UCL Corporate Digital Data Ownership and Access Policy

Information Security Policy

University College London

Document Summary

Author:	Dr Will Miller
Reference:	data access policy final v1.doc
Date:	28/5/2008
Revisions:	Final v1

University College London, Gower Street, London WC1E 6BT
Tel: +44 (0)20 7679 2000
www.ucl.ac.uk

Purpose

1. This policy provides guidelines for the governance of corporate data, its ownership, the responsibilities associated with ownership and principles of access to such information.

A. Background

2. UCL's corporate data are institutional assets and are held by the university to support its fundamental instructional, research, business and public service missions. Effective management requires that corporate information is not freely available but accessible in a user-friendly format to those who require it for legitimate UCL business use. The intent of this policy is to assure that the data are accessible, up-to-date, properly managed, accurate and securely used by UCL staff and other authorised persons.
3. UCL will provide open accessibility of data for the university community to support the performance of assigned duties. Personnel will use the data solely for the purposes related to the UCL strategic mission.
4. Access to information under the Freedom of Information and UCL Publication Plans is dealt with in separate policies. Access to and use of personal data is controlled by the Data Protection Policy, through the UCL Data Protection Officer; this policy is subsidiary to the Data Protection Act and Data Protection policy in respect of personal data.
5. Appendix A provides a list of key data elements, the data owners and custodians for each, who are responsible for the maintenance of these items, and whether the data items are restricted access or not. This list will be updated from time to time.

B. Definitions

6. Corporate Data/Information - is data elements that are consistent with at least one of the following criteria:
    - Needed for the operations, plans, or management of more than one CSS Division or Academic Department.
    - Reported on or used in official UCL reports.
    - Used by more than one system.
    - Referred to or used by a broad cross section of users.
    - Required for legal, statistical, government or historical requirements.
    - Hosted by Corporate Support Systems.
7. Information collected by one CSS Division or Academic Department and has no use outside that division or its host system is not covered by this policy.
8. Data Owner - Data Owners are senior University officials who have a planning and policy-level responsibility for data within their functional areas, and are nominated as having responsibility for complying with the Data Protection Act and granting access to information. In this policy Data Owners are, through the auspices of the Information

Strategy Committee, responsible for recommending policies, procedures and guidelines for University-wide corporate activities.

9. Data Custodian - the individual unit or staff identified by the data owner to be responsible for the collection, creation, modification and deletion of the specified corporate data element(s). Management Systems is the owner for corporate data elements where an owner does not exist or has not been defined.
10. With respect to personal and other data, employees, students and other affiliates have a duty to inform UCL of changes in their personal details, consistent with the requirements of Finance, HR, Registry and other policies.
11. Unrestricted Access Data – read access to data in this category is available to paid UCL staff on receipt of an appropriate system account. Further approvals may be required for disclosure to third parties and for different levels of write access.
12. Restricted Access Data - data elements in this category are limited to access on a needs basis because of legal, ethical, or privacy issues. Access to elements so designated by the Data Owner can be obtained only with the approval of the designated Data Owner.
13. Data Protection Officer (DPO) - is the formal office for regulating and advising on the application of the Data Protection Act. The Act covers the processing of personal data recognising that some data is treated as ‘sensitive’ data (such as sexual preference, religion, political opinions and health), and is subject to special provisions surrounding the collection, storage and access of such information. All personal information collected and stored in a digital form in an organisation must be registered under the terms of the Act. The DPO has a policy remit in the definition, management and dissemination of UCL personal data.
14. Data Dictionary - a reference which describes the available corporate data elements and their alias names. A data dictionary will usually contain a working definition of each element, the values that are allowed, database and other location information, and additional metadata.
15. Data Integrity - the qualities of data validity and reliability, in addition to the accuracy of the values.
16. Domain - The set or range of all possible data values for a specified data element. For example, M and F would be the domain for the data element ‘Gender’.
17. Data Element - A single property or attribute of an object (entity). For example, Name is a data element frequently associated with the entity Person.
18. Data Value - An instance of a data element. For example, Joe X. Blogs is a name of a specific Person.

