

## **LSHTM Information Management and Security Policy**

### **Supporting Policy 7 - User Management Policy**

Endorsed by Academic Affairs - July 2014

1. All users must be registered on a central database managed by IT Services. All users have one or more unique identifier(s) (user ID) for their personal and sole use for access to all the School's information services. The user ID must not be used by anyone else and associated passwords shall not be shared with any other person for any reason whatsoever.
2. IT Services will ensure that a system for password management is maintained, to ensure the implementation of the requirements of the Information Management and Security Policy.
3. Access control standards are established for all information systems, at an appropriate level for each system, which minimises information security risks yet allows the School's business activities to be carried out without undue hindrance. A review period will be determined for each information system and access control standards will be reviewed regularly at those intervals.
4. Access and removal of access to all systems will be managed by IT Services and must be authorised by the service owner. A record must be maintained of such authorisations, including the appropriate access rights or privileges granted.
5. Persons accessing systems remotely to support business activities must be authorised to do so by an appropriate authority within the organisation.
6. Access to LSHTM's email system will be managed by IT Services and users will comply with the LSHTM email policy.