

LONGLEY PARK SIXTH FORM COLLEGE

ICT SYSTEMS ACCEPTABLE USE POLICY

Originator:	Derek Taylor, Network Manager
Date of Last Approval:	14 December 2005
Approval/review by:	Resources Committee/Corporation February/March 2011
Review interval (years):	3
Date of next review/approval:	February 2014

LONGLEY PARK SIXTH FORM COLLEGE - ICT SYSTEMS ACCEPTABLE USE POLICY

1.	PRINCIPLE	3
2.	INTRODUCTION.....	3
3.	SCOPE.....	3
4.	GENERAL COMPUTER USE	3
5.	THE NETWORK.....	5
6.	EMAIL	5
	6.1. Provision of email.....	5
	6.2. Use of Email.....	6
7.	INTERNET	6
8.	LAPTOPS.....	7
	8.1. Software.....	7
	8.2. Virus Protection.....	8
9.	PRINTING & COPYING	8
10.	TELEPHONES (INCLUDING COLLEGE-OWNED MOBILE TELEPHONES).....	9

ICT SYSTEMS ACCEPTABLE USE POLICY

1. PRINCIPLE

- 1.1 The purpose of this policy is to provide a set of standards by which all users of ICT systems at the College will abide. This policy is linked directly to the ICT Security Policy, Staff Code of Conduct, Learner Agreement, Data Protection Policy and MIS Accounts Policy and has therefore been ratified by the Board of Governors and Senior Management

2. INTRODUCTION

- 2.1. The College offers new and exciting opportunities for staff, students and visitors by providing a rich and diverse range of ICT facilities. The College can only provide this excellent facility by maintaining a robust set of policies and procedures, and by adhering to current legislation relevant to ICT.

3. SCOPE

- 3.1. This policy applies to all users of ICT systems at the College. It is essential that all users read, and abide by these guidelines and make themselves aware of their responsibilities and the potential liabilities of using ICT systems. "ICT Systems" means, for example, any piece of computing equipment, printer, photocopier, telephones, network and attached equipment. This is not an exhaustive list and in the case of any doubt, clarification should be sought from Senior Management.

4. GENERAL COMPUTER USE

- 4.1. ICT systems must be treated with care and used only in accordance with the operating instructions. These are available from ICT Support if required.
- 4.2. No attempt must be made to use equipment which is labelled out of order. Likewise, equipment must not be used if there is reason to believe that it may not be in safe working order. Any apparent fault with hardware should be reported promptly to ICT Support.
- 4.3. The use of any ICT equipment for downloading, storage, printing and/or transmission of materials which the College considers to be obscene and/or offensive is strictly prohibited. Some examples are - pornographic, obscene, violent, offensive, copyrighted material etc. This includes storage of licensed music downloaded from the internet, or transferred from external storage media. If you are in any doubt, ask.
- 4.4. Users must take all reasonable steps to exclude and avoid the spread of malicious software, e.g. viruses, and must co-operate fully with all measures instituted by the College to prevent the spread of such software. In particular, users must not install or execute on a College computer any software obtained from a third party source, unless such software has been approved by ICT Support.
- 4.5. Computer programs on the ICT systems are protected by copyright. The College has the appropriate licences for all of the software on its systems. Users must comply with all their legal obligations concerning copyright, and must not copy any software or other data without the prior authorisation from the copyright owner. Such action would be in breach of copyright law.

Authorisation from the copyright owner does not constitute permission to store, execute or download on the College network.

- 4.6 Priority must be given to use of resources for work or educational use. Personal use must not:
- (i) Be of a commercial or profit-making nature, including private consultancy, or for any other form of personal financial gain. This includes using the email system for advertising items for sale
 - (ii) Be of a nature that competes or conflicts with the College in any way
 - (iii) Be excessive
 - (iv) Interfere with your work or study. An example, of this would be personal use outside of allocated break times
- 4.7 If users are in any doubt about what constitutes acceptable and appropriate use, they should seek the advice and guidance from, in the case of staff, their line manager, or in the case of students, their personal tutor. In all cases, advice can be sought from the Network Manager.
- 4.8 Where any of the College's ICT facilities are used to access any external network and/or computer facilities, users must also abide by any additional conditions pertaining to the external facilities that are imposed by the providers of such facilities.
- 4.9 The College views the unauthorised access or interference with any of its ICT facilities as a serious disciplinary offence. Any breach of these regulations shall be dealt with in accordance with the disciplinary procedures of the College applicable to the user concerned. In the case of a serious breach, the authorisation of a user to use particular ICT facilities may be withdrawn immediately, pending investigation.
- 4.10 Users must not by any deliberate or careless act or omission, jeopardise or seek to jeopardise the integrity of any ICT equipment or its software or any information stored within it or accessed through it.
- 4.11 Users must not access or attempt to access any ICT equipment, software or data which they are not authorised to access.
- 4.12 Users must take all necessary steps to protect and maintain the security of any equipment, software, data, storage area and/or passwords allocated for their use.
- 4.13 Users must not use any ICT facility for a purpose other than that for which they are authorised.
- 4.14 Food and drink should not be consumed near computer equipment and it is strictly forbidden to take food and drink into ICT classrooms. This includes classrooms where mobile laptops are being used.
- 4.15 Under the Computer Misuse Act 1990 it is an offence knowingly to corrupt a computer program or any of the data stored in the computer system.
- 4.16 You are responsible for safeguarding your password for the system. For reasons of security, your individual password should not be printed, stored online or given to others. User password rights given to employees should not give rise to an expectation of privacy.
- 4.17 The College operates a password complexity policy. This is currently:
- Minimum of 7 characters
 - Mixture of lower case, upper case and alpha-numeric characters
 - 24 passwords remembered
 - 180 days maximum password age

