Student work and compliance with the Data Protection Act

Approval of proposed work by supervisors

Any work undertaken by students involving the processing of data which relates to identifiable living individuals must comply with the Data Protection Act 1998 (DPA). Departments and supervisors need to have a clear understanding of the data protection requirements regarding student research.

The University is responsible for any use of personal data by students in the course of their studies. It should normally be covered by the University’s notification with the Information Commissioner’s Office, which can be found at [http://www.ico.gov.uk/ESDWebPages/DoSearch.asp?reg=5518409](http://www.ico.gov.uk/ESDWebPages/DoSearch.asp?reg=5518409) and is intended to cover all legitimate uses of personal data for educational and research purposes. Students must not process personal data, using University facilities, for any reason other than those connected with their studies.

Departments should have a procedure in place covering the approval of student research which involves the processing of personal data. This should entail supervisors assessing and authorising such work before it is started. Advice should always be sought from Information Assurance Services if there are any doubts over compliance with the legislation or best practice.

The supervising member of staff should:

a) If unsure, check with Information Assurance Services whether the processing is covered by the University’s notification with the Information Commissioner’s Office.

b) Ensure that the student complies with the DPA (in particular with the eight data protection principles: [http://www2.le.ac.uk/offices/ias/dp/act/principles](http://www2.le.ac.uk/offices/ias/dp/act/principles)) and the Data Protection Code of Practice for Students contained within the Student Regulations ([http://www2.le.ac.uk/offices/ias/dp/studentdata](http://www2.le.ac.uk/offices/ias/dp/studentdata)).

c) Ensure that in the event of a request for access to personal data the relevant material can be supplied in a timely manner.

d) Ensure that the data is deleted or destroyed when it is no longer required.

The University retains control at all times of any personal data used by students in the course of their work. Students must seek the approval of the University before any such information can be disclosed to any external party. Supervisors need to emphasise this requirement for students and should seek guidance from Information Assurance Services if a student seeks consent for such a disclosure.
Student work and compliance with the Data Protection Act

Processing of personal data by students

Personal data is any information which identifies a living individual, either on its own or in conjunction with other information, and can be electronic or hard copy material. The Data Protection Act 1998 (DPA) covers any action performed with personal data (collecting, recording, consulting, amending, using, disclosing, deleting etc).

The DPA contains an exemption that relaxes, to a certain extent, the rules that apply to personal data used for research purposes but nevertheless the following general rules do need to be followed:

i) Any processing of personal data needs to be fair and for a specified purpose. The best way to ensure this is to obtain the consent of the research subjects. Where data is being obtained from individuals a fair processing notice should be issued explaining the following:
   a) What information is being collected
   b) What it will be used for
   c) How long it will be retained
   d) Who it is likely to be shared with
   e) Whether it is likely to be published

ii) If the work involves sensitive personal data (ethnicity, political opinions, religion, trade union membership, physical or mental health, sexuality, criminal record) then the explicit consent of the research subjects is required for its processing. This is best obtained via a consent form, containing the information outlined above, that should be signed by the individual.

iii) Unless required by the nature of the research project, data should be anonymised. The use of a code or key to identify individuals may be appropriate in some scenarios but note that this does not fully anonymise the data; all identifiers need to be destroyed for data to be fully anonymised.

iv) The personal data obtained should be no more than is sufficient to achieve the purpose of the work and should only be kept for as long as is genuinely necessary for this purpose. It should be deleted or destroyed when no longer needed.

v) The security of personal data held by the University and its staff and students is of paramount importance and all personal data should be held, processed and transported in a secure manner at all times. All appropriate measures need to be taken against unauthorised processing and accidental loss of personal data. Particular attention to security matters is required if large amounts of personal data, or any amount of
sensitive personal data, is involved and the use of encryption is likely to be necessary. IT Services and Information Assurance Services can provide further advice and the University’s Information Security Policies, which must be complied with at all times, contain relevant guidance: [http://www2.le.ac.uk/offices/ias/resources/policies/ispolicy](http://www2.le.ac.uk/offices/ias/resources/policies/ispolicy)

vi) Supervisors and students need to be aware of restrictions surrounding sending and transporting personal data to countries outside of the European Economic Area (EEA). This could be a physical or electronic transfer, for instance in the course of a collaborative research project. If a country does not provide adequate data protection this could breach UK law.

vii) Where work involving personal data is undertaken in collaboration with other bodies or institutions a clear agreement needs to be in place outlining who controls the data, what data will be shared and how. The research subjects need to be made aware of these details.

viii) Individuals may be able to request access to their personal data which is held by students for the purpose of their academic work. Any approaches of this nature should be forwarded to Information Assurance Services immediately.

All of these factors need to be considered before a supervisor gives approval for a student to undertake work involving personal data. Non-compliance with any of these elements could involve the University breaching UK law so proposed student work involving the processing of personal data must be subject to an approval procedure with the supervisor acting as a first line of control. Information Assurance Services can provide advice and assistance with any element of this. Please contact [ias@le.ac.uk](mailto:ias@le.ac.uk).