POLICY ON PHYSICAL SECURITY OF IT EQUIPMENT

Policy on Physical Security of IT Equipment

(1) All IT Assets should be included in the University's Asset Register as mandated by the Finance Directorate.

(2) All infrastructure hardware (servers, switches etc.) must be located in secure computer rooms, data centres or communications rooms. These rooms must be lockable and access to these rooms should be restricted to members of staff who require access as part of their routine jobs. All visitors including sub-contractors or staff who do not routinely require access must be appropriately supervised when given access to such restricted areas.

(3) All end user devices (desktops, laptops, tablets, USB hard drives etc.) must be securely stored when not in use. For desktop PCs this can be in a locked office. For equipment that is easily removable such as laptops, tablets, USB hard drives this must be stored out of sight in a locked desk, filing cabinet, cupboard or similar. An alternative is to secure the device with a Kensington lock.

(4) Staff travelling with University IT equipment (e.g. laptops & tablets) must take all reasonable precautions to ensure that such equipment is secure at all times and must comply with:

   a. Protection of Information held on Mobile Devices and Encryption Policy; and
   b. Remote Access to University provided Information Systems and Services Policy.

(5) Lost or theft of any device used to hold University information should be immediately reported to the Information Services Helpdesk. This includes mobile phones and laptops used to access University email.