



# **INFORMATION COMMUNICATION & LEARNING TECHNOLOGIES**

## **ACCEPTABLE USE & SECURITY POLICY FOR COLLEGE STAFF**



*Learn for Life*

# Langside College

*'Learn for Life'*

## INFORMATION COMMUNICATION & LEARNING TECHNOLOGIES - ACCEPTABLE USE & SECURITY POLICY FOR COLLEGE STAFF

### Functional Responsibility

Assistant Principal (Information Services  
& Systems)

### Approval Authority

Development Committee

### Status of this Document:

Live

### Next Review:

Sept. 2005

This Policy sets out the boundaries of acceptable use of ICLT facilities by the College's staff, along with arrangements for policy implementation and review, and operational guidance.

## 1 POLICY STATEMENT

- 1.1.1 This policy concerns the acceptable use of Information , Communications and Learning Technology (ICLT). For the purposes of this policy, ICLT includes any technology for storing and manipulating data, such as computers, networks, software, and electronic learning technologies; owned or operated by the College.
- 1.1.2 Use of ICLT in support of teaching, learning, communications, management and administration is already extensive and will grow in importance in the future.
- 1.1.3 The College encourages all staff to access ICLT resources, including the Intranet and externally to the Internet/World-wide Web, for the purposes of pursuing the College's business, and for the personal development of the individual employee (see Personal Development and Career Review Policy).
- 1.1.4 In general terms, acceptable use of ICLT in the College is bounded by the College's requirements for ethical standards, decency, security, cost effective use of resources, and, in particular, by the requirements of the law. Specifically, through this policy, the College seeks to:
- protect the **confidentiality** of data and **privacy** of its users;
  - safeguard the **integrity** of the College's ICLT data and resources;
  - maintain **availability** of the College's ICLT resources with a reasonable response time;

- achieve user compliance with the College's policies regarding harassment and the safety of individuals;
- protect the College against legal or damaging consequences;
- appropriately respond to claims of infringement of electronically posted copies of copyrighted materials.

1.1.5 The College also permits staff to make reasonable personal use of the ICLT facilities *in their own time*, subject to all the conditions explicit in this Acceptable Use & Security Policy. However, *College ICLT facilities, including, those of Clydenet and UKERNA, may not be used, under any circumstances, by any staff member, for their own personal commercial or monetary gain or benefit.*

1.1.6 The College takes seriously its responsibilities for the Acceptable Use of its ICLT resources. Consequently, the Assistant Principal (Information Services and Systems) or duly authorised staff may examine the ICLT equipment, files, applications and e-mail of any employee at any time to investigate a suspected breach of this Policy.

## 2 CONTEXT

- The Joint Information Services Committee (JISC) has produced a template on acceptable use of ICLT for the HE and FE sectors, which overtakes a previous versions which was the basis of the College's original ICLT Acceptable Use Policy.
- This policy relates to the College's Strategic Vision, Mission, Aims and Objectives in so far as ICLT is an important tool for both management of the College and delivery of the curriculum. However, its misuse may prevent the cost-effective achievement of both the strategic aims and operational plans, and, indeed, damage the reputation of the College.
- This policy supports other College policies relating to Data Protection , Freedom of Information and Copyright, and is subject to the conditions extant in the College's HR policies.
- Use of ICLT resources is subject to Scots, UK and International Law. Consequently, this policy is informed by the relevant legislation, e.g. the Misuse of Computers Act 1990; the Data Protection Act 1998.

2.1.1 The College's investment in both the infrastructure and technical staff to operate and maintain ICLT resources is large and will continue, not least to replace existing equipment and software as it depreciates or becomes obsolete. Consequently, the College has a critical interest in the proper, safe, efficient and effective use of these resources.

2.1.2 Reference should also be made to the following documents:

- Employee Disciplinary Policy & Procedures
- Copyright Policy
- Data Protection Policy
- Harassment Policy
- Personal Development & Career Review Policy
- Access to Library Materials Policy.

### 3 REGULATIONS

#### 3.1 General

3.1.1 By using the ICLT equipment (hardware), software and network services, staff acknowledge, agree to, and are bound by this Policy.

3.1.2 No attempt should be made to load unauthorised software programmes including server software, applications and games onto College computers or systems. No software other than that approved and sanctioned by the ICLT/Technical Services Manager may be installed on any College computer or system.

