Approved by Council
1 December 2009;
revised December 2012 and September 2013

GOLDSMITHS
University of London

RECORDS MANAGEMENT POLICY

Note: For many purposes it will be found most useful to consult the online version of this document, which is mounted by section and contains hyperlinks to related policies.

1 Scope and context for this Policy

This Policy was approved by Council on 1 December 2009. It was last revised in 2012 and will be updated as necessary to ensure that it continues to support the Records Management Strategic Aims and external requirements. Council has delegated to Academic Board authority to approve changes to the Policy which primarily affect academic records, on the recommendation of Information Management and Systems Committee.

The two main drivers for institutional policy in Records Management are internal efficiency and compliance with external requirements, including the Data Protection and Freedom of Information Acts. This Policy is therefore designed to complement the Management Framework for Compliance with Information Law, but at the same time extends beyond the requirements of legal compliance which that Framework addresses.

This Policy seeks to address the need for:

- appropriate arrangements for the security of all information, supported by a programme of risk assessment and related to:
    - availability: knowing that the information can always be accessed;
    - integrity: knowing that the information is accurate and up-to-date, and has not been subject to unauthorised modification: for personal data this is required by the Fourth Data Protection Principle (see below);
    - confidentiality: knowing that levels of access to information of different kinds are appropriate to its content: for personal data this is required by the Seventh Data Protection Principle.
- capacity to locate required information in all categories promptly (including in areas of high staff turnover)
- proactive publication of information where appropriate
- reasonable confidence that all material held by the institution relevant to any specific Freedom of Information request has been successfully located;
- compliance with the *Code of Practice on Records Management* published by the Lord

Chancellor under the Freedom of Information Act;

- adherence to the Data Protection Principles relevant to Records Management, especially those which state that personal data held must be:

  - Processed for limited purposes (Second Principle) (will be breached if personal data is used in ways not notified to the Data Subject when the data was collected, and in most cases if the Data Subject's consent is not also obtained)

;

  - Adequate, relevant and not excessive (Third Principle) (will probably be breached if there is no clear system for destroying personal data no longer needed);

  - Accurate (Fourth Principle) (breached if files are not kept up to date);

  - Not kept longer than necessary (Fifth Principle) (breached if there is no clear system for destroying personal data no longer needed – as is provided by a formal Retention Schedule);

  - Secure (Seventh Principle) (may be breached if files are not clearly classified, as they may be inappropriately stored in relation to their confidentiality level).

- savings in space by destroying paper-based information which does not need to be retained, is unnecessarily kept in multiple copies across the institution, and/or could feasibly be retained in electronic form only.

Ultimate responsibility for compliance with all legislation by the College rests with Council. Council also has an interest in the efficient management of the College is therefore also concerned in broad terms with those aspects of the Policy which are not narrowly directed to legal compliance.

The Registrar and Secretary is responsible for the implementation of institutional strategies and policies relating to Records Management, but delegates many aspects of Records Management Policy to the Head of Information Management. Responsibility for institutional oversight of information risk also rests with the Registrar and Secretary. There are also specific responsibilities for all Heads of Department, and for all staff employed by the College who deal with written materials, which are defined below.

Unlike most universities, Goldsmiths has no professionally qualified Records Manager, and for the time being makes use of external consultancy to bridge the skills deficit. The responsibilities currently assigned will require review when a Records Manager is appointed.

Support for the implementation of the Records Management Policy and the Records Management Strategy is an explicit role of the IT Strategy. Through responsibility for the IT Strategy, the Director of Information Technology has an important role in relation to Records Management Policy implementation. The Records Management Policy is closely linked to the *Electronic Security, Data Backup and Recovery Policy***.**

2 Responsibilities of Heads of Department for Records Management

- appointing a Records Management Coordinator (see below) for her/his Department, and ensuring that the person appointed has sufficient time available, and appropriate

access to information about the Department's activities, to undertake the duties involved;

