

GOLDSMITHS
University of London

MANAGEMENT FRAMEWORK FOR COMPLIANCE WITH INFORMATION LAW

This Framework was approved by Council on 29 June 2006 and revised in April 2011

Minor amendments, to reflect changes in staff posts referred to explicitly in the text, and needs for specific types of Third Party Disclosure, were approved by the Chair of Council in the Spring term 2007, in the Summer term 2008, mainly to reflect the new governance status of the Students' Union, in the Summer vacation 2009, to reflect the abolition of the office of Academic Registrar and the change of title of the Head of Secretariat (to Head of Corporate Governance and Information Management), and during 2010 (to add further powers for specific officers).

Goldsmiths is committed to a fair approach to the handling of information, especially in relation the fair processing of personal data, and to making its policies transparent:

- **to those requesting information about themselves or the College;**
- **to those responsible for managing information, and in particular for the processing of personal data.**

A General

1 Scope and context for this Framework

This Management Framework deals explicitly with compliance with the Data Protection Act (1998) and the Freedom of Information Act (2000). The College's administrative arrangements for complying with the Freedom of Information Act are designed in such a way that they also cover any information falling within the scope of the Environmental Information Regulations (2004).

Ultimate responsibility for compliance with all legislation by the College rests with Council. The Registrar and Secretary is responsible for overseeing the implementation of arrangements which Council has approved, and in so doing may seek the views of Council or of a relevant College committee. Many aspects of policy development and day-to-day management of Data Protection and Freedom of Information compliance at institutional level are delegated to the Data Protection Officer and Freedom of Information Officer,¹ but there are also specific institutional responsibilities assigned to other named members of staff.

¹ The roles of Data Protection Officer and Freedom of Information Officer are currently both assigned to the Head of Corporate Governance and Information Management (until 31 August 2009 Head of Secretariat).

2 Responsibilities of all members of staff for Information Compliance

Members of staff of the College have a responsibility to ensure that they follow the College's *Data Protection Policy and Guidelines* and *Freedom of Information Policy and Guidelines*, which are designed to ensure that the activities of the College comply with the Data Protection Act (1998) and the Freedom of Information Act (2000).² They should acquaint themselves in sufficient detail with these two statements to enable them to ensure that they understand their obligations. This includes knowing which activities they are not authorised to undertake (notably in relation to Data Subject Access requests, requests for transfers of personal data to third parties, and the claiming of Exemptions under the Freedom of Information Act).

Breach of requirements set out in the College's published policies concerning compliance with information law is likely to be treated by the College as a disciplinary offence.

B Data Protection

1 Scope and context for this section

The Data Protection Act (1998) essentially defines "personal data" as data relating to living individuals who are capable of being identified. The term "personal data" is used in this Framework, and in the College's web-based *Data Protection Policy and Guidance*, in this sense.

The College's Notification of personal data processed under its responsibility, lodged with the Information Commissioner, does not include information held by the following separate Data Controllers:

- The Goldsmiths Students' Union (a separate Data Controller from 1 July 2008, when new Articles of Governance for the Union come into effect);
- The Medical Centre, which is directly responsible to the Information Commissioner for the personal data which it holds on students and staff as patients (although the College is of course also Data Controller for Occupational Health and similar reports from the Medical Centre to the College on individuals);
- The central University of London (a separate Data Controller from the Colleges).

The framework of operational responsibilities approved by Council for ensuring compliance with the Data Protection Act (1998) is set out below. More detailed policies, together with guidance for staff and explanations of the requirements of current legislation, are set out in web-based *Data Protection Policy and Guidance* pages, which are mounted on worldwide access.

² The Freedom of Information Policy and Guidelines also deals with compliance with the Environmental Information Regulations (2004).