19. Personal Data – Data that relates to a living individual who can be identified:

    a) from the data; or

    b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller; and

    c) includes any expression of opinion about the individual and any indications of the intentions of the data controller or any other person in respect of the individual.

20. Repository - Information about the data in an organisation's digital systems. The repository is used to catalogue the meta-data or to enable software development tools and operational systems to assess the meta-data.

C. Policy

Governing Committee

21. The Information Strategy Committee.

Applicability

22. This policy applies to all employees of UCL and others contracted by UCL and who have access to and/or use of the information/data, and to all corporate digital information regardless of the form of storage. A typical but not exhaustive list of storage includes: computer applications and databases, websites, computer disks, portable drives, computer/terminal screens, mainframe disks, backup tapes, and computer/communication networks.

Access and Usage

23. Data access and usage rights fall into the categories of read-only, update and external dissemination. Each is discussed in turn below.

24. In general, UCL will provide appropriate access to corporate information for its employees without unnecessary difficulties or artificial restriction. UCL will also protect its data assets through security measures and authorisation levels, to assure the proper use and dissemination of the data.

25. In all cases, information designated as sensitive by the Data Protection Act, such as trade union membership or relating to health, requires access to be restricted to employees with sufficient rights as specified either under the Data Protection Act or UCL policy. The classification of corporate data entities as either restricted or unrestricted must be documented by the Data Owner and communicated to the Data Protection Officer and Management Systems.

26. Following such advice, Appendix A to this policy is to be updated accordingly.

    a) Read-Only Access

       In principle, paid employees will be granted access to unrestricted corporate data on a read-only basis on joining UCL.

Read only access to UCL data can be granted to all other users (e.g., honorary staff, students, off-campus affiliated institutions, etc.) with the permission of the Data Owner.

b) Update Usage

The Data Owner shall grant authority to update data only to personnel, students or others whose job duties or interactions with UCL specify responsibility for data update.

c) External Dissemination

External dissemination of unrestricted data (whether in summary or specific form) by staff is permitted for official reporting, such as HESA and HEFCE returns, and Annual Financial Statements, but the release of any information should be guided by the absolute requirement to respect individual privacy and to protect the integrity of the data. The release of all other data must be approved by the Data Owner(s) for the element(s) involved. This is dealt with further in the section "Data Control", below.

Data Provision

27. Based on the data descriptions at Appendix A, key UCL data will be represented within a single logical data model that will be the source for all data requests and physical data models. Management Systems is responsible for developing this model and corresponding data structures.

28. Users will have access to the data model and repository according to their access rights. Management Systems will ensure that the needs of all users of corporate data are taken into consideration in the development and modification of data structures, elements and acceptable values.

29. When requested, Data Custodians must provide documentation describing each data element to be maintained within a data dictionary conforming to specifications provided by Management Systems. These specifications will include, but are not limited to, domains and acceptable values for each element.

Data Integrity

30. Organisations have a duty to maintain accurate personal information under the Data Protection Act, as well as needing accurate information to run their activities in an effective manner. Data integrity is a legislative as well as an operational imperative for UCL. Instances of inaccurate data should be reported to Data Owners in the first instance, and escalated to the DPO as necessary.

31. It is the responsibility of each Data Custodian to ensure the correctness of the data values for the elements within their charge and to take timely corrective action whenever necessary for data integrity. All employees are expected to bring data problems and suggestions for improvements to the appropriate Data Custodian or

Management Systems. Management Systems is responsible for data integrity at the system application level.

32. Where the same or similar data are held on more than one system, for example Department names in HR and Portico, a Primary Data Custodian and Owner should be declared to be responsible for describing the acceptable values and domains. Secondary Data Custodians are then responsible for maintaining such data according to the definitions set out by the primary custodian.

33. If necessary, the respective ownership of primary and secondary information will be settled by the governing committee.

Data Continuity in context of Business Continuity

34. Policies and plans relating to Business Continuity and the restoration of corporate data in all forms are maintained by individual Departments under the umbrella of UCL's Major Incident Team. Management Systems maintains such plans for restoring databases and relevant systems for accessing data should this be necessary.