ICLT Technicians finding illegal or non-approved software on computers, including servers, will remove the programme(s), and report immediately to the ICLT/Technical Services Manager. N.B. The College has installed and uses remotely software to identify all software programmes installed on its networked PCs.

3.1.3 Information held on College computers, including servers, is not guaranteed to be private. Where material or activities are, *with good cause*, suspected to breach this policy, contain illegal material, or be in support of an illegal act, the College will take action under the provisions and conditions extant in this Policy.

3.1.4 To protect authorised users from the effects of abuse or negligence, the College reserves the rights to limit, restrict, or terminate any account or use of the College's computer resources, and to inspect, copy, remove, or otherwise alter any data, file, or system resources which undermine authorised use. The College will not be liable for inadvertent loss of data or interference with files resulting from this action.

3.1.5 No one shall place confidential information in computers without appropriately protecting it. The College does not guarantee the privacy of files, electronic mail, or other information stored or transmitted on its ICLT resources (see Information Security Policy).

3.1.6 No one shall compromise the privacy of others or the confidentiality of the information contained on the College's ICLT/ILT resources. The provisions,

responsibilities, requirements and obligations of the Data Protection Act 1998 are to be complied with at all times (refer to Data Protection Policy).

3.1.7 Breaches of the acceptable use of equipment and software must be reported to the ICLT/Technical Services Manager, in the first instance.

3.1.8 All equipment and software supplied to for use by staff and students remains the property of Langside College.

### **3.2 Equipment - Personal Computers (PCs/Desktops/Portables), Printers and other Peripherals**

3.2.1 College computers, software and network services and systems *must not* be used for:

- The creation or transmission (other than for properly supervised and lawful research purposes) of any offensive, obscene or indecent images, data or material, or any data capable of being resolved into obscene or indecent images or material.
- The creation or transmission of material designed or likely to cause annoyance, inconvenience or needless anxiety.
- The creation or transmission of defamatory material.
- The downloading, copying or transmission of material such that this infringes the copyright of another person or organisation. N.B. The copyright laws apply not only to documents but also to software.
- The transmission of unsolicited commercial or advertising material either to other user organisations, or to organisations connected to other networks
- Unauthorised access to College services/resources or to other facilities or services via the College , or Clydenet or JANET/SUPERJANET networks.

3.2.2 No one shall connect any computer or network system to any of the College's networks (e.g., direct connection, direct dial-in access) unless it meets the technical and security standards set and approved by the College, and such installation is approved in writing by the ICLT/Technical Services Manager.

3.2.3 No one shall use the College's ICLT resources to transmit chain letters or mass mailings (e.g., "spamming"), or other communications prohibited by law; nor launch denial of service attacks against other users, systems, or networks. Users shall take full responsibility for any electronic messages that are transmitted from their accounts through the College's telecommunications networks and facilities.

- 3.2.4 No one shall install or use network "sniffers" or otherwise inappropriately intercept or monitor a user's network traffic or data communications without prior approval from the ICLT/Technical Services Manager.
- 3.2.5 The reduction of the efficiency of the network services and PCs must be avoided, such as through overly time-consuming or un-focused browsing of the Internet and the downloading of large files such that they needlessly take up storage space on College servers or desktop computers (see also section on E-mail).
- 3.2.6 Staff must ensure that they do not:-
- Corrupt or destroy other users' data;
  - Violate the privacy of others;
  - Disrupt the work of other users;
  - Use the College's, or the Clydenet or JANET/SUPERJANET, networks in a way that denies service to other users (for example, deliberate, reckless or negligent overloading of access links or of switching equipment);
  - Continue to use an item of networking software or hardware after the College or UKERNA has instructed that use cease because of disruption to the correct functioning of networks;
  - No one shall knowingly or negligently create, install, execute, or distribute any malicious code (e.g., virus, Trojan Horse, worm, etc) or another surreptitiously destructive program on any College ICLT resource, regardless of the result.

N.B. Deliberate spreading of viruses is subject to prosecution under the Computer Misuse Act 1990

Where College ICLT systems are being used to access another network, any breach of or abuse under this Acceptable Use policy of that network will be regarded as unacceptable use of the College network system and services

### **3.3 E-mail**

- 3.3.1 E-mail communications should meet the same standards as other written communication and published documents, and staff should avoid making any inaccurate or defamatory statements.
- 3.3.2 All members of staff are assigned an e-mail address published both on the Intranet and in a printed list for the use of other staff. As appropriate staff e-mail addresses are released to College partners and business associates to facilitate communication.

