University for the Creative Arts

Information Handling Policy

Version 1.0
Author: Marion Wilkes
Date: 20 July 2009

Document History

Version History

1.0	20 July 2009	Approved for publication by the IS Board after E&FC approval in June 2009

Purpose and Scope

1. This policy sets out the need to define classes of information handled by the organisation and the requirements for the storage, transmission, processing and disposal of each. Requirements may include confidentiality (in handling, storage and transmission), integrity (e.g. validation processes) and availability (e.g. backups). This policy should be familiar to all staff dealing with information.

Responsibility for and classification of information assets

2. Information assets include, but are not limited to, data in databases and data files, system documentation, user manuals, training materials, operational and support procedures, continuity plans and archived information.

3. Each asset has a nominated owner who is assigned responsibility for defining appropriate use of the asset and maintaining appropriate security measures. A list of owners of key information assets is provided in Appendix A.

4. Information should be classified according to sensitivity of the data. Classifications and associated protective controls for information should take account of organisational needs for sharing or restricting information, and the business impacts associated with such needs, e.g. unauthorised access or damage to the information. In general, the classification given to information is a shorthand way of determining how this information is to be handled and protected. Individual pieces of data or information may be assigned more than one of the classifications given in paragraph 4, e.g. personal confidential.

5. The classification used by the University, consistent with terms used in the Data Protection Act (DPA) is.

Unclassified		Information which is not confidential or personal and which may be disseminated within the organisation and without. An example is the Prospectus.
C	Personal	Data which enables an individual to be identified; data which relates to or is about an identifiable individual. Such data may be processed lawfully by the University provided that staff comply with the DPA and the University's notification.
L A S S I F I	Personal Sensitive	Personal data consisting of information as to— (a) the racial or ethnic origin of the data subject, (b) their political opinions, (c) their religious beliefs or other beliefs of a similar nature, (d) whether they is a member of a trade union (within the meaning of the [1992 c. 52.] Trade Union and Labour Relations (Consolidation) Act 1992), (e) their physical or mental health or condition, (f) their sexual life, (g) the commission or alleged commission by them of any offence, or (h) any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings. Such data may be processed lawfully by the University provided that staff comply with the DPA and the University's notification.
E D	Confidential	Data which may or may not be personal and which should not be disclosed, except to those to whom the information owner sees fit and gives authority. Examples might be the University's application statistics or a set of anonymised student mark profiles prepared for an assessment board.

6. Information and outputs from systems handling classified data should be labelled according to their classification. Information can cease to be sensitive or critical after a certain period, for example, when the information has been made public. These aspects should be taken into account, as over classification can lead to unnecessary additional expense.

7. The responsibility for defining the classification of an item of information and for periodically reviewing the classification rests with the nominated owner of the information.

Information protection – equipment disposal, desk, screen and general

8. When permanently disposing of equipment containing storage media all sensitive data and licensed software will be irretrievably deleted before the equipment is moved off site using procedures authorised by the Head of IT Services

9. Damaged storage devices containing classified data will undergo appropriate risk assessment by the Dean/Head of Department or nominee, to determine if the device should be destroyed, repaired or discarded. Such devices will remain the property of the University and only be removed from site with the permission of the Dean/Head of Department.

10. The University advocates a clear desk and screen policy particularly when staff are absent from their normal desk and outside normal working hours. In addition, screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons.

11. Any necessary permissions to remove off-site any of the University's classified information assets, either printed or held on computer storage media, or to access these remotely, should be properly authorised by the information owner. Prior to authorisation, a risk assessment based on the criticality of the information asset should be carried out.

Backup, media and information handling

12. IT Services in consultation with Information System owners must ensure that appropriate backup and system recovery procedures are in place. Backup of the University's information assets and the ability to recover them is an important priority. IT Services is responsible for ensuring that the frequency of such backup operations and the procedures for recovery meet the needs of the business.

13. Management must ensure that safeguards are in place to protect the integrity of information during the recovery and restoration of data files; especially where such files may replace files that are more recent.

14. The archiving of information and documents must take place with due consideration for legal, regulatory and business issues, with liaison between technical and business staff, and in keeping with the University's Retention Policy and any departmental retention schedules.

15. Storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must also be carefully considered, especially where proprietary formats are involved.

16. All users of information systems must manage the creation, storage, amendment, copying and deletion or destruction of data files in a manner which safeguards and protects the confidentiality, integrity and availability of such files. The degree to which software techniques and disciplined user procedures are necessary should be applied by management and determined by the classification of the information in question.

