UCA

university for the **creative arts**

Information Security Policy
Version 2.1

Approved by: Leadership Team

Date approved: 17/11/2014

Review period: Annually

Date reviewed:

Owner: University Secretary

Version no	**Status/purpose of change**	**Author**	**Date**
1.0	Final version approved by Executive	Marion Wilks	29/06/09
2.0	Approved by Leadership Team. Compliance with PCI standard.	Marion Wilks	28/1/13
2.1	Approved following review by Leadership Team. Compliance with PCI standard 3.	Marion Wilks	17/11/14

University for the Creative Arts

Introduction

1. The University recognises that information and information systems are valuable assets which play a major role in supporting the University's strategic objectives. Information security is important to the protection of the University's reputation and the success of academic and administrative activities. It is also an integral part of the information sharing which is essential to academic and corporate endeavour. The management of personal and financial data has important implications for individuals and is subject to legal obligations and security standards. The consequences of information security failures can be costly and time-consuming.

2. The Information Security Policy sets out appropriate measures through which the University will facilitate the secure and reliable flow of information, both within the University and in external communications. It comprises this document, which sets out the principles and framework, and a set of subordinate and specific policies and guidelines addressing individual aspects of security (listed in Appendix A). The approach is based on recommendations contained in British Standard 7799 - A Code of Practice for Information Security Management and in the UCISA Information Security Toolkit.

Objectives

3. The objective of the Information Security Policy is to ensure that all information and information systems upon which the University depends are adequately protected to the appropriate level.

Scope

4. The Information Security Policy applies to information in all its forms. It may be on paper, stored electronically or held on film, microfiche or other media. It includes text, pictures, audio and video. It covers information transmitted by post, by electronic means including through wifi and by oral communication, including telephone and voicemail. It applies throughout the lifecycle of the information from creation through storage and utilisation to disposal. Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory or contractual obligations.

5. The policy applies to all staff of the University. With regard to electronic systems, it applies to the use of University owned facilities and privately/externally owned systems when connected to the University network directly or indirectly. ('Owned' is deemed to include leased, rented or on-loan). The policy applies to all University owned/licensed data and software, be they loaded on University or privately/externally owned systems, and to all data and software provided to the University by sponsors or external agencies.

Policy statement

6. The University is committed to protecting the security of information through the preservation of:
    - confidentiality: protecting information from unauthorised access and disclosure
    - integrity: safeguarding the accuracy and completeness of information and processing methods
    - availability: ensuring that information and associated services are available to authorised users when required

7. The University will develop, implement and maintain policies and procedures to achieve appropriate levels of information security. These will cover the range of elements that need to be addressed in the management of information security, in particular the following policy requirements:

Authorised use

8. University information systems are provided to support the University's activities including learning, teaching, research, administration and approved business activities. Only staff and other persons authorised by appropriate University authority are entitled to use the University's information systems.

Acceptable use

9. All users have an obligation to use information and information systems responsibly. Rules are defined in the Acceptable Use Policy owned by the IT Services Department.

Monitoring and privacy

10. The University respects the privacy of its users and there is no routine monitoring of e-mail content or individual Web access other than to locate the storage of payment card personal account numbers to ensure adherence to the Payment Card Industry Data Security Standard. The University reserves the right to make interceptions in certain circumstances under the terms of the Regulation of Investigatory Powers Act.

Protection of software

11. All users must comply with the Copyright, Designs and Patents Act 1988 under which it is an offence to copy software or licensed products without the permission of the owner of the copyright.

Retention and disposal of information

12. All staff have a responsibility to consider security when using, storing and disposing of information in the course of their work. The University has determined retention periods for certain kinds of information and departments should establish procedures appropriate to the information held and processed by them, and ensure that all staff are aware of those procedures.

Virus control

13. Staff must not knowingly introduce a virus or take deliberate action to circumvent precautions taken to prevent the introduction of a virus.

Business continuity

14. The University will implement, and regularly update, a business continuity management process to counteract interruptions to normal University activity and to protect critical processes from the effects of failures or damage to vital services or facilities.

Legal and contractual requirements

15. The University will abide by all UK legislation and relevant legislation of the European Community related to the holding and processing if information. This includes the following Acts and the guidance contained in the Information Commissioner's Codes of Practice:
    - Computer Misuse Act 1990
    - Copyright Designs and Patents Act (1988)
    - Data Protection Act 1998
    - Freedom of Information Act (2000)
    - Human Rights Act (1998)
    - Regulation of Investigatory Powers Act (2000)
    - Protection of Freedoms Act 2012

16. The University will also comply with all contractual requirements related to the holding and processing of information:
    - JANET Acceptable Use Policy issued by UKERNA
    - Code of Conduct on the Use of Software and Datasets issued by JISC
    - The terms and conditions of licences and contracts
    - The terms and conditions of authentication systems, e.g. Athens
    - Payment Card Industry Data Security Standard

Responsibilities

Policy owners

17. The Leadership Team is responsible for approving the Information Security and for monitoring its implementation. Responsibility for maintaining the policy resides with the Registrar & Secretary supported by the Head of IT Services

18. Each subordinate policy has a Nominated Officer responsible for updating of that element of policy (see Appendix A). The Nominated Officer will promote awareness of and compliance with the policy, provide advice and guidance on good practice relating to the policy, and bring forward revisions to the policy as necessary.