2 Members of the College with key responsibilities in relation to Data Protection

(i) Data Protection Officer

The Data Protection Officer, under the supervision of the Registrar and Secretary³, is charged with the coordination of data protection compliance arrangements across the College. More specifically, the responsibilities of the Data Protection Officer include the following:

- Keeping the College's published Notification up-to-date, and acting as the College's official channel of communication with the Office of the Information Commissioner for data protection issues;
- keeping the College's web-based *Data Protection Policy and Guidance* under review - in consultation with senior members of the College with key responsibilities for data processing - such that it reflects recognised good practice and any relevant new legislation, and consistency of approach across the College is ensured where desirable;
- ensuring that the need for any changes in this Framework, or more generally in the College's approach to Data Protection, is considered by Council and/or other deliberative bodies of the College as appropriate, and that more minor amendments to the *Data Protection Policy and Guidelines* are introduced as necessary, following consultation with the Registrar and Secretary;
- briefing members of the College, and in particular Heads of Department (or their authorised deputies) as necessary on Data Protection requirements and advisable practices;
- responding to Data Subject Access requests as one of the College's designated officers for this purpose (according to the detailed provisions in Appendix A);
- authorising transfers to personal data to third parties (according to the detailed provisions in Appendix A).

(ii) Director of Student Services, Director of Marketing, Recruitment and Communications (MRC) and Director of Human Resources

The Director of Student Services, the Director of Marketing, Recruitment and Communications, the Director of Human Resources, and their authorised deputies, have the following responsibilities:

- Responding to Data Subject Access requests (see Appendix A);

³ In relation to Data Subject Access Requests and Third Party Disclosures (both within and outside the EEA), the Registrar and Secretary is authorised to make all types of disclosure, but will normally do so only when the other designated officer(s) indicated in Appendix A are not available.

- authorising transfers to personal data to third parties (according to the detailed provisions in Appendix A);
- reporting to the Data Protection Officer at the end of each calendar year with lists of:
 - Data Subject Access Requests to which they have responded directly;
 - Third party transfers which they have authorised (a) within the EEA and (b) outside the EEA.

These responsibilities relate to:

| | |
|---|--|
| Director of Student Services: | Personal data relating to students and former students (including being the named recipient of all Data Subject Access Request forms from current and former students, and normally coordinating responses to student-related enquiries which include the admissions process as part of a broader request) |
| Director of Marketing, Recruitment and Communications: | Personal data of candidates for admission as a student (including being the named recipient of all Data Subject Access Request forms from applicants for admission who are not current students) |
| Director of Human Resources: | Personal data of employees, former employees and applicants for employment |

These responsibilities may be delegated to nominees of the above who have received training organised by the Data Protection Officer relating to the particular types of disclosure involved.

(iii) Pro-Warden (Research and Enterprise)

The Pro-Warden (Research and Enterprise) is responsible for:

- Authorising transfers to personal data to third parties (according to the detailed provisions in Appendix A);
- reporting to the Data Protection Officer at the end of each academic year with lists of:
 - Third party transfers authorised (a) within the EEA and (b) outside the EEA;
 - research material containing personal data whose transfer to another institution has been authorised.

(iv) Head of Health and Safety

The Head of Health and Safety is responsible for:

- Authorising transfers of personal data to regulatory authorities concerning health and safety matters, where Section 31 of the Data Protection Act (Exemptions: Regulatory Activity) applies;
- reporting to the Data Protection Officer at the end of each year the number of such disclosures which have been made.

(v) Director of Finance (and senior members of Payroll staff acting on his behalf)

The Director of Finance is responsible for:

- Making routine disclosures to HM Revenue and Customs and the Department of Work and Pensions for the operation of the tax, pensions and benefits systems;
- responding to Court Orders for the disclosure of payroll information concerning individual employees, and reporting to the Data Protection Officer at the end of each year the number and broad nature of such disclosures that have been made.

(vi) Director Information Technology

The Director of Information Technology is responsible for:

- ensuring the security and appropriate backup of personal data held electronically on central computer systems, in line with recognised good practice.
- ensuring broad conformity with recognised good practice in respect of the publication of information on the World Wide Web and the collection of data using Web-based interfaces.

(vii) Head of Residences, Catering and Conference Services (and designated members of staff acting on her/his behalf)

The Head of Residences, Catering and Conference Services is responsible for:

- disclosures of personal data of students in emergency situations arising in the course of the management of halls of residence.
- disclosures of personal data in connection with the Electoral Roll return for student residences.
- reporting to the Data Protection Officer at the end of each year the number of such disclosures which have been made.

