

LASE Information Assurance and Security Committee

1. Constitution

- 1.1 The Vice-Chancellor has established an Information Assurance and Security Committee (IASC), which reports to the Estates and Digital Board (EDB).

2. Scope

- 2.1 IASC leads the University Group's information security programme. It ensures good information security governance across the University Group;
- 2.2 IASC oversees the University Group's data protection responsibilities, including (but not limited to) compliance with data protection legislation, and records management;
- 2.3 IASC reviews and contributes to the University Group's information security management system (ISMS) and oversees the maintenance of its information and cyber security certifications.

3. Membership

- 3.1 The membership shall be as follows:

Ex Officio

- Group Chief Information Officer (Vice-Chair)
- Director of IT Services
- Associate Director (Office of the CIO) (Greenwich)
- Principal Strategy and Information Security Officer (Greenwich)
- Group University Secretary (Vice Chair)
- General Counsel (Greenwich)
- Data Protection Officer (Kent)
- Representative from Student Life
- Representative from People Directorate
- Representative from LASE University Group Students' Union

Other members

- Chair appointed by the Vice-Chancellor

- 3.2 For the Information Assurance and Security Committee, the quorum is one third of the current membership.

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. Frequency and Format of Meetings

- 5.1 The Committee shall normally meet every two months. The Chair may call additional meetings as necessary.

- 5.2 Meetings will be held either in-person, via electronic means (e.g. online) or via a hybrid format, as determined by the Chair. The Committee may also decide matters by email circulation. In between meetings of the Committee, the Chair of the Committee is empowered to decide matters falling within the Committee's remit by chair's action; matters decided by chairs action shall be reported to the next meeting of the Committee.

6. Delegated Authority

Under the University Group's Executive Delegation Framework, the Committee is authorised by the Vice-Chancellor to approve:

- 6.1 Plans to implement LASE's information security strategy and develop integration across the University Group;
- 6.2 Action plans to take advantage of opportunities and mitigate risks within the committee's remit;
- 6.3 Good practice, standards and procedures, ensuring adherence to legal and regulatory requirements and best practice;

7. Other Duties

The other duties of the Committee shall be to:

- 7.1 Review and contribute to the development of the University's Group's information security strategy, making recommendations to Estates and Digital Board where appropriate;
- 7.2 Oversee the implementation of the University Group's information security strategy and plans;
- 7.3 Regularly review the University Group's information security risk register, assess emerging threats, and monitor the effectiveness of current mitigation strategies;
- 7.4 Improve information security capabilities and cyber resilience through initiatives that reflect best practice;
- 7.5 Review information security and data protection requirements for IT projects approved under the University Group's Delegation Framework, making recommendations for improvement where appropriate;
- 7.6 Review and contribute to the continual improvement of the University Group's information security management system (ISMS) and the maintenance of its information and cyber security certification including:
 - Changes in internal/external issues relevant to ISMS
 - Feedback on information security performance, including audit planning and 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
- 7.7 Oversee information and records retention, ensuring consistency and monitoring compliance. Ensure the effective removal or archiving of data when it is no longer required operationally;
- 7.8 Review and contribute to the development of regulations and policies related to information security and compliance with data protection legislation. Ensure adherence to legal and

regulatory requirements and best practice. Make recommendations to Estates and Digital Board for approval;

- 7.9 Review relevant new legislative requirements and regulations, assess their implications and where necessary consider changes to or new policies and procedures;
- 7.10 Monitor the University Group's adherence to external compliance frameworks (e.g., ISO 27001, Cyber Essentials);
- 7.11 Monitor and audit compliance with information security policies, procedures and statutory requirements. Report to Estates and Digital Board on significant non-compliance issues;
- 7.12 Oversee and review the effectiveness of the University Group's Cyber Security Incident Response Plan (CSIRP) and lessons learnt from emergency/incident response exercises. Review information security and data protection incidents, lessons learnt and make recommendations, or take action, as necessary;
- 7.13 Regularly scan the Higher Education sector and other organisations for trends, issues, best practice and innovation which are worth considering for implementation;
- 7.14 Guide the strategic approach for security awareness programmes and training for staff and students. Promote a culture whereby students and staff are aware of information security and where to get necessary information. Ensure good communications to achieve this;
- 7.15 Provide a forum for sharing good practice about information security across the University Group;
- 7.16 Ensure active consideration of equality, diversity, inclusion and sustainability in the conduct of the Committee's business;
- 7.17 Have particular regard to the importance of freedom of speech and academic freedom in the Committee's business, acting in accordance with the commitments in the University Group's Freedom of Speech Code(s) of Practice.

8. Reporting Procedures

8.1 The Information Assurance and Security Committee reports as follows:

- **Frequently:** through provision of the minutes of each meeting to the next meeting of the Estates and Digital Board. Additionally, an oral report (normally by the Chair/Vice-Chair) is delivered as an item on EDB agendas;
- **Periodically:** via other policies, reports, plans and progress updates which it reviews and/or recommends for approval within the business cycle and its terms of reference;
- **Ad hoc:** where urgent Group-wide matters require direct escalation to the EDB or VCE for decision or discussion.

9. Secretarial Arrangements

9.1 The meeting will be clerked by the Group's University Secretary or their nominee.

10. Review

- 10.1 The Committee will review its own effectiveness annually and in greater depth at a minimum of every three years. Reviews may be performed as part of wider governance effectiveness reviews;
- 10.2 These terms of reference will be reviewed annually to ensure their effectiveness and any amendments recommended to VCE for approval.

11. Version Control

Document Reference Number	TBC
Title	Information Assurance and Security Committee Terms of Reference
Owning Department	Vice-Chancellor's Office
Version	1.1
Approval Date	5 October 2026
Approving Body	Vice-Chancellor's Executive
Review Date	October 2027
Classification	Non-Sensitive

Version	Last Modified	Last Modified By	Document Changes
1.1	09/10/26	Group University Secretary	Minor changes approved by chair's action following discussion at VCE