Introduction

KCLSU needs to keep certain information about employees, students and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, activities organized and legal obligations to funding bodies, regulators and government complied with. To comply with the law, information must be used fairly, stored safely and not disclosed to any other person unlawfully. To do this, KCLSU must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act). In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

KCLSU and all officers, staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, KCLSU has developed this Data Protection Policy.

Status of the Policy

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by KCLSU from time to time. Any failure to follow the policy can therefore result in disciplinary proceedings.

Any member of staff who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the Data Controller initially. If the matter is not resolved it should be raised as a formal grievance.

Notification of Data Held and Processed

All staff, students and other users are entitled to

- Know what information KCLSU holds and processes about them and why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what KCLSU is doing to comply with its obligations under the 1998 Act.

KCLSU will update staff data at least annually. Students' data are updated annually through various processes, including enrolment in activities, data import from King's College, etc.

Responsibilities of Staff

- Checking that any information that they provide to KCLSU in connection with their employment is accurate and up to date.
- Informing KCLSU of any changes to information, which they have provided. E.g. changes of address
- Checking the information that KCLSU will send out from time to time, giving details of information kept and processed about staff.
- Informing KCLSU of any errors or changes. KCLSU cannot be held responsible for any errors unless the staff member has informed KCLSU of them.

If and when, as part of their responsibilities, staff collect information about other people, (eg about students' course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff.

Data Security
All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely.
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorized third party.

Staff should note that unauthorized disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information should be

- kept in a locked filing cabinet; or
- in a locked drawer; or
- if it is computerized, be password protected; or
- kept only on disk which is itself secure.

Student Obligations
Students must ensure that all personal data provided to KCLSU are accurate and up to date. They must ensure that changes of address, etc are notified to the student registration office/other person as appropriate.

Students who use KCLSU computer facilities may, from time to time, process personal data. If they do they must notify the designated Student Data Controller. Any student who requires further clarification about this should contact the designated Student Data Controller.

Rights to Access Information
Staff, students and other users of KCLSU have the right to access any personal data that are being kept about then either on computer or in certain files. Any person who wishes to exercise this right should complete KCLSU "Access to Information " form and hand it in to the General Office, which will forward it to the Data Controller.

In order to gain access, an individual may wish to receive notification of the information currently being held. This request should be made in writing using the standard form

attached.

KCLSU will make no charge for the first occasion that access is requested, but may make a charge of £10 per each subsequent request at its discretion.

KCLSU aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 21 days unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

Subject Consent

In many cases, KCLSU can only process personal data with the consent of the individual. In some cases, if the data is sensitive, **express consent** must be obtained. Agreement to KCLSU processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes information about previous criminal convictions.

Some jobs or courses will bring the applicants into contact with children, including young people between the ages of 16 and 18. KCLSU has a duty under the Children Act and other enactments to ensure that staff are suitable for the job, and students for the courses offered. KCLSU also has a duty of care to all staff and students and must therefore make sure that employees and those who use KCLSU facilities do not pose a threat or danger to other users.

KCLSU will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. KCLSU will only use the information in the protection of the health and safety of the individual, but will need consent to process in the event of a medical emergency, for example. Therefore, all prospective staff and students will be asked to sign a Consent To Process form, regarding particular types of information when an offer of employment or a course place is made. A refusal to sign such a form can result in the offer being withdrawn.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details. This may be to ensure KCLSU is a safe place for everyone, or to operate other College policies, such as the sick pay policy or equal opportunities policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students will be asked to give express consent for KCLSU to do this. Offers of employment or course places may be withdrawn if an individual refuses to consent to this, without good reason. More information about this is available from the Data Controller.

The Data Controller and the Designated Data Controller/s

KCLSU as a body corporate is the Data Controller under the Act, and the board is therefore ultimately responsible for implementation. However, there are designated Data Controllers dealing with day to day matters. The first point of contact for enquirers is

Bryan Taylor, ext 1354

who may either deal with the enquiry himself or refer it to another designated data controller.

Retention of Data
KCLSU will keep some forms of information for longer that others. Because of storage problems, information about students cannot be kept indefinitely, unless there are specific requests to do so. A list is attached of the archiving guidelines and retention times employed by KCLSU.

Disposal of Data
When personal data is no longer required, or has passed its retention date, paper records must be shredded. If there is a significant amount of material which cannot be dealt with by normal shredding machines, this should be disposed of using a reputable disposal contractor.
Computerised records must be permanently deleted, with particular care taken that 'hidden' data cannot be recovered. The appiChar Helpdesk can advise on permanent deletion of computerised records.

Conclusion
Compliance with the 1998 Act is the responsibility of all members of KCLSU. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to KCLSU facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated Data Controller.