(viii) College Superintendent

The College Superintendent is responsible for:

- Providing to the police and other emergency services information about whether particular individuals are likely to be students of the College (subject to final confirmation later by Student Services following more comprehensive verification of records).
- reporting to the Data Protection Officer at the end of each year the number of such disclosures which have been made.

(ix) Heads of Department

The more complex areas referred to below are explained in more detail in the Data Protection Policy and Guidelines.

- Forwarding to the Director of Student Services, the Director of Human Resources or the Data Protection Officer, as appropriate, any Data Subject Access Requests received in their Department;
- ensuring that any College-wide arrangements approved for informal access to data at departmental level by the students and/or staff of the Council are implemented in their Department. ⁴
- ensuring that members of their Department comply generally with the arrangements set out in the College *Data Protection Policy and Guidelines*. (This responsibility may be delegated, provided that the College Data Protection Officer is informed of the arrangements made, and that the period of delegation does not extend beyond the term of office of the particular Head of Department.)
- arranging for appropriate representation of the Department at any briefing meetings on Data Protection organised at College level, and ensuring that information from briefing meetings is disseminated appropriately within the department;
- authorising transfers of personal data held within their Department to third parties within the European Economic Area, provided that the written permission of the Data Subject has been obtained. ⁵
- notifying the College Data Protection Officer of any significant changes in their Department's data processing arrangements which might necessitate a change in the College's Data Protection Notification to the Information Commissioner.

⁴ Such arrangements will be published in the College's Data Protection Policy and Guidelines following approval by the Registrar and Secretary, as well as being notified by circular to departments when first introduced or modified.

⁵ Note that Authorisation at Head of Department level is not necessary for personal references: see (viii) below.

- ensuring (in teaching departments only) that where coursework or other marks are assigned on the basis of purely automated decisions, a formal statement is freely available to students (eg in the Student Handbook), explaining the logic behind the assessment or grading system involved.⁶
- where the Department has members of staff whose work includes research involving personal data, ensuring that if they leave the College they are made aware of the obligation to consult the Pro-Warden (Research and Enterprise) on any transfers of personal data.

(x) Members of staff of the College generally

(See also generic responsibilities at A(2) above.)

The Data Protection obligations which apply to all staff in the College may be summarised as follows:

- avoiding as far as possible writing down (in electronic or hard copy form) opinions or facts concerning a Data Subject which it would be inappropriate to share with that Data Subject;
- ensuring that personal data (in electronic or hard copy form) is kept securely, so that it is protected from unintended destruction or change and is not seen by unauthorised people;
- avoiding giving personal data by telephone unless there is a very high degree of certainty that the caller is the person he/she appears to be, and is an appropriate person to receive the data in question;
- ensuring, if working on personal data as part of their Goldsmiths employment (whether for research or other purposes) when away from the College site, that the College's *Data Protection Policy and Guidelines* are observed, in particular in matters of data security;
- ensuring that any staff⁷ or students processing data under their supervision - whether for administrative purposes or in the course of a joint research project - are appropriately briefed on the relevant requirements of the Data Protection Act (1998) as set out in the College's *Data Protection Policy and Guidelines*;
- ensuring that the College has the most accurate, up to date personal information about themselves on record, and notifying the Human Resources Department and/or their Heads of Departments of any changes, for example to their address, telephone numbers, qualifications etc.

⁶ Situations where this requirement of the Data Protection Act applies are expected to be very rare at Goldsmiths.

⁷ "Staff" in this context includes temporary staff, and individuals working in the College but employed through an agency.

C Freedom of Information

1 Scope and context for this section

Note: Section C also applies to the Environmental Information Regulations (2004) where relevant. These Regulations operate in a very similar way to the Freedom of Information Act.

