

Data Protection Policy

Approved by Information Services Board on 17th November 2009

1 Introduction

Queen Mary, University of London (the “College”) is required by law to comply with the Data Protection Act, 1998 (the “Act”). This Act came into force on 1st March 2000 and relates to the holding and processing of personal information. The College needs to keep certain personal information about individuals such as employees, students, graduates and others, defined as *Data Subjects* in the Act, to fulfil its objectives and meet legal obligations. Such data must only be processed in accordance with this policy and with the terms of the College’s Notification to the Information Commissioner, which sets out the purposes for which the College holds and processes personal data.

To comply with the law all data must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the College must abide by the eight *Data Protection Principles* set out in the Act. These state that personal data shall be:

1. processed fairly and lawfully and shall not be processed unless certain conditions are met;
2. obtained for specified and lawful purposes and not further processed in a manner incompatible with these purposes;
3. adequate, relevant and not excessive;
4. accurate and where necessary kept up to date;
5. kept for no longer than necessary;
6. processed in accordance with Data Subjects' rights;
7. protected by appropriate technical and organisational security, and;
8. not transferred to a country or territory outside the European Economic Area, unless that territory ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of personal data.

This policy shall guide all who process data in the College to ensure that these principles are followed and any breach, whether deliberate or through negligence, may lead to disciplinary action being taken.

2 Definitions

Processing is given a broad interpretation in the Act: it covers collecting, holding, sorting, destroying of data etc. Every person who holds any personal data about another individual in some form or medium (hard-copy or electronic) from where it can be retrieved is ‘processing’ data.

Personal Data is defined in the Act as data that relate to a living individual who can be identified from those data; or 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 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. Examples are name, address, date of birth, attendance details, comments on coursework, a photo.

Sensitive Personal Data is defined in the Act as personal data consisting of information as to:

- The racial or ethnic origin of the Data Subject
- His/her political opinions
- His/her religious beliefs or other beliefs of a similar nature
- Whether he/she is a member of a trade union
- His/her physical or mental health or condition
- His/her sexual life
- The commission or alleged commission by him/her of any offence
- Any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

Note 1: the definition of health is considered broadly under the Act; it is not defined exhaustively but includes preventative medicine, medical diagnosis, DNA sequences, medical research, provision of care and treatment and the management of healthcare services.

Note 2: personal demographic data are also considered to be sensitive (e.g. home address, salary, and bank financial details).

Data Controller is the person or entity who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. Queen Mary, University of London, as a corporate body, is the Data Controller under the Act; so are its employees.

Data Processor is any person other than an employee of the Data Controller who processes data on behalf of the Data Controller. For example, this could be a supplier to which some service, such as a payroll, has been outsourced.

Data Subject is the living individual to whom the data relates. For example, for the College this would mean employees and students, among others.

3 Rights to Access Information

The Act gives Data Subjects a right of access to personal data held about them by the College, and allows the College to charge a fee for such access.

All such requests to the College must be made in writing and a record must be kept of all requests for access to personal data. Access does not include the right to amend data, but the Data Subject has the right to request any errors or omissions identified are corrected.

All formal Subject Access Requests must be responded to within the terms laid down by the Act, and must be notified to the Records & Information Compliance Manager as soon as they are received.

The College will ordinarily charge the prescribed maximum fee (currently £10) for Subject Access Requests and take steps to verify the identity of the applicant.

4 Responsibilities of the Data Controller and Data Processors

Compliance with this Policy is mandatory and disciplinary action may be taken against anyone who fails to do so. The accompanying Guidelines should also be followed.