Appendices

1 Staff Guidelines for Data Protection (including checklist for recording data)
2 Standard Request for Access to Data
3 Standard Form for consent to process sensitive data
4 Standard Form for notification of Personal Data held by KCLSU
5 Guidelines for archiving
6 CRB retention Policy

Appendix 1 to the Data Protection Policy : Staff Guidelines for Data Protection

1. All staff will process data about students on a regular basis, when processing membership information. King's College London ensures, through registration procedures, that all students give their consent to this sort of processing, and are notified of the categories of processing, as required by the 1998 Act. The information that staff deal with on day-to-day basis will be 'standard' and will cover categories such as:

- General personal details such as name and address,
- Details about enrolment
- Details about involvement

2. Information about a student's physical or mental health; sexual life; political or religious views; trade union membership or ethnicity or race is sensitive and can only be collected and processed with the student's consent. If staff need to record this information, they should use KCLSU standard form.
Examples : recording information about dietary needs, for religious or health reasons prior to taking students on a field trip; recording information that a student is pregnant, as part of personal duties.

3. All staff have a duty to make sure that they comply with the data protection principles, which are set out in KCLSU Data Protection Policy. In particular, staff must ensure that records are:

- accurate;
- up-to-date;
- fair;
- kept and disposed of safely, and in accordance with KCLSU policy.

4. KCLSU will designate staff as 'authorised staff'. These are the only staff authorised to hold or process data that are :

not standard data; or
sensitive data

The only exception to this will be if a non-authorised staff member is satisfied that the processing of the data is necessary :

in the best interests of the student or staff member, or a third person, or KCLSU;

AND

he or she has either informed the authorised person of this, or has been unable to do so and processing is urgent and necessary in all the circumstances.

This should only happen in very limited circumstances.

Example : A student is injured and unconscious, but in need of medical attention, and a student support staff member tells the hospital that the student is pregnant or a Jehovah's witness.

5. Authorised staff will be responsible for ensuring that all data is kept securely.

6. Staff must not disclose personal data to any student, unless for normal membership administration purposes, without authorisation or agreement from the data controller, or in line with KCLSU policy.

7. Staff shall not disclose personal data to any other staff member except with the authorisation or agreement of the designated data controller, or in line with KCLSU policy.

8. Before processing any personal data, all staff should consider the checklist.

Staff Checklist for Recording Data

Do you really need to record the information?

Is the information 'standard' or is it 'sensitive?

If it is sensitive, do you have the data subject's express consent?

Has the student been told 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?

Are you sure that the data is secure?

If you do not have the data subject's consent to process, are you satisfied it is in the best interests of the student or the staff member to collect and retain the data?

Have you reported the fact of data collection to the authorised person within the required time?

Appendix 2 to the Data Protection Policy : Standard Request Form for Access to Data

Standard Request Form for Access to Data
I, _____*(insert name)* wish to have access to either

(delete as appropriate)
1. All the data that KCLSU currently has about me, either as part of an automated system or part of a relevant filing system; or
2. Data that KCLSU has about me in the following categories (please tick):

☐ Academic enrolment details
☐ Disciplinary records
☐ Health and medical matters
☐ Political, religious or trade union information
☐ Any statements of opinion about my abilities or performance
☐ Personal details including name, address, date of birth etc.
☐ Other information : please list below

_____
(Please tick as appropriate)

I understand that I will have to pay a fee of £
(Fee of £10 per request payable for second and subsequent requests for the same category(ies) of information within a twelve month period)

Signed

Dated

Appendix 3 to Data Protection Policy : Standard form for Consent to Process Sensitive Data

Standard Form For Consent To Process Sensitive Data

I _____*(insert name)* give my consent to KCLSU recording and processing information about me in the following categories:

Race and ethnic origin
Membership of a trade union
Physical or mental health or medical condition
Criminal records

The information will be used for the following purpose:

Administering sick pay and sick leave schemes;
Managing the absence control policy
Checking suitability and fitness to work at KCLSU
Checking suitability and fitness for placements
Administering KCLSU and statutory maternity leave and pay schemes
Managing and maintaining a safe environment
Managing duties and obligations under the Disability Discrimination Act
Statistical Monitoring to ensure that KCLSU complies with Equal Opportunities good
practice

I understand that this information will be used only for the purpose set out in the statement above, and my consent is conditional upon KCLSU complying with their obligations under the Data Protection Act 1998.

The particular information to be recorded and processed has been shown to me on

_____
(insert date)
and I confirm that it is correct.

NB: KCLSU Data Protection Policy stipulates that individuals will be advised of any sensitive data to be processed about them.

Signed

Dated

Appendix 4 to Data Protection Policy : Standard Form for Notification of Personal Data

Standard Form for Notification of Personal Data held by KCLSU

This notice is served as part of the requirement of the Data Protection Act 1998. It sets out the types of personal data that we currently hold about you, and gives details of that data.

When you receive this form you should

- **Check that the information included about you is correct**
- **Tell us if there are any errors or if any of the data is incomplete**
- **Ask to see any of the information if you want further details**

We cannot provide all the data on this form, but you do have the right to access most of the information we have about you.