- 3.3.3 Staff should use professional discretion in deciding to whom they release their College e-mail address and the names and e-mail addresses of colleagues. Under no circumstances should they divulge the names or addresses of students unless in compliance with the specific circumstances indicated in the College's 'Data Protection Policy'.
- 3.3.4 The College respects the rights of staff to privacy; hence the *contents* of e-mail messages are not subject to examination, *except* where a breach of the Acceptable Use Policy or the law is suspected with good cause, reported or otherwise made known. However, regular checks are made on the timing, volume, frequency, source and destination of e-mail messages.
- 3.3.5 Staff should manage their e-mail correspondence properly. As with voice-mail, e-mailboxes should be checked regularly. The storage of e-mails takes up space on College servers. Accordingly, each member of staff is limited to a maximum total storage of 5Mb. It is in staff interests to delete old, irrelevant, or redundant e-mails from mailboxes. If a mailbox is at capacity you will not be able to receive new messages until space has been created.
- 3.3.6 Wrongly delivered messages should be re-directed to the correct person. If the e-mail contains confidential information, use may not be made of that information, nor must it be disclosed under penalty of the Data Protection act 1998
- 3.3.7 Staff should remember that e-mail messages are not secure unless they are encrypted. Disclosure of certain confidential information may prejudice the College, or may be in breach of the College's obligations to third parties, or may invalidate the College's intellectual property rights in that information.
- 3.3.8 Staff shall not e-mail College confidential information and trade secrets and material that is otherwise confidential to the College unless encrypted and shall only send such information to other College staff or parties who have entered into binding confidentiality agreements with the College.
- 3.3.9 Care should be taken when e-mailing third party material, as use of such material may infringe the intellectual property rights of a third party. Staff should ensure that they have authority to disclose any such material, for example by licence. If in doubt, staff should check with the Assistant Principal (Information Services & Systems).
- 3.3.10 Information held by the College about identifiable individuals (the "personal data" of "data subjects") is protected under the Data Protection Act 1998. Any use or transfer of such data, particularly overseas, must be in accordance with certain legal restrictions (see 'Data Protection Policy'). Any employee proposing to include personal data in e-mail should obtain prior clearance from the Assistant Principal (Information Services & Systems).

### 3.4 Conduct with Regard to Other Persons

#### 3.4.1 Harassment

Staff must not use ICLT resources of any kind in a manner that may harass, intimidate or cause deliberate offence to another person or group of people. This includes harassment of a political, racial, religious or sexual nature, or use of abusive language or image. This includes attempting to access, store, or distribute, electronically or otherwise, documents, images, audio files, mail messages or files of any other type which would enable harassment.

#### 3.4.2 Other Users' Passwords

Staff must not attempt to log into any computer system using the user account of another person.

#### 3.4.3 Other Users' Data

Staff must not attempt to copy, alter or destroy data belonging to another person, group of people or organisation

### 3.5 Security - Staff should refer to the Information Security Policy and the Data Protection Policy, but in essence:

#### 3.5.1 Staff must not:

- Attempt to ascertain or ascertain and /or use the user name, password or personal details of any other user, except where by reason of their responsibilities - for example ICLT Network Administrators and Technicians, and Lecturers in some curricular areas - they have to create or provide user-names and passwords for other staff or users, such as students and/or intervene for the purpose of equipment maintenance
- Deliberately or negligently (this includes having details on a 'post-it' stuck on a PC or on the office wall or desktop) divulge their user name and/or password to any other person.
- Attempt to gain access to any College ICLT resource or area or computer or network system which they are not authorised to enter or use

3.5.2 No one shall give any account authentication (e.g. logon and/or password) to an unauthorised person, nor obtain another user's authentication by any means. Since passwords are the first line of defence to the College's ICLT/ILT resources, users must choose passwords carefully and comply with password guidelines for effective password protection.

3.5.3 Attempt to circumvent or otherwise bypass system security on any computer system or network whether owned by the College, or others connected to the

network, including Clydenet, JANET/SUPERJANET and other Internet connections.

3.5.4 The College reserves the right to immediately disconnect any and all system(s) from the network while assessing and/or repairing any discovered or reported security incident in order to minimize risk to the rest of the College network.

