

<b>Document Title</b>	<b>Code of Practice 7: Protection of certain categories of personal data – students and research data</b>
Version	02/12/20
Author	Information Compliance Manager, VCO
Owning Department	Vice-Chancellor’s Office
Approval Date	02/12/20
Review Date	31/12/22
Approving Body	Information Assurance and Security Committee
Relevant to	All academic and professional services staff and students

1. The University, including individual supervisors, is responsible for personal data which is processed by students, where:
  - The student is processing the personal data for the purpose of research or study, or
  - In pursuit of an academic qualification, and
  - Is under the supervision of a member of staff.
  
2. Students must not process personal data unless and until they have permission from their supervisor and (where relevant for research purposes) from UREC / FREC.
  
3. Students should not be granted access to University held personal data (other than data created by themselves or about themselves), unless the student is also a member of staff and access is necessary for the fulfilment of their employment duties.
  
4. All staff and students collecting and processing research data should ensure that the Data Protection principles are adhered to.
  - Staff supervising research students should ensure that this happens. Refer to Code of Practice 1 for more information.
  - For consent from research participants to be valid, it must be fully informed and freely given.
    - Participants must be able to understand what they are agreeing to participate in.
    - Subjects should know that their participation is optional, and that they can withdraw their consent.
    - A nil response to a request for consent does not signify freely given consent.
    - It is not necessary to require specific consent, if it would constitute disproportionate effort to do so, and the research would not cause significant damage or distress to the participant. The collection of sensitive personal data, however, always requires consent.
  - Research data can be held indefinitely, if necessary, however good practice would be to have a fixed retention period.
  - Researchers should be aware of who has access to research data in accordance with the protocols of the relevant committee.

- Researchers should have clear security measures in place to guard against unauthorised access or accidental loss, damage or destruction of the data.
  - Personal data collected for research purposes is exempt from disclosure to the data subject.
5. Students and staff should be aware that they may need to go through the correct ethical processes for research.