

Birkbeck, University of London

Malet Street, Bloomsbury

London WC1E 7HX

**Network Security Policy**

1. **Introduction**

 The IT network and the computer systems connected to it are critical to administrative, teaching and learning, and research activities of the College.

The network permits high-speed connections to the Internet and is at present operated with a minimum of restrictions to enable flexibility of communications between connected computers. This flexibility of operation, however, poses potential security risks. In order to safeguard the stability, integrity and security of the College IT network, steps need to be taken by IT Services (ITS) and each School/Department to ensure that machines under their control are properly managed to minimise the risks.

The objectives of this policy are to:

* ensure that the College’s IT network and computing facilities are adequately protected against misuse or abuse;
* create across the College awareness that appropriate security measures must be implemented to safeguard the effective operation of the IT network;
* ensure that all system administrators and users understand their own responsibilities for protecting the IT network;
* to ensure the high availability of an effective network and to facilitate the rapid tracking down and resolution of any network problems by ITS and others;
* to protect Birkbeck’s reputation;
* help preserve the integrity and privacy of users’ information; and
* to reduce interruptions to the service, and unnecessary calls on support staff.

Personal devices connecting to the Birkbeck wireless network infrastructure via eduroam are not subject to the formal system management described below. However, staff using such devices, including phones for accessing and storing confidential data need to consider the Mobile Device Security Policy.

1. **General policy**

 The following general policy statements apply to all Birkbeck-owned computers in the College:

* Every computer connected to the Birkbeck College network (excluding eduroam wireless network) must be subject to formal system administration.
* Responsibility for administration and security of computers should be assigned to a suitably trained and technically competent member/s of staff.
* The staff assigned to the system administrator role must have adequate time in which to undertake the maintenance of computers under their control.
* Adequate provision of cover during sickness or holidays should be made where key systems may be affected.
* Access to any network connected computer must be via a logon process that identifies and authenticates the user, except where read-only access is given to certain systems (e.g. the Library Catalogue), or unprivileged access is normal and appropriate safeguards are in place (e.g. Web browsers in kiosk mode, access to a contained website).
* Any networked system which will be unused for extended periods (typically several days or more) should be switched off.
* Accounts which remain unused for five months should be disabled where possible.
* Accounts used by system administrators should be cancelled immediately on departure of member of staff.
* No shared accounts will be created, except where absolutely necessary, and under the condition that a list is kept of the users of the account, and that they are jointly responsible for any action taken using the account.
* Accounts should not be re-used, except where absolutely necessary, and under the condition that details are kept of the users of the account.
* Lists of users and their data (such as userids) must not be available to anonymous users or, where possible, to other users and systems administrators.
* Computers in open areas should be physically secured.
* Computers in other areas should be accessible only by authorised persons, and security imposed as appropriate.
* Computers offering services external to the College (e.g. web, email, ftp etc), must be authorised by School or ITS support staff.
* Details of any networked system which is operating as a server (including file serving, print serving, web serving, ftp serving, or applications server) must be given to ITS Systems staff or to School support staff in the cases of Schools responsible for maintaining their own servers (e.g. Computer Science and Information Systems, Biological Sciences, Economics, Mathematics and Statistics,  the Library).
* Access to equipment should be possible at all times (in the event of a report being received by ITS or School support staff out of hours) unless precluded by Health and Safety requirements.
* Personal equipment may not be connected to the College wired network except where the connection is made to a School or Departmental network with the written authorization of the School/Department System Administrator.

In addition to the general policy above, the following sections suggest the responsibilities of three distinct groups:

* Systems Administrators
* IT Services
* Users

1. **Responsibilities of systems administrators**

A nominated Systems Administrator should be appointed by Schools and Departments who is responsible for the secure operation of their computers. This may be an individual responsible for a collection of systems, or the user who normally uses the system (in particular for office equipment). The responsibilities of system administrators should include:

* Installing and maintaining the operating system and network connection in order to reduce the chance of unauthorised access.
* Ensuring that systems security patches are kept up to date where possible and such that the service is not adversely affected.
* Monitoring Systems in order to detect breaches in security. In the event of any breach ITS Systems staff must be alerted.
* Restricting the use of privileged accounts. Users including systems administrators, should normally login with userids without unnecessary (“superuser”) privileges. Privileged accounts should be used only for systems administrative work and monitoring.
* When undertaking systems work demanding privileged user status, administrators should login in under their own account before assuming privileged status (to maintain audit information).
* Ensuring that all software is properly licensed.
* Ensuring adequate backup procedures are in place.
* Ensuring adequate virus protection software must be installed.
* Changing passwords regularly and restricting knowledge of the super-user password.
* Providing a copy of Superuser and system administrator passwords to ITS or School/Dept Computer staff for use in emergency.
* Maintaining logging information, and in particular a record of logins on the computer, for one year.
* Administrators must not amend any audit or system information which may be used as part of an audit trail in cases of security breach.
* If necessary to protect or maintain service, administrators will disconnect a system, individual workstation, or software from the School.
* Monitoring activity and/or record traffic on the network if appropriate, including periodic intrusion detection testing either internally or by third party.
* Ensuring that adequate security (such as dial back or secure protocols) is utilized when connecting out of band equipment to allow remote management/troubleshooting.