17. Day to day data storage must ensure that current information is readily available to authorised users and that archives are both created and accessible in case of need.

18. Highly sensitive or critical documents should not rely upon the availability or integrity of (external) data files over which the author may have no control. Key documents and reports should normally be self-contained and contain all the necessary information.

19. Hard copies of classified material must be protected and handled according to the distribution and authorisation levels specified for those documents by the originator or asset owner.

20. All employees should be aware of the risk of breaching confidentiality associated with the photocopying (or other duplication) of sensitive documents. Authorisation from the document owner should be obtained where documents are classified as Confidential or Personal or Personal Sensitive.

21. All information used for, or by the University, must be filed appropriately and with regard to its classification.

22. All signatures authorising access to systems or release of information must be properly authenticated.

23. All hardcopy documents of a sensitive or confidential nature are to be shredded or similarly destroyed when no longer required. The document owner must authorise or initiate this destruction.

24. Any third party used for external disposal of the University's obsolete information bearing equipment or hardcopy material must be able to demonstrate compliance with the University's information security policies and also, where appropriate, provide a service level agreement which documents the performance expected and the remedies available in case of non-compliance.

Exchanges of Information

25. Prior to sending classified information or documents to third parties external to the University, not only must the intended recipient be authorised to receive such information, but the procedures and information security measures adopted by the third party must also be seen to continue to assure the confidentiality and integrity of the information.

26. Personal, Sensitive or Confidential data or information, may only be transferred across networks, or copied to other media, once it has been encrypted and password protected. Transfer should only occur when the confidentiality and integrity of the data can be reasonably assured throughout the transfer.

27. Web browsers are to be used in a secure manner by making use of the built-in security features. IT Services must ensure that managers are made aware of the appropriate settings for the software concerned.

28. All parties are to be notified in advance whenever telephone conversations or videoconference events, such as lectures, are to be recorded.

29. Email addresses and faxes should be checked carefully prior to dispatch, especially where the information content is sensitive; and where the disclosure of email addresses or other contact information, to the recipients is a possibility.

30. Any fax received in error is to be returned to the sender or destroyed. Its contents must not be disclosed to other parties without the sender's permission.

31. Unsolicited or unexpected faxes should be treated with great care until the sender has been identified.

32. The identity of recipients or requesters of sensitive or confidential information over the telephone must be verified.

33. Electronic mail must not be used to communicate confidential or sensitive information unless appropriate measures have been taken to ensure authenticity and confidentiality, that it is correctly addressed and that the recipients are authorised to receive it.

34. Electronic commerce systems, whether to buy or to sell goods or services, may only be used in accordance with the appropriate financial regulations. Staff authorised to make payment by credit card for goods ordered over the telephone or internet, are responsible for safe and appropriate use.

Information in application systems

35. Important transaction and processing reports should be regularly reviewed by properly trained and qualified staff.

36. Email should only be used for business purposes in a way which is consistent with other forms of business communication and in accordance with the University's email policy. The attachment of data files to an email should be done with reference to any classification of the information being sent.

37. Information received via email must be treated with care due to its inherent information security risks. File attachments from unknown sources should be scanned for possible viruses or other malicious code.

Owners of Key Information Assets

Information Asset	Owner
Personal Data	
Student record (from application to graduation)	Academic Registrar
Registers of student attendance	Executive Dean
Student health & welfare records	Director of Academic Services
Careers guidance records	Director of Academic Services
Student accommodation records	Director of Estates
Library usage records	Director of Academic Services
Student work placement records	Executive Dean
Alumni records	Director of Marketing
Staff records	Director of Human Resources
Non-personal data	
Application and enrolment statistical data	Academic Registrar
Assessment statistics	Academic Registrar
External Examiners reports	Academic Registrar
Destinations statistics	Director of Academic Services
Estates data	Director of Estates
Health & Safety statistics	Pro Vice-Chancellor Corporate Resources
Library administration	Director of Academic Services
Course descriptions	Executive Dean
Tutorial records	Executive Dean
Course administration	Executive Dean
Market research information	Director of Marketing
University Committee agendas and minutes	Director/Exec Dean responsible for administering the committee
Board Committee agendas and minutes	University Secretary
Asset registers	Director of Finance
Supplier data	Director of Finance
Finance records	Director of Finance