3.5.5 Reporting Security Incidents / Infractions

Users are expected to report any information concerning instances in which they suspect or have evidence that the above Standards have been or are being violated.

3.5.6 No one shall misrepresent his or her identity or relationship to the College for the purpose of accessing or attempting unauthorised access to College ICLT resources nor misrepresent his or her identity to other networks (e.g., IP address "spoofing") from the College's ICLT resources.

3.5.7 Any breach of security must be reported immediately to the ICLT/Technical Services Manager in the first instance.

**3.6 Copyright and Intellectual Property (see also Copyright Policy and Annex 1 of this document)**

3.6.1 Users must not:

- Use College ICLT resources in any manner which may result in a breach of the Copyright, Design and Patents Act 1988, the Data Protection Act 1998, Computer Misuse Act 1990 or any other laws pertaining to the uses/misuses of information, including images.
- Distribute electronically, or by any other means, and/or publish any material created by another person or organisation without the express written permission of that person or organisation.
- Copy or remove software from computer systems or networks owned by the College or accessed via College ICLT resources.

3.6.2 Principles

- Langside College respects the rights of copyright holders and will respond promptly to valid complaints.
- The College supports the fair use rights of its students, faculty, and staff.

3.6.3 Compliance with Copyright Law(s)

- Langside College will accommodate and not interfere with standard technical measures that identify and protect rights of copyright owners.
- The College is committed to informing members of the College community of their rights and responsibilities under Copyright Law(s).
- Account holders will be warned in advance that material may be taken down if an infringement complaint is received and that disciplinary action may be taken if they infringe copyrights. Copyright Law compliance information will appear in the Staff and Student Intranets, staff handbooks, student handbooks.
- A decision not to disable access to materials will be made if the College's reasonable belief that the complaint is substantially incomplete, without sufficient foundation, or that a legal defense may apply.

### **3.7 Theft and Damage**

#### **3.7.1 Staff must not**

- Attempt to remove any ICLT equipment or any other ICLT resources which are the property of the College. Under certain circumstances approval may be given to staff to remove College-owned equipment and/or software to a non-College location. For the avoidance of doubt, this may be carried out only with the written approval of the ICLT/Technical Services Manager
- Deliberately or negligently damage or degrade, either physically or electronically, College ICLT resources

### **3.8 Enforcement**

- 3.8.1 Breaches of this Policy will lead to penalties. These may include, among others and not limited to, suspension of accounts, the application of the College's Disciplinary Procedures, reporting to the Police, and subsequent legal action under Scots Criminal or Civil Law.
- 3.8.2 Deliberate or negligent misuse, maltreatment or damage to College equipment and/or software, including failure to comply with the requirements of the ICLT/Network Security Policy, will be subject to the College Disciplinary Procedures and/or Scots Law.

## **4 IMPLEMENTATION and REVIEW**

### **4.1 Promulgation of New/Revised Policy**

- 4.1.1 This Policy will be archived in the College's Document Management System (e-intranet) from where it will be published to the College intranet (Policy Section). Hard copy will be lodged in the LITEhouse (library) and at Reception on each of

the College's campuses.

N.B. Each member of staff will be required to sign off the Acknowledgement Form that they have read and agree to abide by the conditions and regulations set out in this Policy (see end page of this Policy document).

## **4.2 Training and Briefing of Staff**

4.2.1 The Learning Innovation Unit provides appropriate training programmes and courses to all staff in the use of computers and software applications to allow all users both to meet their obligations and responsibilities under the requirements, conditions and regulations set out in this Policy, and the effective and efficient discharge of their work tasks.

N.B. If your skill level is inappropriate, please ensure, through your Career Review and Personal Development entitlement that you undertake relevant training to allow you to make efficient use of the Intranet and Internet.

All members of staff should be able to log on to a computer, and access and use Software applications appropriate to their duties. As a rule all should be competent sending, opening, replying to, forwarding, deleting, and making attachments to, e-mail, including the orderly storage of e-mails in a structured folder system. For further information please contact the Learning Innovation Unit.

## **4.3 New In-post Staff**

New staff, either internal appointees to a new position, or from external locations, will receive induction, including training in basic ICLT applications where necessary, including the acceptable uses described and prescribed in this document. Where the job requires more advanced training that will be provided as appropriate.