- Consent - In order to process data the College shall obtain consent from Data Subjects. In the case of sensitive personal data, express consent must be obtained
- Data Security - All College users of personal data must ensure that all such data they hold is kept securely, for example in a locked cabinet or password protected. They must ensure that it is not disclosed to any unauthorised third party in any form either accidentally or otherwise. Please see the College's [Information Security Policy](#) for further information on data security
- Third Parties - If the College enters in to agreements with third parties which include the sharing of personal data it shall ensure that adequate protection is offered and will use the data in accordance with defined purposes

5 Responsibilities of Data Subjects

All Data Subjects have an obligation to:

- Ensure that any information that they provide is accurate and up to date
- Inform the College and/or their department of any changes to information which they have provided, e.g. changes of address
- Inform the College of any known errors

6 Retention of Data

Personal data must only be kept for the length of time necessary to perform the processing for which it was collected. This applies to both electronic and non-electronic personal data. The College will keep some forms of information for longer than others. Data shall be retained in accordance with the College [Records Retention Policy](#) and associated [Records Retention Schedule](#).

7 Assessment Data

Students are entitled to information about their marks for all types of assessment, as well as decisions made on academic progress, award and classification. These are normally available as a matter of course but the College may withhold marks, transcripts and certificates or notification of decisions relating to academic progression or award in the event of a student being in debt to the College. However, access to this information is within the provisions of the Act and marks and other data will be released if a subject access request is made.

Note 1: examination scripts (answer books) are exempt from a right of access.

Note 2: "debt" refers only to debts directly related to academic study; tuition fees, book and equipment loans etc. It does not relate to accommodation or nursery fees etc.

8 Related College Policies

- Records Retention Policy
- Information Security Policy
- Policy on Access to Information by Staff and Students
- Research Ethics Policy
- IT PC Disposal Procedure
- CCTV Policy

9 Staff Checklist for Processing Data

Anyone in the College processing personal data shall consider the following

- Is this information really needed?
- Is the information 'standard' or 'sensitive'?
- If it is *sensitive*, has the Data Subject's express consent been obtained?
- Has the Data Subject been informed that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the Data Subject that the data is accurate?
- Will the data be securely held?
- If you do not have the Data Subject's consent to process, are you satisfied that it is in his/her best interests to collect and retain the data?
- How long does the data need to be kept and are there arrangements for its review/secure disposal?

10 College Duties

As required by the Act, the College has notified the U.K. Information Commissioner that it processes personal data. The registration number of the Notification is Z5507327 and can be viewed on the ICO website at: <http://www.ico.gov.uk/ESDWebPages/DoSearch.asp?reg=5174010>. The Data Protection Officer is Wendy Appleby (Secretary to Council & Academic Secretary), but any query relating to the implementation of the Act within the College should be referred to the Records & Information Compliance Manager who has been given day to day responsibility for data protection and reports to the Secretary to Council & Academic Secretary.

Guidelines are appended to this policy to advise staff on best practice procedures to follow. These guidelines may be subject to change or revision by the Data Protection Officer or her delegate.

Further information about this policy, Subject Access Requests, retention and disposal of data and/or any other data protection issues should be addressed to data-protection@qmul.ac.uk

Appendix – Guidelines

These Guidelines should be read in conjunction with the College's Data Protection Policy. Examples are set out below to illustrate some of the scenarios staff in Queen Mary might experience and best practice to be adopted.

I. What are my responsibilities?

All staff will process personal data in one form or another and as such have a duty to ensure that this is done fairly, stored securely and disposed of when it is no longer required. As such, all staff should be aware of the eight Data Protection Principles and bear in mind the '[Checklist for Processing Data](#)' detailed in the Policy. In particular, be aware of what constitutes sensitive personal data and the special circumstances under which it can be processed.

II. Dealing with Subject Access Requests

Anyone who wishes to make a Subject Access Request (SAR) should fill in an [SAR Form](#) available on the website. Any SAR received within Queen Mary should be copied to the Records & Information Compliance Manager (contact details below) so it can be logged. If in doubt as to whether you have received an SAR or how to respond to it please contact him for assistance.