The Freedom of Information Act (2000), which applies to most organisations in receipt of substantial public funding, requires to the College to publish a *Publication Scheme* listing the documents which it routinely makes available to the public. (Like most public authorities, Goldsmiths does this via its website.) The College is also obliged to operate a system for releasing to members of the public on request, and within a legally specified framework, any other information which it holds, unless the Act exempts the relevant type of information from disclosure.

2 Exemptions from Disclosure under the Freedom of Information Act: designated College officers

The only members of the College authorised to apply the Exemptions in the Freedom of Information Act (ie to decide that access to requested information which the College holds will be refused) are as follows. (Special arrangements apply to Exemption 36 (*Prejudice to the Effective Conduct of Public Affairs*), as in respect of this Exemption the Warden exercises a delegated Ministerial responsibility which may not be further delegated.)

- All Exemptions except Exemption 36: the Freedom of Information Officer and the Registrar and Secretary;
- All Exemptions: the Warden; ⁸
- All Exemptions: the Chair of Council (but only in the event of an appeal against the application of an Exemption by one of the individuals above⁹).

Normally members of the College who believe that they have received a request for information to which an Exemption applies should refer the case to the Freedom of Information Officer in the first instance. The Registrar and Secretary and the Warden will not normally deal with any request initially, unless the Freedom of Information Officer is unavailable.

Note: The Complaints procedure for individuals who are dissatisfied with the way in which their requests for information under the Freedom of Information Act have been handled (and for complaints relating to Publication Schemes) is a separate Policy approved by Council (March 2010).

⁸ The Warden will normally only be directly responsible for applying Exemption 36, and then only after any possible alternative Exemptions have been investigated by the Freedom of Information Officer, in consultation with the Heads of Departments with policy responsibilities relevant to the particular request.

⁹ This would be under the Complaints procedure relating to Freedom of Information, separately approved by Council.

3 Members of the College with other key responsibilities in relation to Freedom of Information

(i) Freedom of Information Officer (Head of Corporate Governance and Information Management)

- Keeping the College's web-based *Freedom of Information Policy and Guidelines* under review, such that it reflects recognised good practice and any relevant new legislation, and that consistency of approach across the College is ensured where desirable;
- ensuring that the need for any changes in this Framework, or more generally in the College's approach to Freedom of Information, are considered by Council and/or other deliberative bodies of the College as appropriate, and that more minor amendments to the *Freedom of Information Policy and Guidelines* are introduced as necessary, following consultation with the Registrar and Secretary;
- briefing members of the College, and in particular Heads of Department (or their authorised deputies) as necessary on Freedom of Information requirements and advisable practices;
- investigating, in consultation with senior members of the College responsible for the relevant area(s), whether Exemptions may apply to particular items of information requested;
- acting as the College's official channel of communication with the Office of the Information Commissioner for issues regarding the Freedom of Information Act.

(ii) Heads of Department

- Ensuring that a prompt and complete reply (within the relevant legal timescale) is given in response to any straightforward requests for information which can be responded to directly by the Department;
- forwarding to the Freedom of Information Officer, normally within two working days, any request for information not held, or not held in its entirety, by their Department, or where it seems likely that an Exemption should be applied to all or part of the information;
- forwarding to the Freedom of Information Officer, normally within two working days, any request for information in respect of which it seems likely that it is being sent to all universities (or the members of any other grouping of which Goldsmiths is a member);
- ensuring that members of their Department comply generally with the arrangements set out in the College's *Freedom of Information Policy and Guidelines*;
(This responsibility may be delegated, provided that the Freedom of Information Officer is informed of the arrangements made, and that the

period of delegation does not extend beyond the term of office of the particular Head of Department.)

- Arranging for appropriate representation of the Department at any briefing meetings on Freedom of Information organised at College level, and ensuring that information from briefing meetings is disseminated appropriately within the department;

(iii) Members of staff of the College generally

(See also generic responsibilities at A(2) above.)

- Knowing that a written request for information (in hard copy or electronic form) which is not for personal data relating to the applicant normally has the legal status of a Freedom of Information request even if the request itself does not mention the Act, and/or if the requestor is unaware of the Act when making the request, and following the College's Freedom of Information Policy and Guidelines accordingly (particularly in respect of speed of response);
- referring promptly to their Head of Department any requests for information which are not straightforward in terms of Freedom of Information requirements (eg because the information requested is distributed across more than one department);
- never refusing themselves to supply information which the College holds (but instead passing the request to their Head of Department).