## **4.4 Monitoring**

4.4.1 All staff have a duty of care and responsibility to monitor this Policy in action. More specifically, the ICLT/Technical Services Staff routinely, and frequently, monitor the policy in action as part of their everyday duties. Equipment and software has been installed to monitor installed software and web traffic, including e-mails (destination and frequency only). Low order non-compliance will be reported to the ICLT/Technical Services Manager. More serious non-compliance will be reported to the Assistant Principal (Information Services & Systems).

The Policy as a whole will be monitored on a quarterly basis by the Assistant Principal (Information Services & systems) and the ICLT/Technical Services Manager. The former will report annually to the Strategic Management Team and Board of Management Development Committee on policy compliance, effectiveness and any unanticipated costs associated with the implementation of this Policy.

#### **4.5 Review**

4.5.1 This policy will be subject normally to annual review by the ICLT User Group. In the event of unanticipated changes in legislation and/or exceptional College circumstances relating either to the policy itself or its effective implementation, a review may be instigated by the SMT. Members of staff are encouraged to contribute ideas, observations and critiques of the policy at any time.

### **5 OPERATIONAL GUIDANCE**

#### **5.1 E-mail**

Increasingly internal communication will be by e-mail. Consequently, you should evaluate your competence in its use. This includes the sending only of relevant e-mail messages and avoiding the automatic forwarding of all messages to long circulation lists - increases traffic unnecessarily as well as time spent dealing with irrelevant correspondence. If in doubt, consult the E-mail checklist on the Intranet.

Training in the use of e-mail will be provided. Please contact the Learning Innovation Unit.

There is no way to prevent the redistribution of E-mail messages. Never assume that any message is a one-time, one-to-one communication.

#### **5.2 Discovery of Viruses**

Any computer virus infection should be notified to the ICLT Help Desk, where expert assistance can be provided. Staff must NOT try to conceal the existence of a virus, or deal with it themselves. This may put other users at risk.

Isolate the PC(s) involved and any floppy disk or CDs (software/data/backups). The ICLT Section will advise other users who may be at risk. Any infected disks will be dealt with and returned to staff. It may be necessary to inform the originator of the disk about the virus.

#### **5.3 Internet Access and Use**

Staff are expected to exercise good judgement and act in a professional manner whenever accessing the Internet.

The term 'Internet' is used to describe all services that exist on the Internet such as the World Wide Web (WWW), FTP, Gopher, etc.

#### **5.4 Downloading Software**

Downloading software from the Internet is prohibited without first gaining permission from the ICLT/Technical Services Manager. Additionally, staff should note that although material may be available for "free" on the Internet, this does not necessarily mean the employee has the legal right to copy it. If a College employee does receive permission to download software, they should exercise caution when downloading large files (i.e. over 1Mb, including text and multimedia files). Downloading large files can take a long time and therefore degrade network performance for everyone on the network. The best time to download such files is during out of office hours when there is the least number of users on the network.

#### **5.5 Security**

The Internet is not a secure environment - staff should not assume any activities are private. Staff must not leave their computer unattended while connected to the Internet and should always terminate their connection to the Internet as soon as possible after they have completed any task.

Staff must not transmit Ids, usernames, passwords, internal network configurations or addresses, or system names over the Internet.

Staff must not attach a modem to their PC to gain access to the Internet (or any other electronic based resource).

#### **5.6 Home PCs**

If an employee has permission from his/her departmental manager to transfer files from a College computer, via floppy disk or CD, to their home PC, then floppy disks or CDs that are taken out of the College must be virus checked on return, on each and every occasion. If required, the ICLT Section can supply a disk that can perform a regular virus-check on an employee-owned PC.

#### **5.7 New Software**

The ICLT/Technical Services Manager is responsible for the purchase, distribution, installation and secure holding of all software masters and software licences.

#### **5.8 User Responsibilities**

There is an expectation of confidentiality/privacy on College resources inherently granted to users. Although the College cannot guarantee that privacy, it strives to

protect it. Users are expected to act in a responsible, ethical, and legal manner with the understanding that the College's ICLT resources are conducted in a public forum - electronic communications, such as electronic mail, are public records that can be used as evidence in a court of law.

Users should respect the rights of others (especially rights of privacy and confidentiality), freedom of expression, intellectual property rights, law, and due process.

Although system administrators or other designated Security Officers strive to provide and preserve the security and integrity of files, account numbers, authorisation codes, and passwords, security can be breached through actions or causes beyond their reasonable control. Therefore, users are urged to safeguard their data, personal information, passwords, and authorisation codes by taking full advantage of file security mechanisms built into their computer's operating system.