Queen Mary, as Data Controller, must respond to such a request, in full, within forty calendar days. There are certain requirements that must be satisfied by the Data Subject before the forty day period begins:

- the request must be in writing, preferably using the appropriate SAR form
- any fee must have been paid (not exceeding £10) †
- the person making the request must have properly identified him/herself (if the request is by email it needs to be from a Queen Mary address or other details verified)
- enough information must be provided to locate the data (i.e. the request must be sufficiently clear as to what is being sought: a Data Subject can't simply say "give me everything you have on me" and expect a full response) *
- there must not have been repeated or similar requests from the Data Subject unreasonably close in time (if so, it may not be necessary to respond)
- there must not be a 'disproportionate effort' involved in responding to the request (although this is a difficult point to argue)

† this fee will be waived for basic requests from current students such as a minute from an examination board

* data which may be produced in the event of an SAR is usually to be found in what the Act defines as a 'relevant filing system'. However, if the request contains a description of the data, the individual would have a right of access to unstructured data. For further details, please use the contact details below.

III. Processing data

When processing personal data it is important that this complies with the eight Data Protection Principles. For example, at the point of collection the form or web page should state the purpose for collection and no data other than that required for that particular transaction should be collected. For help drafting such a fair processing notice please use the contact details below. It is good practice to keep a record of the

consent given as an audit trail. The fair processing notice to students, displayed on (re-)enrolment, makes data sharing between departments possible. Also, appropriate security measures must be taken when storing, moving or transmitting data, such as encryption.

- What to do

At the point of collection the following information should be provided:

- The identity of the Data Controller
- The purpose(s) for which the data is being collected
- The recipients to whom the data may be disclosed (or transferred)
- Details of how to opt-out of any subsequent re-use

III (i) Storage and handling of data

Personal data should be marked with an appropriate classification as per [SOP DG09 – Information Classification](#) and stored and handled (and disposed of) as determined by these. Data is to be given appropriate levels of access control and security. This means that it should be safeguarded by means of lockable cabinets and password and/or encryption protection, depending on format. See [SOP DG14 – Storage of Information](#) and [SOP DG15 – Handling of Information](#).

Handling and exchange of patient information must in addition comply with the [Access to Health Records Act 1990](#) where only those with a professional or contractual duty of confidentiality are permitted access to patient information. Please also see the [Records Management Procedures](#).

- What to do

Make sure you use passwords which are strong and hard to guess. Never share or write passwords down and keep a log of who has access to secure areas. Secure personal information physically by restricting access to only those who need it for the performance of their duties and lock cabinets, rooms and computers when the information is not in use.

III (ii) Sensitive data

Sensitive personal data should only be recorded when the Data Subject has given express consent. The only exceptions are when it is required in order to protect the vital interests of the individual or another person or in the administration of justice. See also the Advice and Counselling Service's [Confidentiality and Data Protection Policy](#).

- What to do

When recording data like absences, extenuating circumstances or disciplinary offences on a file, only brief notes should be made with little or no detail e.g. "absent due to ill health".

IV. Examinations and assessment data

- Exam *scripts* are exempt from the Act
- Examiners' *comments* and marks are not exempt and access may be requested

- What to do

Markers could make their comments on a separate sheet (although it should be remembered that data must be presented in "an intelligible form" to a Data Subject making an SAR). It is acceptable to destroy the marking sheets/scripts once marks have been finalised at the examination board, if this is part of standard procedure. In

all cases markers should be aware that their comments may be read by the candidate, so offensive, subjective or opinionated statements must be avoided. Please see the current Assessment Guide for further details, available on the [Policy Zone](#), and the [ICO's good practice note](#).

IV (i) Automated decisions

If any form of assessment relies purely on automated means then a Data Subject has the right:

- to be informed of the logic behind the process
- to be able to request that decisions are not made solely through the automated process

IV (ii) Disclosure of results

- Telephone queries for exam results should not be answered unless there is a system of security questions/passwords to confirm the identity of the caller
- Publication of results on a notice board may be reasonably expected by students, but to protect identification numbers should be used rather than names
- Exam results *may* be withheld due to non-payment of fees where the debt relates to academic study

- What to do

If exams are not marked until fees are paid then there will be no data to access. However, this could be argued to be a form of student bias and even infringe human rights. Exam results should be provided if an SAR is submitted but re-enrolment or graduation could be prevented. Publishing examination results is a common and accepted practice. Nonetheless, if exam results or classifications are to be published publicly, such as at a degree ceremony, it is good practice to gain consent and offer an opt-out. See also the current Assessment Guide.