Administrators should also operate within the guidelines of the Charter for System and Network Administrators prepared by Janet.

1. **Responsibilities of IT Services**

In addition to the above (for systems maintained by ITS), ITS will also:

* Liaise with external organizations (such as UCL Network Group and Janet) in the development and maintenance of the network.
* Inform system administrators of security information, hacking attempts, tools etc via an email list.
* Provide information and good practice guidelines.
* Assist School/Dept Systems Administrator to correct a security or breach, especially where the integrity of the network may be at risk, or it is affecting systems elsewhere.
* If necessary to protect and maintain service, disconnect a system, individual workstation, software, School network or building from the wider College network.
* Monitor activity on the network, including periodic intrusion detection testing either internally or by third party. If during a scan an obvious weakness is found, ITS will provide advice and assistance to the appropriate systems administrator.
* If no administrator is available, depending on the nature of the loophole, the offending system may be disconnected from the network.
* Maintain central checking of malicious code, including of email passing through central mail systems.
* Maintain site licences of virus protection software.
* Coordinate the development and maintenance of the security policy.
* Maintain perimeter firewall and internal rules to protect the College’s computer infrastructure.

1. **Responsibilities of users**

Authorised users have access to computing facilities, software, electronic mail and network services located at Birkbeck and other sites. With these facilities there are direct and implied responsibilities on the part of the College and on the user. Some of the following are highlighted here, but may be more appropriate in an Acceptable Use Policy or an Email and Web Policy.

5.1 Userid/Password

* Authorised users are allocated a username and password, and must ensure that nobody else uses it. The user is responsible for the confidentiality of the username and password.
* Users must not use anyone else’s username/password.
* Users must not obtain or try to obtain anyone else’s password.
* Users must inform ITS (or their School/Dept systems support staff) immediately if they suspect someone else of using their userid/password.
* Office computers must not be left unattended when logged in unless a password protected screen-saver is used.
* Shared computers must not be left unattended when logged in.

5.2 Filestore

* Users must not gain access or attempt to gain access to any files owned by someone else unless the owner (or School/Dept system support staff) has specifically granted access.
* Users must not use equipment in contravention of the law.
* Users must use anti-virus products and must not introduce malicious code including viruses, network worms, Trojan horse, logic bombs etc
* User must not download or install software/hardware which could be used to scan, attack or compromise security or service.
* Users must not install software on shared equipment which may interfere with the normal operation of that equipment.

5.3 Email

* Email should be treated in the same way as ordinary mail and the same standards of behaviour apply.
* Email which is confidential or of a sensitive nature should not be sent unless appropriate precautions are taken.
* Users must not transmit email that causes “annoyance, inconvenience, or needless anxiety to other people”.
* Users must not send or attempt to send forged electronic mail.
* Users should contact ITS if they receive mail which they find offensive. The original message should not be deleted.

5.4 Network

* Users must not deliberately interfere or attempt to interfere with the operation of the network or computer systems.
* Users must not connect equipment to the College wired data network without first receiving the authority from School Systems Support staff or Computer Representatives.
* Users must not operate any equipment or software designed to eavesdrop on wired or wireless network communications.

1. **Other policies**

The following College Policies, or national guidelines are also relevant to this policy, and all users are required to be familiar with them:

* Birkbeck College Computing Regulations
* Data Protection Policy
* JANET Acceptable Use Policy
* Code of Conduct on the Use of Software and Datasets, issued by the Joint Information Systems Committee (JISC)
* Birkbeck Wireless Network Policy
* Mobile and Remote Device Security Policy

1. **Implementation of the policy and sanctions**

The responsibility for implementing this policy rests with Deans of Schools and Professional Services. Any breach of network security should be reported to the relevant systems administrator who will ensure that appropriate action is taken. In the event of a suspected or actual breach of security, the systems administrator may remove the affected system from the network.

Failure of an individual student or member of staff to comply with this policy may lead to the instigation of the relevant disciplinary procedures for students and staff. This could result in suspension of students or dismissal of staff. In the event of a serious infringement the College may also decide to institute legal proceedings under civil or criminal law relating to computer misuse.

*Last review: December 2016*