### **5.9 Good Practice Guide**

This section is intended to explain the College's policies and procedures with regard to PCs and their usage. It covers the mandatory procedures staff are required to undertake as PC users within the College.

### **5.10 Online Help**

The ICLT Section can provide first line support to all staff concerning any aspect of their PC. However, staff are also encouraged to use the online help that is supplied with software packages. Many packages allow the user to key in questions using 'natural language'. By doing so, staff can reduce the time taken to resolve queries and also learn more about the software package in question.

### **5.11 E-mail Read and Delivery Receipts**

If staff are sending an important E-mail or have reason to believe that the intended recipient's E-mail system is faulty, they should attach a delivery receipt and/or read receipt to the E-mail in question. That way, staff will have definite confirmation of whether the recipient has received the E-mail. Please bear in mind that although a read receipt confirms that the intended recipient has read the E-mail, it does not indicate that they have read and understood the contents. Full instructions are included within Outlook 2000 online help.

### **5.12 Good sender habits:**

- Use distribution lists with caution.
- Be succinct and to the point in e-mail communications.
- Keep focused on the topic.

- Use a descriptive SUBJECT line to help recipients prioritise, file, and search.
- Use message tags and flags appropriately.
- Do not 'REPLY TO ALL' unless necessary.
- Use URL (<http://server/file.doc>) or UNC links (<\\servershare>) instead of sending large and numerous attachments.
- Avoid long dialogues and discussion threads via e-mail.
- Avoid complex or large graphical signatures in messages.

### **5.13 Good receiver habits:**

- Establish regular intervals or time blocks for e-mail.
- Delete messages when no longer needed.
- Organize messages into folders outside of your inbox.
- Browse messages by subject line to prioritise.
- Eliminate unnecessary replies or acknowledgements.
- Delegate mailbox access when unable to retrieve messages.
- Use inbox rules sparingly and keep them simple.
- Avoid membership in unnecessary distribution lists or subscriptions, and review such membership to evaluate its usefulness

### **5.14 Out of Office Tool**

Staff should use the Out of Office tool to let other E-mail users know they are on annual leave, business trips, or any planned event that causes the employee to be away from the office. This is supplied as standard with Outlook 2000 and full instructions are included within online help.

### **5.15 Maintaining your Mailbox**

Employee Inbox, Sent Items and Deleted Items folders can quickly grow in size and the College has placed a limit on the amount of E-mail that can be stored in employee mailboxes. Therefore, staff should periodically clean up their

mailboxes by archiving old items and emptying deleted items folders. Full instructions are included within Outlook 2000 online help.

### 5.16 PC Security

Staff should immediately inform the ICLT/Technical Services Manager of any communications or system problem or other circumstance that they think may indicate a breach of security or other risk to the integrity of the College's system.

Unless written permission has been granted from the ICLT Manager, contractors and temporary/specific purpose contract staff are not permitted to use college PCs or college IT resources. All other third parties are not to be permitted access to PCs, except for approved field engineers.

Computer programs, files, printouts, disks or any other item capable of recording and storing information for use with PCs, remain the property of the College at all times. Anyone who needs to remove systems/data must ensure that its removal is authorised and the information is safeguarded at all times.

All sensitive data, whether paper, magnetic backup disks or optical disks must be securely and safely filed when not in use, preferably in locked, fireproof cabinets.

### 5.17 Passwords

Passwords should be changed regularly in order to maintain their effectiveness. As a guide this should be done at least once every six months. Staff should never use another user's password, nor permit any other person to use their password. **If someone knows your password they can read your E-mail from any web browser.**

The security of confidential word processing documents, spreadsheets, etc. may be enhanced with the use of passwords wherever a user deems necessary. Refer to the online help that is supplied with the applications software for details on how to do this.

### 5.18 System Performance

Staff should not tamper with or carry out any act that may in any way affect the output or performance of the College's computer equipment and systems. This includes installing any type of software or hardware/peripheral.

Staff must not attempt to access parts of the computer system to which they have not been granted access permission.

## **5.19 Leaving Applications Open/Switching Off Your PC**

Staff should close all applications whenever they are going to be away from the PC for any length of time. Staff should also make sure that their PC is switched off when they leave the office to go home.

