Document Reference Number	**UoG/ILS/IASC/ToR/ 001**
Date	October 2022
Title	Information Assurance and Security Committee Terms of Reference
Author	Information Security and Compliance Manager
Owning Department	Information and Library Services
Version	4.0
Approval Date	12.10.22
Review Date	11.10.23
Approving Body	IT Management Board

Version Control

Version	Date	Author	Rationale
3.0	30.09.20	ISCM	
4.0	12.10.22	ISCM	Membership and duties updated. New document template applied.

Information Assurance & Security Committee

1. Constitution

1.1 The Vice-Chancellor's Group (VCG) has established an Information Assurance & Security Committee (IASC), which reports to the IT Management Board (ITMB).

1.2 IASC will liaise with the Capital Programmes Board, when necessary, to ensure they support each other and do not duplicate efforts.

2. Scope

2.1 IASC leads the University's information programme. It ensures good information security governance across the University.

2.2 IASC oversees the University's data protection responsibilities including but not limited to compliance with the data protection legislation, including the effective removal or archiving of data when it is no longer required operationally.

2.3 IASC reviews the University's information security management system (ISMS) and oversees the maintenance of its information & cyber security certification.

3. Membership

3.1 The membership shall be as follows:

Ex Officio

- Academic member appointed by VCG *(Chair)*
- Executive Director and Chief Information Officer (ILS) *(Vice-Chair)*
- University Secretary *(Vice-Chair)*
- Head of Digital Strategy, Security & Compliance (ILS)
- Information Security & Compliance Manager (ILS)
- Head of Infrastructure (ILS)
- Cyber Security Manager (ILS)
- Head of Service Delivery (ILS)
- Legal Advisor (Information Compliance and Contracts) (VCO)
- Greenwich Students Union CEO or nominee

Other Members

- Member from Student & Academic Services
- Member from Human Resources
- Laboratories & Technical Services Director (FES)
- Associate Dean – Student Success (GBS)
- Faculty Operating Officer (FEHHS)
- Drill Hall Library representative

The Other Members of the Committee shall normally be appointed annually to the Committee by the Chair.

4. Attendance at meetings

4.1 At the discretion of the Chair, other staff who are not members of the Committee may be invited to attend on an ad hoc basis for specific items where their attendance can inform and support the Committee.

5. Delegated Authority

The Committee is authorised by the Vice Chancellor's Group to approve the following:

5.1 Plans to implement the information security strategy;

5.2 Regularly review key risks within the Committee's remit. Approve action plans to take advantage of opportunities and mitigate risk;

5.3 Good practice and procedures, ensuring adherence to legal and regulatory requirements and best practice;

6. Other Duties

The other duties of the Committee shall be to:

6.1 Develop and review the University's information security strategy. Make recommendations to ITMB.

6.2 Oversee the implementation of the University's information security strategy and plans.

6.3 Improve information security capabilities and cyber resilience through initiatives that are reflective of best practice. Make recommendations to ITMB for resources to enhance support;

6.1 Review information security and data protection requirements for projects undertaken by ITMB, the Capital Programmes Board and any other Boards charged with delivery of a University sub-strategy or enabling strategy. Recommend projects to enhance information security to the appropriate Board in accordance with the University Delegation Framework and assist ITMB in implementation as required;

6.2 Review the University's information security management system (ISMS) and the maintenance of its information & cyber security certification including:

- Changes in internal/external issues relevant to ISMS
- Feedback on information security performance, including audit results, non-conformities and corrective action, and fulfilment of security objectives
- Results of risks assessments and risk treatment plans
- Opportunities for continual improvement of ISMS

6.3 Oversee information and records retention, ensuring consistency and monitoring compliance;

6.4 Review and develop policies related to the University's information security. Ensure adherence to legal and regulatory requirements and best practice. Make recommendations to ITMB for approval;

6.5 Review relevant new legislative requirements and regulation, assess their implications and where necessary consider changes to or new policies and procedures;

6.6 Monitor and audit compliance with information security policies, procedures and statutory requirements. Report to ITMB on significant non-compliance issues;

6.7 Review information security and data protection incidents, lessons learned and make recommendations or take action, as necessary;

6.8 Regularly scan the Higher Education sector and other organisations for trends, issues, best practice and innovation, which are worth considering for implementation.

6.9 Promote a culture whereby students and staff are aware of information security and where to get necessary information. Ensure good communications to achieve this;

6.10 Provide a forum for sharing good practice about information security across the University; and

6.11 Ensure active consideration of equality, diversity, inclusion and sustainability in the conduct of the Committee's business.

7. Standing Orders

7.1 The Committee must adhere to the Standing Orders for Academic and Executive Committees.

8. Meeting Frequency

8.1 The committee shall meet every 2 months.