i.e. access is granted at the minimum level necessary for the role).

d) 'Everything is generally forbidden unless expressly permitted'.

e) Requirements for formal authorisation of each access right to each IT system and business application.

f) Prohibit user initiated changes to user permissions.

g) Any privileges that users actually need to perform their roles, subject to it being on a need-to-use and event-by-event basis.

h) Roles with enhanced privileged access requirements.

i) Management of access rights in a large complex distributed IT network

ACCESS CONTROL POLICY

6 Luminate Education Group has standard user access profiles for common roles to access the IT Network.

7 User access requests, authorisation and administration are segregated by application.

8 Amendments to user access requests are subject to formal authorisation and review through the IT Help Desk FRESH System.

9 Each inactive IT network account is reviewed every 90 days to determine if the account is still required. Inactive accounts older than 90 days are disabled.

10 Termination of employment are subject to formal authorisation from HR with a leaver request automatically sent to the IT Service Desk team to process and remove all access. All Luminate Education Group assets (mobile phones, laptops, keys, staff ID cards) are returned at termination of the users employment contract.

11 Access to buildings is managed for each building. Access controls are managed and assigned in the student record system integrated in real time to the Access Control barrier system NET2.

Document owner and approver

The Luminate Group Director of IT is the owner of this document and is responsible for ensuring that this procedure is reviewed annually.

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

This policy is issued on a version controlled basis.

Change History Record

Issue	Description of Change	Date of Policy
1.0	Initial Draft	17/08/2021
1.1	Review completed	03/10/2022
1.2	Review completed- No changes	12/11/2023
1.4	No amends	05/10/2024
1.5	Annual Review – No Amends	08/07/2026