Computer Use Policy

Controlled Document – refer to Intranet for latest version

Category: Information and Technology	Date Created: September 2007
Responsibility: Director of Information Systems & Technology	Date Last Reviewed: March 2020
Approval: Chief Financial Officer	Version: 20.1

Purpose

UCOL provides computing facilities to support its educational mission. It is in the best interests of all users that the operation of these facilities is in accordance with practices which ensure that the rights of all users are protected and the goals of UCOL are achieved.

This policy establishes guidelines for employees, students and contractors who may be given access to UCOL's computing facilities. This policy promotes the responsible and ethical use of the computing facilities provided by UCOL.

Scope

This policy applies to **all** "Authorised Users" of computer and computer communication facilities owned, leased, operated or contracted by UCOL. The computing facilities are provided for work and study related purposes, although occasional use for personal reasons will be permitted provided that such use does not impact on the employee's role and efficiency or interfere with the learning of others. UCOL's computing facilities are not to be used for commercial purposes without the prior written permission of the Chief Executive or his authorised delegate. Only Authorised Users are permitted to use UCOL's computing facilities.

'Authorised Users' hereafter referred to as "Users' are those Staff, Students or Contractors who have been assigned a log-in ID and password. Authorisation to use UCOL's computing facilities ceases when the relationship with UCOL ceases, i.e. when the employment terminates, the enrolment expires or the contract terminates.

Responsibility

All Users of UCOL's computing facilities are required to be aware of, and adhere fully to this policy.

Policy Statements

1. All users of computing facilities should act responsibly and in a manner consistent with normal ethical obligations.

2. Users must not attempt to interfere with the normal operation of computing facilities. Specifically Users are not permitted to:-

    - use computing facilities in a way that violates any applicable laws, contractual agreements, or licenses, including, but not limited to the Films, Video and Publications Classification Act 1993 and the Copyright Act 1994;

- use computing facilities and resources in a way that may misrepresent UCOL, or violate any other UCOL policy;
- use computing facilities and resources in a manner considered harmful or harassing to another person.
- Access, copy or store inappropriate or objectionable material using UCOL computing facilities.

3. Users must respect the rights of other users to security of files, confidentiality of data and the ownership of their own work. Users are not permitted to:

   - use the computer access privileges of others; and/or
   - access, copy, or modify the files of others without their explicit permission; and/or
   - copy of software or data illegally; and/or
   - harass others in any way or interfere with their legitimate use of computing facilities.

4. Users must not use computers in an unacceptable way. The following are examples of unacceptable use which have been provided as a guide to interpreting this section and the principles above:

   - copying of licensed or Copyrighted software not permitted by law or by contract;
   - purposefully accessing and/or transferring Inappropriate, offensive or Objectionable material from the Internet; for example, racist or sexually explicit content;
   - sending harassing or libellous electronic mail;
   - sending electronic mail fraudulently, for example, by misrepresenting the identity of the sender;
   - utilising a loophole in a computer's operating system or knowledge of a privileged password to damage a computer system or to gain access to a system or resource which they are not authorised to use;
   - using UCOL computing facilities for commercial purposes without prior arrangement;
   - knowingly allowing another person to use your log-in ID and the password to your computer or account;
   - reading someone else's electronic mail without their permission;
   - using UCOL facilities to gain unauthorised access to computer facilities off-campus; and
   - Intentionally using an abnormally large amount of resources, such as processing time, disk space or bandwidth without prior permission.

Interim Policy Statement – Use of Personal IT Equipment for UCOL Business

UCOL's current policy is that privately owned IT equipment (e.g. computers, phones, etc) should not be used to conduct UCOL business. This is because the storage of UCOL information and intellectual property on private equipment constitutes a security and privacy risk. UCOL is unable to determine or manage the state of virus protection and other security measures on privately owned equipment. Where it is necessary for employees to carry out UCOL business at home or away from a UCOL campus, they will be provided with UCOL-owned and managed equipment for this purpose. However, under **exceptional circumstances** (as described below) it **may** be necessary for privately owned IT equipment to be used.