Before switching off their PC, staff should make sure that all applications have been closed as this minimises the risk of data loss.

## **5.20 Games**

The downloading, uploading and/or use of computer games is strictly forbidden, including Internet based games.

## **5.20 When an Employee Leaves**

Managers responsible for staff who utilise PCs must ensure that all access to computer facilities and their associated data is removed immediately from personnel who leave the College. Managers should note that in certain circumstances where members of staff are serving notice, it might be necessary to carry out this action before the member of staff actually leaves.

The ICLT Section is responsible for assisting management in enforcing these security policies, and to give advice on any aspect of computer security.

## **5.21 Data Backup**

The most important and valuable component of any computer system is the information, or DATA, it contains; as application software is easily replaced. Staff must therefore ensure that it is securely controlled at all times. Staff should never take the risk of not backing up their information as it can take hours of wasted time and effort to restore all the data that has been lost. The 'My Documents' folder is stored on the main fileserver and is backed up routinely every evening. However, if staff store data locally on their C:\ drive, then they are responsible for ensuring that this data is backed up safely. Staff should take all reasonable care of their data, remembering that it is their responsibility to look after it.

The ICLT Section will assist with the setting up of backup procedures on PCs.

## **5.22 PC Faults**

In the event of a PC fault staff should notify the ICLT Section (via the On-line Help section of the Intranet or by telephone) who will decide which company is to be used for the repair, if it cannot be repaired in-house. If a service engineer is

unable to rectify a fault on site only the ICLT Section can authorise the removal of any computer hardware or media from the premises.

## 5.22 Software Copyright

It is not permitted to use unlicensed copies of any software program on any computer.

It is possible that use of unlicensed or pirated software may introduce a computer virus. This is a hidden program that is designed to copy itself from disk to disk without the knowledge of the user.

Normally, on purchasing a software package, the buyer receives a licence to use the product that does not convey the right of ownership for the contents of the disks. The licence normally allows for the computer program to be used in a single computer unless otherwise stated by the manufacturer.

Initial enquiries regarding the purchase of software packages should be made to the ICLT Manager who will provide any assistance in selecting the correct software to fulfil a particular requirement.

Once the correct software has been selected an order should be raised and presented to the appropriate manager for approval and upon purchase should be registered with the ICLT Section.

Most software packages permit the buyer to take a single copy of the software to use either as a working copy on a hard disk or as a backup in case of problems. If the buyer no longer uses a package and wishes to permanently transfer the software licence from one PC to another then this is normally permissible provided all copies on the original PC are destroyed.

Any software packages that are no longer required must be returned to the ICLT Section.

The software copyright laws are designed to prevent staff from making multiple copies of a product without paying for each copy. The pirating of software is theft, and staff will be held personally responsible if they break the terms of the software licence. As a guideline staff should have one copy of the program (either a backup on floppy disk or CDs or a working copy on a hard disk) and a complete set of documentation for each software package on their PC1. The ICLT Section will hold original disks centrally.

Staff are not expected to have in their possession copies of Microsoft Office, Windows or any other standard company software, as licenses for these are held centrally by the ICLT Section.

Many software packages are supplied with a registration document that must be completed and returned to the supplier. In these circumstances such documents

must be completed in the name of the College and not in the name of the individual user/employee. This safeguards against any problems arising through changes in the responsibilities of a registered individual.

### **5.23 Software Piracy**

The unauthorised copying or use of copied software has serious implications for individual staff, for the College, and for its Board of Management. "Copying" ranges from the making of single copies for backup purposes to deliberate and wholesale duplication for commercial gain. In all cases, copying must be specifically authorised beforehand by the software owner (whether by licence or user agreement, or under conditions of sale or an express assignment of ownership).

The potential risks of unlicensed copying include:

- a) Substantial criminal penalties (such as unlimited fines and/or imprisonment) and civil liability (e.g. injunctions and/or damages) for breach of copyright, attaching as appropriate to the College and to its directors, officers and individual staff personally.
- b) Possible search of premises and seizure of offending software, without warning.
- c) Jeopardy of the right to make legitimate copies and/or to use programs, and loss of access to technical support, instruction and updates.
- d) Adverse publicity and threat to the reputation of the College.
- e) Increased exposure to viruses compared with the use of original proprietary software.
- f) Disruption and loss of management time and expense.