- ensuring that any processing of personal data in their department complies with the generic staff or student Data Collection/Fair Processing Notice as appropriate, and (if the personal data was collected after entry ot the College) with the Notice issued to the Data Subject at the time;[1]

- ensuring that all written records generated by, or used by, the Department, are notified to the Head of Information Management for inclusion in the College Retention Schedule;

- ensuring that the retention and destruction protocols in the Retention Schedule are observed, for items in respect of which they are identified as the accountable Head of Department; *[A first version of the Retention Schedule, focusing on the holdings of administrative departments, which have already been subject to a comprehensive Information Audit, will be published by the time this Policy comes into force; Heads of academic departments will have this responsibility once the Retention Schedule is extended to include material for which they are responsible, and the date for this is to be agreed.]*

- ensuring that no data of any kind is held on servers not owned by the College, or remote from the main campus, unless the arrangements concerned have been approved by Information Management and Systems Committee or (for educational partnerships only) as part of the Due Diligence Process within the Collaborative Provision Framework.

3 Responsibilities of Records Management Coordinators

This applies to administrative departments only: as these duties become relevant to academic departments (eg when a Retention Schedule has been developed for them), the Departmental Administrator will be expected to have the equivalent role.

When nominating Records Management Coordinators, Heads of Department should as far as possible select individuals already well-informed about the range of information held by the Department, the business processes supported by this information, and the ways in which it relates to the information holdings of other departments. A high level of problem-solving ability and determination, as well as practical competence in the main functions of Windows Explorer, have also been identified as pre-requisites for the role. There are advantages in a Records Management Coordinator also being the primary editor of any webpages for which the Department is responsible, and Heads of Departments are asked to consider the feasibility of this in the light of local circumstances.

Responsibilities of Records Management Coordinators will vary between departments according to the nature and volume of the data held, and will be as delegated by the Head of Department. However, unless the Head of Department has notified other arrangements in writing to the Head of Information Management, these delegated duties will include:

- coordinating generally their Department's input to cross-departmental reviews of records management issues (including in particular ensuring that detailed information is provided on the records held by the Department);

[1] See the Data Collection section of the Goldsmiths Data Protection Policy. From that page, there are links to the current Framework Collection Notices for staff and students.

- providing general liaison between the College's central Information Management function and their own Department, on their Department's ongoing contribution to the College Publication Scheme;

- for personal data collected by the Department, keeping a systematic local information base on the processing purpose for which that data is held, and the wording of the data collection/fair processing notice which notified that processing purpose to the Data Subjects;

- Keeping the Head of Information Management informed about new records series in their Departments not currently included in the Retention Schedule, and providing the information necessary for the updating of the Schedule.

- acting as an "ambassador" for central records management policies in the Department.

In large departments, Heads of Department may find it necessary to split the work between two or more members of staff; however one individual should always be identified as the primary Records Management Coordinator, who in particular will be responsible for ensuring that a timely response is made on behalf of the department to any institutional level circulars to Records Management Coordinators generally. Heads of Department may nominate themselves as Records Management Coordinators.

4 Responsibilities of all Staff

These responsibilities are closely related to those relating to Data Protection in the Management Framework for Data Protection, but are broader as they apply to all written materials which they handle in the course of College employment.

- Whether working on- or off-campus, avoiding the storage of electronic data on web-based services,[2] unless these are:

  - provided by the College via its own website;

  or

  - made available through a contract between the College and the provider of the service;

  or

  - explicitly approved by Information Management and Systems Committee as a special case;

  or

  - generated in the context of an inter-institutional research project where there are contractual arrangements between the institutions involved forming a basis for the filesharing arrangements, including which institution is the holder of the data.