1. Wherever possible, UCOL equipment must be used to carry out UCOL business.

2. Privately owned equipment is only to be used in exceptional circumstances such as the activation of the Emergency Management Plan, and for a limited period of time.

3. Privately owned equipment is not to be used unless specifically directed or approved by the UCOL Incident Management Team, or another authorising body.

4. UCOL staff must take all reasonable precautions to ensure that UCOL data stored on private equipment is protected, safe and confidential.

5. The minimum amount of UCOL data required to carry out essential work should only be stored on privately owned equipment.

6. UCOL data must only reside on the privately owned equipment for the duration of the exceptional circumstances, as defined by the UCOL Incident Management Team.

7. Staff must remove all UCOL data from privately owned equipment as soon as UCOL equipment becomes available, or as directed by the UCOL Incident Management Team.

8. UCOL will support privately owned equipment on a best-efforts basis for the duration of the exceptional circumstance only. UCOL will not subsidise the use of private equipment, or cover the cost of internet connections and other consumables unless previously approved.

Software

Only software authorised by the Information Technology Department may be run on UCOL equipment. This authorisation will only be given to properly licensed software that is to be used in support of UCOL's Mission and Charter. **All** Users are expected to abide fully by the conditions specified in the license.

Hardware

The unauthorised installation, removal or modification of computer equipment is strictly prohibited.

Disk Space

Authorised users are allocated disk space on the network servers for their own use (H Drive). This drive is to be used for storing work or study related material only. Personal material such as music, photographs or video clips should be stored either on a memory stick or, in the case of staff, it may be temporarily stored on the C drive. Users are expected to minimise unnecessary storage and erase material no longer required or known to be stored as an original version elsewhere.

In addition, faculties will be provided with a lecturer resource area (I Drive) and a student resource area (G drive).

All users will also be given a mail account together with disk space on the mail server. This space will be limited to 30 Mbytes and is not expandable. Users wishing to store mail permanently should use their home directory (H drive) for this purpose.

The data on the H, I & G drives will be backed up to tape on a daily basis with files being available for restore up to 10 working days after deletion from the server. All staff mail is archived and can be recovered upon request. Student Mail is only backed up for disaster recovery purposes and no individual file restore service is available.

Termination of account

Log-on access, together with file space and e-mail allocations, will be removed from the fileservers ninety days after a staff member ceases to be employed by UCOL or fourteen days following the completion of a programme. Managers, Deans and Heads of School may request access to an account, or the redirection of incoming e-mails, during the grace period prior to removal of the account. All files contained in the users home directory will be erased and incoming e-mails returned to sender when the account is terminated.

Monitoring

Staff, Student and Contractor use of computers will be monitored and breaches of this policy may result in formal disciplinary action being taken.

Disciplinary Actions

Violation of the principles described in this policy may result in disciplinary action. Such action will be taken as outlined in the Student Discipline Statute or the Staff Disciplinary Procedure. Notwithstanding the above, where such a violation is believed to have contravened the Crimes Act or the Films, Videos or Publications Act or the Harmful Digital Communications Act, the matter will be referred to the Police.

This Computer Use policy does not diminish the authority and responsibility of the IT Department to take immediate and appropriate action in the case of possible abuse of computing facilities. Where IT takes such action they will do so with due regard for:

- the protection of UCOL's computing infrastructure and data systems
- UCOL's obligations under law as a public institution
- the risk to UCOL's reputation
- the protection of users' work
- the Student Discipline Statute
- the Staff Disciplinary Procedure

All usage records will be made available during investigation of criminal computer use.

Relevant Legislation

- Human Rights Act 1993
- Harmful Digital Communications Act 2015
- Privacy Act 1993
- Employment Relations Act 2000
- Films, Videos and Publications Classification Act 1993
- Copyright Act 1994
- Crimes Act 1961
- Public Records Act 2005

Related Documentation

- Harassment Prevention Policy for Employees
- Disciplinary Procedure
- Information Systems Security Policy
- Student Harassment/Bullying Prevention Policy