Portal Access Rights Policy and Procedure

Version 1.1

Policy Author	Geoffrey Tanti	**Designation**	Senior Manager IT	**Dept.**	Information Department
Policy Reviewer	Administration Board	**Designation**	N/A	**Dept.**	N/A
Policy Approver	Administration Board	**Effective Date**	15/03/2024		

1. Policy Statement

1.1 This policy establishes guidelines for granting access rights to the Institute for Education Online Portal. The objective is to ensure secure access, protect sensitive information, and facilitate a streamlined experience for authorised users.

2. Principles

2.1 The IfE assigns the minimum level of access rights necessary for users to perform their duties effectively. Each role has specific permissions tailored to its responsibilities and privileges.

2.2 The IfE avoids granting excessive permissions that could potentially compromise security or privacy.

2.3 The IfE fine-tunes access rights to specific functions, features, or resources within the LMS. Provide administrators with the ability to customize permissions at a granular level to meet the diverse needs of users and courses.

2.4 The IfE ensures that access rights and permissions align with relevant regulatory requirements, such as data protection laws. Protect the privacy and confidentiality of user data by enforcing strict access controls.

3. Aims and objectives

3.1 The aims and objectives of this Policy are the following:

- Ensure data security and compliance.
- Enhance user experience and satisfaction.
- Support organisational efficiency and scalability.
- Define access levels, permissions, and user groups.
- Conduct regular access audits and reviews.
- Continuously review and update access policy for optimisation and improvement.

4. User Access Request

4.1 All requests for Portal access must be submitted through email seeking approval from the CEO.

4.2 Requests should include the user's full name, position, department, required access and justification for access.

5. Authorisation

5.1 Access requests will be granted by the IT Department who are the portal administrators upon receipt of an email containing the approval from the CEO.

5.2 Authorisation will be based on the user's role, responsibilities, and the principle of least privilege (bare necessary).

6. User Categories

6.1 Users will be categorised into appropriate roles such as course participants, or staff. Staff can then be assigned roles such as Learning Programmes Development Experts, administrators, etc or any other relevant designation.

6.2 Each role will be assigned specific access rights aligned with the user's responsibilities within the IfE on a need-to-know basis.

6.3 User categories clearly outline the permissions associated with each access level.

7. User Training

7.1 The Head/ Senior Manager of each department should ensure that users under their responsibility who have been granted access receive the necessary training on their responsibilities and proper use of the portal by the IT department.

7.2 Users are to be informed by the IT department about the available resources and documentation to guide them in using the portal functionalities effectively.

8. Periodic Access Reviews

8.1 The IT department is to conduct regular reviews of user access rights to ensure alignment with current roles and responsibilities.

8.2 The respective departments are to inform the IT department to remove or modify access for users whose roles have changed or are no longer applicable immediately.

9. Password Security

9.1 Users are encouraged not to share login credentials and report any suspected security breaches promptly to the data protection officer and the IT department through email.

10. Account Deactivation

10.1 The IT department is to deactivate user accounts promptly upon employee resignation.

10.2 The IT department is to keep a log of deactivated accounts for audit purposes.

11. Data Privacy

11.1 Portal Users are to ensure compliance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act (Cap 586) which regulate the processing of personal data when handling user information within the portal.

11.2 Regularly review and update privacy settings to safeguard sensitive data.

12. Incident Reporting

12.1 The IT department is to investigate and take corrective actions in the event of a security incident.

13. Relevant documents

- Data Protection Act
- Data Protection Policy
- General Data Protection Regulation
- Reporting Security Incidents, Breaches, or Unauthorised Access Procedure

14. Version history

Originator	Version	Dates	Changes Done
Senior Manager IT	1.0		Initial Release
QA Dept.	1.1	30/04/2024	Updated links