**Approved (including table at Appendix A)
by the College Council on 29 June 2006,¹⁰ with revisions on 7 April 2011
*Revisions approved on behalf of Council March 2007, June 2008, July 2009 and
June 2010***

¹⁰ Data Protection Provisions are based on a Management Framework approved by Council on 23 March 2004.

GOLDSMITHS
University of London

Responsibilities and powers of named officeholders in the College in relation to Data Subject Access Requests, Third Party transfers of personal data, and personal data held for the purposes of research.

Note: The Head of Health and Safety and the Director of Finance are not included in the table for reasons of space: please see the main text.

| AREA OF DATA PROTECTION POLICY | RESPONSIBILITIES OF DESIGNATED COLLEGE OFFICERS | | | |
|---|---|---|--------------------------------------|---|
| | Data Protection Officer | Director of Student Services/Director of Marketing, Recruitment and Communications /Director of Human Resources (in respect of personal data of present and past students (Director of SS and Director of MRC) and employees (Director of HR) | Pro-Warden (Research and Enterprise) | Head of Department (all Heads, whether of academic or administrative) |
| Data Subject Access Requests | Responding to data subject access requests and informal enquiries from data subjects, or ensuring that these are dealt with by another appropriate member of the College. | Responding to Data Subject Access Requests. <i>(Normally the Data Protection Officer will not be involved in dealing with individual straightforward requests which clearly come from students, staff, or prospective and past students or staff.)</i> | | Forwarding any Data Subject Access request received from students or staff to the Director of Student Services, Director of Marketing, Recruitment and Communications or Director of Human Resources as appropriate, or to the Data Protection Officer. |
| Third party transfers to EEA destinations (personal data not for research purposes and not transmitted as personal references) | Authorising transfers of personal data to third parties within the EEA without the consent of the data subject in circumstances where this is permitted or required by current legislation, and where to do so seems advisable in the light of the individual situation. | <i>(As Data Protection Officer - see left)</i> | | Authorising transfers of personal data held within their Department to third parties within the European Economic Area, provided that the written permission of the Data Subject has been obtained. |
| Third party transfers to non-EEA destinations (personal data not for research purposes and not transmitted as personal references) | Authorising transfers of personal data to third parties outside the EEA where this is permitted or required by current legislation, and where to do so seems advisable in the light of the individual circumstances. | <i>(As Data Protection Officer - see left)</i> | | |

| | | | | |
|---|---|--|--|---|
| Personal data held for research purposes | In consultation with the Pro-Warden (Research and Enterprise), ensuring that the development of policy on data protection issues affecting research data is properly integrated with the approach of the College to data protection generally, and that College policy reflects nationally recognised requirements and good practice. | | Authorising transfers of personal data held for research purposes to third parties outside the EEA, where this is permitted or required by current legislation, and where to do so seems advisable in the light of the individual circumstances. <i>(Note: Since much research data is anonymised, obtaining the consent of the Data Subject will rarely be a relevant issue.)</i> | Where the Department includes members of staff whose work includes research involving personal data, ensuring that - particularly if they intend to leave the College - they are aware of their obligation to consult the Pro-Warden (Research and Enterprise) on any transfers of personal data. |
| Reporting obligations to College Data Protection Officer | | Reporting to the Data Protection Officer at the end of each calendar year with lists of: Data Subject Access Requests to which they have responded directly Third party transfers which they have authorised (a) within the EEA and (b) outside the EEA. | Reporting to the Data Protection Officer at the end of each calendar year with lists of: third party transfers which they have authorised (a) within the EEA and (b) outside the EEA and on research material containing personal data which has been transferred to another institution. | |

Note: In relation to Data Subject Access Requests and Third Party Disclosures (both within and outside the EEA), the Registrar and Secretary is authorised to make all types of disclosure, but will normally do so only when the other designated officer(s) indicated above are not available.