NB The timescale for responding to Subject Access Requests that relate to examination marks or results is extended from forty days to:

- five months from the time when the request is received and validated, or
- forty days from the announcement of the examination results, if earlier

IV (iii) Examination boards

- Minutes of examination boards may be subject to access if a candidate is referred to, whether by name or some other identifier

- What to do

Board secretaries should ensure that minutes are purely factual. If access is provided, any other individual's details must be redacted unless they have given their consent to the disclosure.

V. Research

There are specific provisions in the Act for the use of personal data in research (Section 33). The College's Research Ethics Policy should be studied and complied with and an application form should be completed by anyone undertaking research that will be supported by Queen Mary's facilities – this includes sections on 'Confidentiality, anonymity and data storage' and 'Consent'.

- Data used for one piece of research can be re-used in other research for a different purpose (see Research Ethics Policy guidelines on secondary use)
- Research data *may* be kept indefinitely (but not for use in new research)

- Research data is exempt from SAR rules (as long as living individuals are not identified and no substantial damage/distress is caused to any individual)

- What to do

Your research should fulfil all the following criteria:

- the information is to be used *exclusively* for research purposes (includes statistical or historical research purposes) and no other use, not even an incidental one
- the information is not to be used to support measures or decisions relating to *any* identifiable living individual (not just the Data Subject but anyone who may be affected by your research)
- the data must not be used in a way that will cause, or is likely to cause, substantial damage or distress to any Data Subject
- the results of your research, or any resulting statistics, must not be made available in a form that identifies the Data Subjects. For example, if a name of an individual is disguised you would not meet this criterion if you describe their circumstances (such as in a case study) in such detail it may be possible for someone to identify that individual.

Before using personal data in research, approval should be sought from the College's Research Ethics Committee as part of the application process. Where possible informed consent should be obtained from all participants and if this is not possible then data should have all personal identifiers removed. Researchers should adopt a system of anonymous coding (pseudonymisation) as the identity of Data Subjects must not be given away without consent. All data must be processed in accordance with the eight [Data Protection Principles](#) – there is no blanket exemption.

VI. References

- Internal references provided for the purposes of education, training or employment are exempt from SARs

- What to do

Concentrate comments in references on factual matters (e.g. dates of attendance, duties performed); any subjective observations or academic judgements must be based on fact.

- External references sent to Queen Mary *may* only be released if consent has been given by the referee or if it is reasonable in all the circumstances

- What to do

Requests for references could routinely include a note asking the referee to indicate (non-) willingness for its release on request *or* if there is no consent, the text could be redacted so as to remove anything that would reveal the identity of the referee – in reality impractical. For example, Admissions' reference request form states, "Referees are asked to note that the applicant may seek disclosure of this reference under the provisions of the Data Protection Act".

- References provided by Queen Mary are exempt from SARs made to it, but the Data Subject may see the reference if they make an SAR to the third party to whom the reference has been provided

In writing a reference the author should always indicate how long (s)he has known the individual and in what capacity. Again, comments must be factually accurate and honest and subjective personal opinions must be avoided. As a general rule, you are

advised not to include information in a reference that you would not wish the individual concerned to see. Spent disciplinary sanctions must not be referred to (usually six years after case closure). Nonetheless, students would not normally object to the confirmation of attendance, degree classifications etc. which come from prospective employers (NB this type of enquiry should be treated as an FOI request). References provided in a personal capacity by staff should state this clearly and not be provided on Queen Mary stationery. See also the [ICO's guidance](#).

