• ISS INFORMATION GOVERNANCE & COMPLIANCE •

Data Protection

KING'S College LONDON

A brief guide for staff and students

The Data Protection Act 1998 sets out the legislative framework for managing personal information. This includes student records, staff files and personally identifiable research data. The Act establishes mandatory standards for information handling and provides a right of access by data subjects to all of the information that the College holds about them.

The Information Commissioner's Office (ICO) oversees compliance with the Act and maintains a public register of organisations that use personal data. The ICO handles complaints from individuals and can take action against organisations that are in breach of the Act.

Scope of the act

The Act regulates the 'processing' of '**personal data**'. 'Processing' has a very wide definition and includes collecting, holding, using and destroying.

Personal data is defined as:

- Information which relates to a **living** individual
- Information from which an individual can be identified, either directly or indirectly
- Information including expressions of opinion about an individual or indications of the intentions of anyone in respect of that individual

Personal data across the College is varied and diverse and includes:

- Paper student files, emails that discuss students, student database records
- Staff files, payroll records, appraisal forms and training records
- Identifiable research records including interview transcripts, images or databases of names and addresses

Sensitive personal data

In addition to defining personal data generally the Act identifies a special category of information – **sensitive personal data**.

Sensitive personal data includes information about an individual's:

- Racial or ethnic origin
- Political opinions
- Religious beliefs
- Trade Union membership
- Physical or mental health
- Sexual life
- Criminal record

Information of this kind is often caught in student, staff and research records. It must be handled with particular care and consideration.

The data protection principles

At the heart of the Data Protection Act are eight principles of good information handling. All personal data must be managed in compliance with these principles. Compliance is the responsibility of everyone at College who collects or uses personal data, both staff and students.

Principle	What it says	What it means
Principle 1	Personal data shall be processed fairly and lawfully.	Data should be processed with consent and rights of privacy should be respected.
Principle 2	Personal data shall only be processed for the purposes for which it was collected.	Data collected for one purpose should not be used for another without fresh consent. For instance an email list of research study participants should not be used for commercial marketing.
Principle 3	Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is processed.	Only the information required to do the job should be collected and used.
Principle 4	Personal data shall be accurate and, where necessary, kept up to date.	Data quality should be maintained. For instance we should avoid multiple databases of student information and maintain instead a single integrated record.
Principle 5	Personal data shall not be kept for longer than necessary.	When personal records are no longer required they should be destroyed securely, in line with College policy.
Principle 6	Personal data shall be processed in accordance with the rights of data subjects.	Individuals' personal rights to access their own data must be respected and data should not be shared beyond the College without consent.
Principle 7	Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage.	Personal information must be stored securely. Paper files should be locked away and electronic records should be protected by passwords and encryption.
Principle 8	Personal data shall not be transferred outside of the European Economic Area (EEA) unless an adequate level of protection can be ensured.	Transfer beyond the EEA must be to a territory, partner or contractor who can assure us that their data handling will meet DPA standards.

There are exemptions to some of these principles for special purposes including crime, taxation and, in certain circumstances, research. These exemptions are conditional and limited though.

Right of access

The Act gives individuals a right of access to their own data. This means that staff, students, alumni, donors, contractors, research participants and others can all request copies of the information that we hold about them including paper records, electronic files and emails.

If any of the information that we hold is incorrect a data subject has the right to have it amended. This may involve correcting a record in a database or adding a note to a paper file.

Dealing with access requests

Data protection requests at King's are coordinated centrally by the Information Governance and Compliance (IGC) team.

For staff and researchers dealing with data subjects at first hand though, the following guidance should prove useful:

- Data subjects must make their information requests in writing and provide proof of their identity.
- They are required to be as clear as possible about the information that they are looking for. So, 'please send me a copy of my student file' would be a valid request whereas, 'please send me copies of all the information you hold about me' would need more clarification.
- The College may charge £10 for processing requests and we are allowed up to 40 days to respond in full.
- Data subjects should be directed to the IGC web pages to make a formal data protection request: www.kcl.ac.uk/iss/igc/dpa

Requests by third parties

The Data Protection Act exists to protect the privacy of individuals so you have no right of access to the personal data of anyone other than yourself. The implication of this is that data should never be disclosed beyond the College without consent. Even spouses, parents, friends and sponsors are not entitled to access a data subject's information.

There are some conditional exemptions to this rule:

- A range of specified information can be disclosed for regulatory and reporting reasons to bodies including HESA, local education authorities and research councils.
- Information relating to crime detection or to the collection of taxes can be disclosed to the Police, the Inland Revenue and to council tax offices. Proper procedures should be followed here so that only necessary information is disclosed and the correct formal paperwork is used.
- Personal data can be disclosed in emergencies when the health, safety or other vital interests of a data subject are engaged. For instance, it would be legitimate to share the personal address or phone number of a student if they were otherwise at risk of danger.

If asked for personal information by a third party it is always crucial to check whether they are entitled to it and to confirm their identity. If you are unsure, seek advice.

Issues for researchers

Research is significantly affected by the Data Protection Act and it is important that researchers fully understand their responsibilities.

More detail can be found on our website, but the following points are crucial:

- All research involving human participants must gain ethics approval.
- Participants must consent fully and freely to the use and reuse of their personal data.
- Identifiable data can only be reused for secondary research under certain conditions; if you are unsure, seek advice.
- Personal data should usually be anonymised and should only be published in identifiable form with consent.
- Research data may have ongoing value beyond a single study. Data can be retained for research purposes in compliance with the Data Protection Act, though certain conditions apply.

Misuse of personal data by researchers is a serious offence. It is a breach of College regulations and may be a civil or criminal offence too.

Where do I go for further information and support?

The Information Governance and Compliance team are happy to help further.

- Visit our website for up to date guidance and FAQs www.kcl.ac.uk/iss/igc
- Visit our training page to find out about data protection courses www.kcl.ac.uk/iss/igc/training
- Contact our legal compliance experts directly legal-compliance@kcl.ac.uk

Useful references

The Data Protection Act 1998
http://www.opsi.gov.uk/Acts/acts1998/ukpga_19980029_en_1

The Information Commissioner's Office (ICO)
http://www.ico.gov.uk/what_we_cover/data_protection.aspx

JISC Legal
http://www.jisclegal.ac.uk/LegalAreas/DataProtection.aspx