We currently hold information in the following categories:

1. Personal details: this includes, name, address; next of kin

2. Details of physical and/or mental health: this includes details about specific conditions individuals may suffer from, such as asthma or diabetes: information about pregnancy, if appropriate, information about sickness absences and any medical reports we may have received.

3. Membership/non membership of trade unions

4. Details about course registration and student group involvement

5. Details about employees work performance, including notes of supervision sessions, appraisals, and training assessment.

6. Personnel information. This includes details about start date; pension and pay details; your next of kin; any current disciplinary or grievance matters; any deductions from salary or any loans.

7. Details about any criminal record

8. Other categories (should list other categories of data held, following the audit of data systems)

Signed on behalf of KCLSU_____

Dated

Appendix 5 to Data Protection Policy : Guidelines for Archiving

Type of Data	**Retention Period**	**Reason**
Personnel Files; training records; notes of grievance and disciplinary hearings	6 years from the end of employment	Provision of references and limitation period for litigation
Staff Application forms; interview notes	1 year from the date of the interviews	Limitation period for litigation
Facts relating to redundancies (less than 20)	3 years from the date of redundancies	Limitation period for litigation
Facts relating to redundancies (20 or more)	12 years from the date of redundancies	Limitation period for litigation
Income Tax and NI returns; correspondence with Tax Office	3 years after the end of the financial year to which the records relate	Income Tax (Employment) Regulations 1993
Statutory Maternity Pay records and calculations	3 years after the end of the financial year to which the records relate	Statutory Maternity Pay (General) Regulations 1986
Statutory Sick Pay records and calculations	3 years after the end of the financial year to which the records relate	Statutory Sick Pay (General) Regulations 1982
Wages and salary records	6 years from the last date of employment	Taxes Management Act 1970
Records and reports of accidents	3 years after the date of the last entry (or in the case of students under 18, 3 years after their 18th birthday)	RIDDOR 1995
Health Records	During Employment	Management of Health and Safety at Work Regulations
Health Records where reason for termination of employment is concerned with health, including stress related illness	3 years	Limitation period for personal injury claims
Medical Records kept by reason of the Control of Substances hazardous to health	40 years (general monitoring records 5 years)	COSHHR 2002
Student Records	10 years	Provision of references.
CRB disclosures	2 years	Limitation of validity

Appendix 6 to Data Protection Policy : CRB Data retention

General principles
As an organisation using the Criminal Records Bureau (CRB) Disclosure service to help assess the suitability of applicants for positions of trust, KCLSU complies fully with the CRB Code of Practice regarding the correct handling, use, storage, retention and disposal of Disclosures and Disclosure information. It also complies fully with its obligations under the Data Protection Act 1998 and other relevant legislation pertaining to the safe handling, use, storage, retention and disposal of Disclosure information and has a written policy on these matters, which is available to those who wish to see it on request.

Storage and access
Disclosure information should be kept securely, in lockable, non-portable, storage containers with access strictly controlled and limited to those who are entitled to see it as part of their duties.

Handling
In accordance with section 124 of the Police Act 1997, Disclosure information is only passed to those who are authorised to receive it in the course of their duties. We maintain a record of all those to whom Disclosures or Disclosure information has been revealed and it is a criminal offence to pass this information to anyone who is not entitled to receive it.

Usage
Disclosure information is only used for the specific purpose for which it was requested and for which the applicant's full consent has been given.

Retention
We do not keep Disclosure information for any longer than is necessary. This is generally for a period of up to two years (the full validity of the Disclosure), to allow for the consideration and resolution of new project applications, as well as any disputes or complaints. Throughout this time, the usual conditions regarding the safe storage and strictly controlled access will prevail.

Disposal
Once the retention period has elapsed, we will ensure that any Disclosure information is immediately destroyed by secure means, i.e. by shredding, pulping or burning. While awaiting destruction, Disclosure information will not be kept in any insecure receptacle (e.g. waste bin or confidential waste sack). We will not keep any photocopy or other image of the Disclosure or any copy or representation of the contents of a Disclosure. However, notwithstanding the above, we may keep a record of the date of issue of a Disclosure, the name of the subject, the type of Disclosure requested, the position for which the Disclosure was requested, the unique reference number of the Disclosure and the details of the recruitment decision taken.

Acting as an Umbrella Body
Before acting as an Umbrella Body (one which countersigns applications and receives Disclosure information on behalf of other employers or recruiting organisations), we will take all reasonable steps to satisfy ourselves that they will handle, use, store, retain and

dispose of Disclosure information in full compliance with the CRB Code and in full accordance with this policy. We will also ensure that any body or individual, at whose request applications for Disclosure are countersigned, has such a written policy and, if necessary, will provide a model policy for that body or individual to use or adapt for this purpose.