INFORMATION SECURITY POLICY

Introduction

1. The University recognises the importance of information governance and security management. This policy sets out the corporate intention for the safe management of personal data and business information (Information Assets) the University handles, whether it be printed or written on paper, stored electronically, transmitted by post or using electronic means, stored on tape or disk drives, or spoken in conversation.

2. The University is responsible for the care and welfare of its students, employees, faculty and contractors data and information. As a result, much of the information we come into contact with, store and process, needs to be secure, with the potential for significant harm to be caused if that information were disclosed to people who should not have access to it, or were it not available to people who needed it.

3. The University will endeavour to:

   a) Protect the Information Assets from all threats, whether internal or external, deliberate, or accidental, to ensure business continuity, minimise organisational damage and maximise return on investments and organisational opportunities.

   b) Safeguard the information the University holds about the people we care for, including students, employees, contractors, and visitors.

   c) Meet our obligations under relevant legislation including the Data Protection Act 2018

Scope

4. This policy applies to all Information Assets handled by the University, its employees, contractors and third parties working on our behalf.

5. If an employee changes role or their contract is terminated, their line manager must follow the steps in the SLAM Process. This ensures that access to information systems is maintained and appropriate.

6. All employees are responsible for helping to protect Information Assets from loss of confidentiality, integrity, and availability.

7. The University has measures in place to protect Information Assets, such as technology-based safeguards, adopting 'privacy by design' and these measures are reviewed on a regular basis using tools such as Data Protection Impact Assessments (DPIA).

Roles and Responsibilities

8. The University Board is ultimately responsible for ensuring that information security is properly managed, under guidance from the Head of IT and external consultants.

9. The IT Data Governance Committee (ITDGC) is responsible for approving and authorising the issue of the Information Security Policy and approving opportunities for continuous improvements.

10. Agreements with third parties involving accessing, processing, communicating, or managing University Information Assets, or information systems, must cover all relevant security requirements, and be covered in contractual arrangements.

11. Any material changes in this policy or associated policies will be shared with our students and other relevant/interested parties.

12. All managers are directly responsible for implementing the Information Security Policy within their organisational areas. All employees are responsible for adhering to this policy, and for reporting suspected breaches or incidents to the IT department or DPO.

Compliance

13. The University has established this policy to promote information security and compliance with relevant Data Protection Legislation (the UK General Data Protection Regulations and Data Protection Act 2018) and regards any breach of information security requirements as a serious matter which may result in disciplinary action.

14. Relevant legislation includes, but is not limited to:

- The Computer Misuse Act (1990).
- The Data Protection Act (2018).
- The Regulation of Investigatory Powers Act (2000).
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations (2000).
- The Freedom of Information Act (2000).
- The UK General Data Protection Regulations (2018).
- Family Educational Rights and Privacy Act (FERPA).
- California Consumer Privacy Act (CCPA)
- Virginia Consumer Data Protection Act (VCDPA)
- Colorado Privacy Act (CPA)
- Nevada Revised Statutes Chapter 603A (Nevada privacy law)
- Connecticut Personal Data Privacy and Online Monitoring
- Utah Consumer Privacy Act

Supporting Policies and Procedures

15. Supporting policies and procedures are published on the intranet.

16. These policies and procedures give specific guidance about employee obligations when handling and processing organisational Information Assets, and all employees should familiarise themselves with this guidance on a regular basis.

Objectives

17. The University sets itself the following objectives:

- Meet legislative requirements.
- Minimise the impact of or eliminate any information security incidents.
- Maintain a strong employee and student alignment to standards and policies.
- To ensure our employees and students have a high level of data protection & information security awareness.

Change Management

18. The ITDGC and Change Advisory Board (CAB) exists to provide better governance over information change and data projects. The ITDGC is responsible for ensuring effective management of information risk and providing the University with assurances that best practice mechanisms for information governance are in place within the organisation.

19. Change is defined as anything that happens within the University that can introduce risk, or change an existing risk with regards to information and data protection, examples are:

a) New or changed information processing activity.
b) New or changed information system.

20. Frequent change sources within the University are as follows:

a) Incident response
b) Systems patching
c) Policy and process change

Risk Treatment

21. The degree of security control required depends on the sensitivity, or criticality of the Information Asset. The first step in determining the appropriate level of security is a process of risk assessment, in order to identify and classify the nature of the Information Asset held, the adverse consequences of security breaches, and the likelihood of those consequences occurring.

22. Where appropriate, Information Assets must be labelled and handled in accordance with their criticality and sensitivity.

23. Information security risk assessments must be repeated periodically and carried out as required during the operational delivery and maintenance of the University infrastructure, systems and processes.