Proceedings for infringement of copyright might be commenced by an individual software owner or (more commonly) by organisations representing the interests of software houses such as the Federation against Software Theft (FAST). Successful actions have recently been pursued, for example, against Marconi Instruments and Mirror Group Newspapers resulting in prosecutions or the making of 'contributions' (in some cases amounting to £250,000) in return for the threat of prosecution being dropped.

### **5.24 As a matter of course, the ICLT Section will:**

- a) Monitor the acquisition and location of all PCs and software, and monitor the permitted copying of software.

- b) Maintain a file containing details of all software purchases and all licence and user agreements.
- c) Arrange regular and unannounced software audits, using professional policing software where necessary, carrying out physical inventories of software and ensuring the destruction of any unauthorised software that is discovered.
- d) Ensure that access to software is restricted to persons with a need for access in connection with their duties and that software is stored securely when not in use.

**All staff MUST read and understand these instructions, which detail the law and its penalties. Notwithstanding the foregoing, each employee must obtain the ICLT/Technical Services Manager's express consent before:**

- a) Installing any new software
- b) Removing any software or PC from any site.
- c) Disclosing any software to any third party.
- d) Copying any software.
- e) Using any software on a PC other than that for which authorisation has been given.

Note that the College will take disciplinary action against any employee found to be in breach of these instructions.

## **5.25 Use of Personal PCs and Software**

As a result of the widespread use and availability of PCs it has become far easier for individuals to copy and retain data and software from a variety of sources. This form of copying, which if unauthorised, amounts to theft, is not particularly easy to detect, but its implications are very serious and far-reaching.

PCs and software owned by staff must not be used to process or store data that is owned by the College. Employee-owned PCs shall not be brought onto premises nor should employee-licensed software be stored on College PCs without prior written authorisation from your manager.

Under no circumstances should disks be taken home for use on employee-owned PCs. Disks used on privately owned PCs should not be loaded onto college PCs. (Exceptions can only be made in conjunction with a work related requirement and management's approval).

## APPENDIX 1 COPYRIGHT ISSUES

### **Receiving a Complaint of Online Copyright Infringement**

Complaints of on-line Copyright Infringement will be handled by the Assistant Principal (Information Services & Systems) who will first determine the nature of the College's role.

### **Determining the Role of the College**

The College may take advantage of Internet Service Provider (ISP) limitations on liability only if the /College is acting as an ISP, and not as a content provider.

### **Take-Down**

If the College is eligible for the ISP liability limitation, and the complaint is complete, the Information Security Manager will immediately disable access to the work.

### **Consultation with Account Holders**

As soon as a complaint is received, the Information AP (ISS) shall notify the account holder of the allegation of infringement. A standard notification will include a copy of the complaint, information on counter-notification, put back, and basic copyright rights and responsibilities. This will allow the account holder to voluntarily remove the challenged material or formulate a counter notification of fair use. Under certain circumstances it may be appropriate for the College to participate in the determination of whether fair use or some other exemption may apply that would allow the work to continue to be used.

If the material is to remain down, it is important that the account holder understands why a complaint was made and agrees to refrain from further infringements.

### **Counter-Notification**

If the account holder files a counter-notification claiming that the work is misidentified, or the owner is mistaken and the use is lawful, the Assistant Principal (Information Services & Systems) will send the counter-notification to the complainer, explaining that the material will be put back in a reasonable time, and not more than 15 working days.

## **Put Back**

Access to the material will be re-established in not more than 15 working days unless the complainer sends notice that a court order is being sought or other legal action will be taken.

## **Other Responses to Infringement Allegations; Investigating Fair Use**

Allegations of infringement for which the College is the content provider and for which the College is not eligible for liability limitation as an ISP will be referred to both the account owner and the AP (ISS). The College shall respond to these allegations by conducting an investigation into whether the allegedly infringing materials are authorised by law or otherwise do not infringe on copyright protections.

# Learn for Life



50 Prospecthill Road  
Glasgow G42 9LB

Main Switchboard  
Tel: 0141 649 4991  
Fax: 0141 632 5252

Student Services  
Tel: 0141 272 3636  
Fax: 0141 632 5252  
[enquireuk@langside.ac.uk](mailto:enquireuk@langside.ac.uk)  
[www.langside.ac.uk](http://www.langside.ac.uk)



ECDL  
European Computer  
Driving Licence



Langside College is a registered Scottish charity.  
Scottish charity no. SC021202