Information asset owners

19. 'Owners' of information assets (such as student or staff records) are responsible for defining the use of those assets and maintaining appropriate security measures. An 'Owner' is normally deemed to be the Director or Head of the Department which owns and manages the business process utilising that information. The exception is the core student record, which though 'owned' by the Head of Student Administration is shared with other process owners, such as Library & Student Services and Accommodation Services. A list of owners of key information assets is provided in Appendix A to the Information Handling Policy.

Systems administrators

20. Those responsible for information systems, for example database and IT systems administrators, must ensure that appropriate security arrangements are established, maintained and updated including ensuring vendor-supplied security patches are installed within one month of release. Those responsible for information systems must also carry out periodic risk assessments of their security controls in place. They must take into account changes in business requirements, changes in technology and any changes in the relevant legislation and revise their security arrangements accordingly.

21. Access by software vendors of systems by remote access to enable maintenance and support will be granted only when required.

Information users

22. Executive Deans, Directors and Heads of Departments are responsible for ensuring that information and information systems used within their faculties/departments are managed and used in accordance with information security policies, protocols and guidelines. Executive Deans, Directors and Heads of Departments are required to carry out periodic risk assessments and establish and maintain effective contingency plans.

23. Everyone granted access to University information systems has a personal responsibility to ensure that they, and others who may be responsible to them, are aware of and comply with the policies, codes of conduct and guidelines.

24. Each individual is responsible for protecting the University's information assets, systems and infrastructure, and will protect likewise the information assets of third parties whether such protection is required contractually, legally, ethically or out of respect for other individuals or organisations.

Breaches

25. All staff other authorised users should report immediately any observed or suspected security incidents where a breach of the University's security policies has occurred, any security weaknesses in, or threats to, systems or services. Reports should be made to the Executive Dean/Director/Head of Department or, where the IT infrastructure is involved, via the IT Services Help Desk to the Head

of IT Services. Executive Deans/Directors/Head of Department or the Head of IT Services should investigate the report and, in the event that a weakness in or breach of security is found, should report this to the University Secretary.

26. Regular internal vulnerability testing, including the identification of unauthorised wireless access points will be carried out by the IT department on a quarterly basis.

Policy awareness and disciplinary procedures

27. The Information Security Policy will be made available to all staff via the document store. Staff, authorised third parties and contractors given access to the University information systems will be advised of the existence of the relevant policies, codes of conduct and guidelines. Users will be asked to confirm that they understand the policy before being given access to university systems.

28. Failure to comply with the Information Security Policy may lead to suspension or withdrawal of an individual's access to information systems.

29. Failure of a member of staff to comply with the Information Security Policy may lead to the instigation of the relevant disciplinary procedures as specified in their terms and conditions of employment and, in certain circumstances, legal action may be taken. Minor infringements, such as causing inconvenience to other users, may lead to a verbal or written warning. Major infringements, such as major breach of confidentiality, harassment, or illegal activities may lead to a formal warning, suspension or termination of employment. This is not an exhaustive list of possible offences and the University will determine whether a case is minor or major having regard to all the circumstances of each incident.

30. Failure of a contractor to comply could lead to the cancellation of a contract and, in certain circumstances, legal action may be taken.

Information security education and training

31. The University recognises the need for all staff and other users of University systems to be aware of information security threats and concerns, and to be equipped to support University security policy in the course of their normal work. Appropriate training or information on security matters will be provided for users and departments will supplement this to meet their particular requirements.

Maintenance

32. The Information Security Policy will be monitored by the Leadership Team and reviewed once a year and updated as needed to reflect changes to University objectives and the risk environment.

33. The Registrar & Secretary will report on a summary and exception basis, will notify issues and bring forward recommendations.

Acknowledgments

This policy includes material adapted from policies developed by Imperial College, Warwick and Oxford Brookes University. All institutions have kindly agreed to this use of their material and their assistance is acknowledged and appreciated.

Appendix A: Information security and related policies

Title	**Policy Owner**	**Status**
Information Security Policy and Infrastructure		
Information Security Policy	Registrar & Secretary	Published
Information Handling Policy	Registrar & Secretary	Published
Information Security: mobile and remote working policy and guidelines	Registrar & Secretary	Published
Electronic Mail Policy	Head of IT Services	Published
IT Use Policy	Head of IT Services	Published
Business Continuity Management and Planning	Head of IT Services	Planned
Personnel and Third Parties	Registrar & Secretary /Dir of HR	Published
System and Network Management	Head of IT Services	Planned
Software Management	Head of IT Services	Planned
Related Policies		
Data Protection Policy	Registrar & Secretary	Published
Records Management Policy	Registrar & Secretary	Published
Receiving Payments using a Payment Card	Compliance Accountant	Published