6.3 Guidelines on Security and Confidentiality for Staff Working in EUROCAT Central Registry

1. All personal data are regarded as confidential.

2. The Data Protection Act 1998 legislated on the fair obtaining, processing, storing and disclosure of data held on computer, paper or in machine form.

3. Security of data within EUROCAT Central Registry is maintained by careful procedures to maintain:

   a) The physical environment

      i EUROCAT data are held on personal computers for which passwords are required. It is backed up to a network drive to which only Central registry staff have access.
      ii The EUROCAT office (administration and data management) is accessed through a door with a special security lock. Filing cabinets with case information are locked.
      iii Central registry staff will work on individual data within this office only, except where written permission is given by the Project Leader.

   b) Staff practices and procedures regarding security of EUROCAT premises:

      All windows and doors must be secured at night and during prolonged absence from the room.

      All visitors must be accompanied while on the premises.

      Only EUROCAT staff, the Head of Security, university security staff, out of hours security staff providers “Resource” and cleaning staff at the University of Ulster also provided by “Resource” hold the key to the EUROCAT office. Master keys are controlled by a tracker key management system, and are signed in and out.

      Room access for system support purposes will only be available between 8am and 6pm in the presence of other EUROCAT staff.

      Staff must always “log out” of their terminal/PCs when leaving the office to attend meetings if the office is not attended by another member of staff.

      A back-up of the Central Database will be taken weekly (or more often if required) and stored in a locked filing cabinet in the office.

      Archives of data files used for publications or studies will be held for up to 5 years following publication, stored in a locked filing cabinet in the administrative office. Archive files will contain only the cases and the variables used for the study, together with the local ID number in the event that case lists need checking.

      The passwords for the computer system will be frequently changed.

4 Central registry staff may analyse any data in the Central registry database for purposes in keeping with EUROCAT objectives approved by the Project Leader, and for internal communication. Any publication of data must first be approved by both the Steering Committee and contributing registries, and is subject to the agreed authorship guidelines (see EUROCAT Terms and Conditions at http://www.eurocat-network.eu/aboutus/requestingeurocatdata).

5 Transport of Data

(a) Transfer/transport of information will periodically be reviewed.

(b) Data files for transmission by local registries or Central Registry should be password protected where possible to ensure security and confidentiality. The password should be sent separately. Emailed data should be sent to Ruth Greenlees at r.greenlees@ulster.ac.uk. The next version of EUROCAT Data Management Program may include a data encryption facility.

(c) Day and month of birth should be removed from individual data files leaving Central Registry except where express permission has been obtained on the basis of declared need for this information, security of information, and destruction when no longer needed.