Personal Data

24. Personal data must be handled in accordance with the Data Protection Legislation and in accordance with the University Data Privacy Policy.

25. The Data Protection Legislation requires that appropriate technical and organisational security measures are adopted to mitigate against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

26. A higher level of security must be provided for special categories of personal data which is defined in the Data Protection Legislation as data relating to ethnic or racial origin, religious beliefs, physical or mental health, sexual life, political opinions, trade union membership, or the commission or alleged commission of criminal offences. There are further examples of special category data available on the Information Commissioner's Office (ICO) website.

Business Continuity

27. An IT disaster recovery plan is in place which details how the University can continue to operate and access systems should a disaster prevent access to the Chiswick campus.

28. The disaster recovery plan forms part of the University's overarching Emergency Management Plan which is published on the University Website, with confidential aspects being separately transmitted to relevant parties.

Protection of confidential information

29. Identifying confidential information is a matter for assessment in each individual case. Broadly, however, information will be confidential if it is of limited public availability; is confidential in its very nature; has been provided on the understanding that it is confidential; and/or its loss or unauthorised disclosure could have one or more of the following consequences:

    a) Financial loss.
    b) Reputational damage.
    c) An adverse effect on the safety or well-being of those associated with the University.

Storage

30. Information must be kept secure, using, where practicable, University secure online applications rather than local hard disks, and have an appropriate level of security.

31. All mobile workstations must have disk encryption enabled.

Access

32. Information must be stored in such a way as to ensure that only authorised persons can access it.

33. All users must be appropriately authenticated. Users must follow good security practices in the selection and use of passwords.

34. Suitable password expiry and complexity rules will be enforced according to the level of access granted and the sensitivity of data handled.

35. Where necessary, additional forms of authentication will be required.

36. To allow for potential investigations, access records must be kept for a period of time as considered appropriate.

37. Physical access will be monitored, and access records maintained.

Remote Access

38. Any remote access must be controlled by secure access control protocols using appropriate levels of encryption and authentication.

39. Where remote access is required, access controls must be used in accordance with University policies.

Copying

40. The number of copies made of Information Assets, whether on portable devices or media or in hard copy, must be the minimum required, and, where necessary, a record kept of their distribution. When no longer needed, the copy must be deleted or, in the case of hard copies, destroyed.

41. Hard copies should be stored in a secure location such as a safe, or lockable storage box.

Disposal

42. Policies and procedures must be in place for the secure disposal/destruction of Information Assets, both in digital and electronic form. This includes destruction by means of cross shredding, deletion, and secure destruction.

Use of portable devices or media

43. Procedures must be in place for the management of removable media in order to ensure that they are appropriately protected from unauthorised access.

44. Portable devices, or media storage locations, should be encrypted where possible, and/or password protected.

45. The passphrase of any encrypted portable device must not be stored with the device.

46. Personal data must not be transferred by removable media.

Exchange of Information and use of Email

47. Controls must be implemented to ensure that electronic messaging is suitably protected.

48. Email must be appropriately protected from unauthorised use and access.

49. Email must only be used to transfer Information Assets where the recipient is trusted, and appropriate safeguards have been taken. Information Asset files should be password protected or shared using encrypted links where the personal data or confidential information is sensitive.

50. Where feasible, Information Assets will be shared using encrypted links (from our internal corporate file solution) to ensure that the data is encrypted in transit. Only individually authorised users are able to do this, and they have enhanced authentication measures imposed.

Backup

51. IT must ensure that appropriate backup and system recovery procedures are in place. Backup copies of all important Information Assets must be taken and tested regularly commensurate with the criticality of the system.

Hard Copies

52. Documents containing University Information Assets should be marked appropriately.

Physical Storage

53. Wherever practicable, documents with personal data and confidential information must be stored in locked cupboards, drawers, or cabinets.

54. Keys to cupboards, drawers or cabinets must not be left on open display when the room is unoccupied.

Transmission

55. If personal data or confidential information in documents are sent by external post, they must be sent by a form of recorded delivery. The sender must ensure that the envelope is properly secured.

Failure to Comply

56. Incompetence, misconduct and/or performance issues will be addressed through standard HR policies.

VERSION MANAGEMENT

Responsible Department: IT			
Approving Body: Operations Committee			
Version no.	**Key Changes**	**Date of Approval**	**Date of Effect**
1.0	Initial Version	11/04/2022	11/04/2022
1.1	Updated to reflect move to CP	25/05/2023	22/06/2023
1.2	Minor Change: Initial Version formatted according to current policy template	01/10/2023	01/10/2023
	Restricted Access? *Tick as appropriate*: Yes ☐ No☒		