VII. HR records

VII (i) Disciplinary procedures

- The outcome of grievances is only disclosable to the person who is the subject of the process, not to any other parties

- What to do

If there is a disciplinary process against an employee, then only that employee has a right to know the details of that process. For example if an accusation is made by a student or member of staff against another member of staff, expectations should be managed from the start. The accuser does not have a right to be kept informed or to know the outcome of the process. Only tell them that the procedure has been completed when it has, but not how.

VII (ii) Sick notes

- Sick notes contain sensitive personal data and should only be seen by those who need to know

- What to do

Sick notes should not have to be seen by line managers unless explicit consent has been given by the employee.

VIII. Images

- Photos/video taken for official use are covered by the Act and people in them should be advised why they are being taken
- Photos/video showing a crowd scene (e.g. in a public place) would not be considered to be personal data because the purpose of capturing the individuals is not to identify them
- Photos of staff on the intranet need no consent but consent is required if the site is an Internet one

- What to do

Consent should be sought wherever possible, especially of individual shots because they can be readily identified. Where this is not practical for each individual, for example at an event or at a degree ceremony, Data Subjects should be made aware: a statement should appear on tickets/programmes and/or a notice be displayed explaining that photographs/video are being taken and the purpose to which these may be put. All photographers should be clearly identified, e.g. with a visible badge. If taking photographs of children consent must be obtained from a parent or guardian.

If a student or member of staff objects to having a photograph published, on a departmental website for instance, then it must be removed. Prior consent should be sought wherever possible.

The [Creative Services](#) Team can provide a photo release form which Data Subjects should sign if their photo will be used in a College publication.

In addition, individuals whose image has been recorded by CCTV have a right of access to a copy of those images by making a subject access request. This is covered by Queen Mary's [CCTV Policy](#).

IX. Direct marketing

- Data Subjects have the right to ask organisations to stop, or not to start, direct marketing aimed at them

- What to do

It is accepted that, for example, alumni might reasonably expect the College to send a variety of mailings to them. However, alumni (or anyone else receiving direct marketing material) should be advised of their rights and given the opportunity to opt out in every communication.

X. Third parties/countries and outside agencies

The Act makes it clear that it is a serious offence to disclose any personal data to a non-authorised person, including orally. It can usually only be released with the Data Subject's consent, unless one of the exemptions is met or a court order issued.

- When dealing with a third party acting as a Data Processor

- What to do

Parties such as BUPT may process data which has been passed to it by Queen Mary. It is important to ensure that a written agreement is in place covering the services the third party is to provide and that it includes specific provisions covering its responsibilities for the personal data passed on to them (e.g. an obligation to assist the College in responding to an SAR) and references the Act. Ideally the third party should provide an indemnity covering any penalties the College might suffer as a result of their use of the data. The burden is on the College to ensure that Data Processors do not breach the Act. Other data processors of the College might be Barts and The London NHS Trust or the Universities Superannuation Scheme. Note that there exists a Student Personal Information Sharing Agreement between Queen Mary and the Students' Union.

- When personal data may be transferred outside the EEA, going against the eighth principle

- What to do

Personal data may be passed to partnering organisations in countries outside the EEA, such as BUPT, which do not have the same levels of protection for personal data as long as certain safeguards are in place (though there are some exemptions). In this case the other party may become a data processor. The ICO and the Data Subject must be informed prior to any transfer. Details of these safeguards and of standard contractual clauses which may be employed are available from the Records & Information Compliance Manager. See also section XI. below.

- Individual enquiries e.g. from friends or relatives in person, by telephone, email etc. need to be handled with care

- What to do

The correct procedure is to pass any message on to the Data Subject (if over 18) and leave it up to them to contact the caller. Even if the message is from an apparently anxious parent, there is no requirement to reveal details or even confirm the Data Subject exists! If an enquirer telephones (or emails from a non-College account) and

claims to be the Data Subject, to provide some measure of authentication, offer to call back. Otherwise there needs to be some system of security questions/passwords to confirm the identity of the caller. Note that a sponsor does not have any automatic right to a student's marks or progression details without the consent of the student.