Data Control

35. Data which are taken or derived from corporate systems or databases and stored or used locally in CSS Divisions or Academic Departments must be appropriately protected to ensure continuity of the same security, integrity and availability criteria that governs the data at source.

36. It is a common and necessary practice to query corporate systems or databases and save data locally on departmental computers, disks and networks. Often the data are saved in application software such as Microsoft Word, Excel and Access. In some cases, data may be imported into a department database such as SQL Server or Oracle. System security must prevent unauthorized access to saved data files and any application work files.

37. Restricted data, as defined by Appendix A, must not be stored on mobile devices, including laptops and PDAs, portable hard-drives or other removable media (e.g. DVDs or CDs) without authorisation from the Data Owner and only where such devices are encrypted. Such permission may be delegated by the owner to the responsible line manager. Further policy guidelines on the use of restricted data can be found at Appendix B.

38. In addition to 37, unrestricted personal information from corporate systems must be encrypted before being transferred offsite if one or more of the pieces of information by which an individual may be identified (name, address, postcode, email, telephone numbers) is combined with information which could reasonably be expected cause harm or distress if released.

39. Corporate information should be secured in line with Computer Security Team policies and recommendations, the requirements of the DPO, and the access privileges that govern the corporate data at source. Access controls are necessary, for example, to limit

and/or detect access to data or applications, thereby protecting these resources against unauthorised modification, loss, and disclosure. Failure to appropriately consider these controls may result in a user's access being removed.

Data Lifecycle

40. Some sets of data will need to be maintained for a set number of years to comply with Tax Law, UCL Financial Regulations or UCL Records Policy, and it is the responsibility of the Data Owner for clearly setting out the policy of longevity for data sets.

41. Data in ‘lookup tables’, for example postcodes, course codes, VAT rates, will change periodically, depending on the data provider. Data custodians need to ensure that this static information is kept up to date, and it will affect the quality of data in other systems.

42. Revisions to the data schema at Appendix A should in the first instance be sent to the Director of Management Systems. Changes to the sensitivity level should be agreed by the Data Owner.

Document History

Document Location

The source of the document can be found in:
http://www.ucl.ac.uk/cert/swg/policy/Data_Access_Policy.doc

Revision History

Date of this revision: V0.6 13/2/2008

Date of next revision:

Revision Date	Revision number	Summary of Changes	Reason for changes
11/09/07		Initial Draft sent to CSS Divisions	
19/09/07		Nigel Percival	Initial comment
08/10/07		Richard Tittle	Initial comment
11/10/07		David Booth	Initial comment
24/10/07		Jennie Moule	Initial comment
29/10/07		Chris Hallas	Initial comment
4/12/07		Sara Brandt	Initial comment
13/12/07		Jan Cropper	Initial comment
25/1/08		Tim Perry	Initial comment
10/4/2008	V0.7	Data Controller definition removed	Not referred to elsewhere in document
10/4/2008	V0.7	New para 17. Addition of mobile device authorisation requirement	Internal audit requirement
8/5/2008	V0.8	Change to Background to note superiority of Data Protection Act and policies, inclusion of portable disk media under mobile devices, and Director of MS as point of contact for changes to Appendix A.	Revisions following discussions with Chair of SWG
13/5/2008	V0.9	Inclusion of Audit requirements surrounding offsite working	Revisions following discussions with Chair of SWG
22/5/2008	V.10	Inclusion of SWG comment	Views of committee members
28/5/2008	Final V1	Encryption policy made into Appendix B	Requirement from AdSSC

Approvals

This document requires the following approvals

Name	Signature	Title	Date of Issue	Version
Information System Committee				

Distribution

This document has been distributed to:

Name	Date of Issue	Version
CSS Divisions, MS Managers, Roland Rosner	11/09/07	0.1 – 0.4
Library Services	3/12/07	0.5
Academic Services	18/1/08	0.5(WM)
Computer Science	12/2/08	0.6
SWG Chair (Paul Lamb)	March 2008	0.6
SWG	21 May 2008	0.9
AdSSC	21 May 2008	0.9