- Ensuring that information generated by them which is significant in the operation of College business processes, or legacy data for which they have been made responsible, is held on network drives or other approved locations to which at least one other person has access, according to a record-keeping system which it is

[2] Common examples of such storage locations are Googledocs or the online file storage facilities provided with the EEEpc range. Staff should not, in the course of their work for the College, store files under their private identity via such facilities.

understood by that person or likely to be transparent to them. *[Note: Principal Investigators have additional responsibilities in relation to research data: see section of this Policy on Research Data Management]*

- Avoiding the storage of any data on the hard drives of personal computers and laptops, or portable devices such as CDs or USB flash drives (except for temporary copies used over a short period, or work in progress which will shortly be transferred to the College network); *[This obligation will not apply fully to all staff until after the rest of this Policy comes into force: Information Management and Systems Committee is in process of considering the best approach to implementation.]*

- Avoiding the copying of files stored on the College network to personal computers or mobile devices (except for short periods when access to the College network is expected to be difficult).

- Ensuring, as far as possible, that any written information for which they are responsible in the course of their employment is held at a level of access and security appropriate to the importance and confidentiality of the information concerned.

- Keeping their Department's Records Management Coordinator (or Head of Department if he or she requests this) informed of any new records series created by them, so that it can be included in the published Retention Schedule of the College. *[Until further notice, applies only to staff of administrative departments.]*

5 Research Data Management

Goldsmiths recognises research data as a vital asset and recognises also that the curation and sharing of research data is key to its mission to create knowledge. The College fully supports the Research Council UK's statement that publicly funded research is a public good that should be made openly available to the public when legally and ethically appropriate. Across all academic disciplines, research data should be managed to agreed standards and according to funding body requirements throughout the research data lifecycle. Responsibility for research data management during any research project lies with Principal Investigators (PIs).

PIs are required to consider data creation, curation and sharing in the development of their research proposals and grant applications. All new research proposals must include research data management plans that explicitly address data capture, management, integrity, confidentiality, retention, sharing, re-use and publication.

The College will provide training, guidance and support for the development of research data management plans and their implementation, and the infrastructure and expertise for long-term curation, preservation and access to research data.

PIs should record research data upon creation and deposit it according to their plan (often within six months of publication of research findings). College will preserve access for as long as specified by the data management plan (which can be up to ten years after it was last accessed). Any data which is retained elsewhere, for example in an international data service or domain repository, should be registered with the College.

Data should not be deposited with any organisation that does not commit to its access and availability for re-use, unless this is a condition of funding or would prevent commercial interests. Before committing to restrictions on accessibility, researchers

should satisfy themselves that these restrictions are sustainable in the context of the fairly limited exemptions from disclosure available under the Freedom of Information Act.

Open access to research data will be granted under appropriate safeguards according to conditions and timeframes specified by researchers, commercial partners and funding bodies. The College will support this through the provision of a data repository.

6 Privacy

Staff have no absolute right of personal privacy in relation to the contents of their College email account, or electronic files which they have stored on College computing facilities which they use in the course of employment. However, access to these materials will normally be only be by those to whom the member of staff concerned has authorised access, or where there is a system of shared access known to the member of staff. (Abnormal circumstances in this context include investigations of criminal activity or suspected serious misconduct: in these cases access will be authorised by the Registrar and Secretary.)

Particular attention is drawn to the rights of Data Subjects to have access to their personal data held by or generated by others. Staff should not expect that their email or other correspondence about an individual can be kept confidential from that individual if they request access. (See also the Duties of Staff within the Data Protection Policy.)

In the event of a unplanned absence or permanent departure from College by a member of staff which threatens to disrupt the work of the College, arrangements may be made by the Registrar and Secretary or those authorised by her/him to have access to the personal network drive, email account and other computing facilities used by the absent member of staff. *[Currently the Registrar and Secretary authorises Heads of Department to obtain access to the email of their staff under these circumstances.]* However, folders, files and messages marked "Personal" in the name or subject line, or containing a clear indication that Trades Union business is involved, will not normally be read unless there is specific reason to suspect that these labels are being used with intention to deceive, or in the course of an investigation of criminal activity or serious misconduct.

Approved by Council, 1 December 2009;
update approved by the Chair on behalf of Council
December 2012, primarily by the addition of the Research Data section;
minor amendments September 2013 to reflect administrative restructuring