- Enquiries from the police or other crime prevention or law enforcement organisations (or revenue-collecting authority)

- What to do

The agency must complete a Section 29 form (available on request) to apply for access specifying the purposes for which it is required. The data must be necessary, not just helpful to these purposes. Even then Queen Mary is not compelled to release the data without the Data Subject's consent: rights and interests should be balanced in coming to a decision. NB Such an enquiry *may* also come from an investigation in to tax/benefit fraud or immigration e.g. from local government or the Home Office/Border Agency. It's important to verify the identity of anyone making such requests and ensure the request is counter-signed by an authorised individual. This should be someone who is senior in rank/position to the requester.

- Protecting the vital interests of the Data Subject or preventing serious harm to a third party

- What to do

The consent of the Data Subject is not required if a failure to release data would result in her or a third party's harm or if required to perform a regulatory function, such as securing health and safety at work. See also the [Missing Students Policy](#).

XI. Which countries outside the European Economic Area have adequate protection for personal data?

The European Commission has recognised the following territories as having adequate data protection:

- Argentina
- Canada
- Switzerland
- Guernsey
- Isle of Man
- Jersey
- United States (under safe harbor rules only)

XII. What other exemptions are there to the release of information?

- Data protection legislation does not cover the deceased
- Data may be released to the police or other law enforcement organisation in pursuit of an active investigation (see X. above)
- Disclosure of data may be necessary in the case of a medical emergency
- The College is legally obliged to pass certain data to certain third parties such as HESA, HEFCE etc.

XIII. What other relevant guidelines are there in the College?

There are other College policies and procedures which are applicable to data protection, for example the [Information Security Policy](#) provides guidance on storage, access, safeguards, removal etc. and the Records Retention Schedule details how long data should be kept. The [Records Retention Policy](#) lays out staff responsibilities.

In addition, the [Guidelines on the right to privacy and the monitoring of data](#) give information on the rights of employees and the right of the College to monitor employees' activities. Students should refer to the Fair Processing Notice that they view on (re-)enrolment too.

XIV. What are the penalties for Data Controllers if they breach the law?

- Section 60(2) of the Act states that fines may be imposed on Data Controllers in breach of the law
- Criminal prosecutions may be brought against not just the directors or trustees of an organisation but also other officers (i.e. employees) who are responsible for a breach. This personal liability is important to note
- A Data Subject can bring a claim for compensation for a breach which resulted in their suffering damage or distress
- A Data Subject can also apply to the courts for an order which: requires the Data Controller to comply with an SAR; requires it to stop processing their data where it is being used for direct marketing or is likely to cause damage or distress; or, requires erasure/rectification of data where it is inaccurate
- The Information Commissioner may serve an enforcement notice on a Data Controller if an investigation results in a finding that one of the eight principles has been breached. The Information Commissioner sets out the remedial steps which need to be taken by the Data Controller in question and failure to comply with these instructions would also be a serious offence under the Act
- Other legislation may be applicable, for example monetary penalties for data breaches can be issued under the Criminal Justice and Immigration Act 2008

XV. What if I want to process data for a purpose not covered by the College's notification to the ICO?

Any new purposes must be added to the College's Registration with the ICO before the processing of data begins. Therefore, you must inform the Records & Information Compliance Manager to notify the ICO to make the amendment. Note that the Students' Union has its own separate notification (reg. no. Z520302X).

XVI. Who has the authority to report any breaches?

Any (suspected) breaches should be notified to the U.K. Information Commissioner. Although there is no legal obligation on Data Controllers to report breaches of security which result in loss, release or corruption of personal data, the Information Commissioner believes serious breaches should be brought to the attention of his Office.

XVII. Who in Queen Mary can I contact for more advice?

The Records & Information Compliance Manager can be contacted on ext. (13) 7596 or by emailing data-protection@qmul.ac.uk