- 4.18 Your ability to connect to other computer systems through the network does not imply a right to connect to those systems or to make use of those systems unless authorised to do so.
- 4.19 You should not alter or copy a file belonging to another user without first obtaining permission from the creator or owner of the file.
- 4.20 A computer must never be left unattended whilst logged on in a publicly accessible place. This is a serious breach of the Acceptable Use Policy and may be treated as misconduct.
- 4.21 Users must seek advice from the Network Manager if they have any doubt about their authority to use any of the ICT facilities.
- 4.22 The amount of storage space for users' data is finite. All users should exercise good file and folder management to avoid wastage from duplication of information. Furthermore, users should avoid storing unwanted, outdated or irrelevant files.

5. THE NETWORK

- 5.1 The College provides a high speed network infrastructure using wireless and fixed cabling technologies. Whilst the fixed network points on walls may look alike, they connect to a variety of configurations "behind the scenes". For this reason, any network moves (including telephones) must be carried out by ICT Support staff.
- 5.2 The College provides both desktop and laptop computers that have been configured specifically for the tasks that they perform. College-owned computers are configured to link directly to security systems, such as Anti-virus systems, that are approved and managed by the College. Users must not, under any circumstances, connect any unauthorised equipment to the College network without first seeking approval from the Network Manager. The consequences of such action can be very serious for the integrity and stability of the network and any such action will be treated as misconduct or, in some cases, gross misconduct.
- 5.3 The College provides "guest" wireless access to a secure zone on the network. This is a very restricted zone, offering minimal services to users. Permission to connect to this system is not an automatic right and may be withdrawn at any time. Connection settings must be sought from ICT Support.

6. EMAIL

6.1 Provision of email

- 6.1.1 Email accounts are the property of the College and are provided primarily to assist the performance of your work or study. You should therefore have no expectation of privacy in any email sent or received, whether it is of a business or personal nature. The College reserves the right to monitor any and all aspects of its email system and to record and track any communications made by any user.
- 6.1.2 There is no automatic right to the use of email. Any misuse of the system may result in withdrawal of the facility. This may be treated as misconduct, and in certain circumstances, gross misconduct.
- 6.1.3 Where a user has had email withdrawn, this can only be reinstated by a request to ICT Support from the member of staff who requested the withdrawal or from a member of senior management.

6.2 Use of Email

- 6.2.1 Emails should be drafted with care. Due to the informal nature of email it is easy to forget that it is a permanent form of written communication and that material can be recovered even when it is deleted from your computer.
- 6.2.2 It is an inappropriate use of email for any user to store or send any material which might reasonably be considered to be obscene, offensive, abusive, sexist, racist or defamatory. You should be aware that such material is commonly contained in jokes sent by email. Such misuse of electronic systems will be treated as misconduct and will, in certain circumstances, be treated by the College as gross misconduct. The College reserves the right to use the content of any email in any disciplinary process.
- 6.2.3 The email system must not be used to send or forward trivial messages such as jokes.
- 6.2.4 Good housekeeping extends to email and users should keep an efficient filing system, regularly deleting unnecessary messages to prevent over-burdening the system.
- 6.2.5 Reasonable private use of email is permitted but should not interfere with your work (~~See 4.6 above~~). The contents of personal emails must comply with the restrictions set out in these guidelines and you should be aware of the information at 6.1.1 and 6.2.1 above.
- 6.2.6 Excessive private use of the email system during working hours may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct.
- 6.2.7 By sending emails on the College's system you are consenting to the processing of any personal data contained in that email and are explicitly consenting to the processing of any sensitive personal data contained in that email. If you do not wish the College to process such data you should communicate it by other means.
- 6.2.8 All emails that are sent externally are accompanied by the College's standard notice which currently includes the following statement:
- "This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. The views expressed in this email are that of the sender and not of the College, unless stated otherwise. If you have received this message in error, please contact postmaster@longleypark.ac.uk"*
- 6.2.9 Do not forward any virus warnings of any kind to **ANYONE** other than the Network Manager. It doesn't matter if the virus warnings come from an anti-virus vendor or have been confirmed by a large computer company, a colleague or your best friend! **ALL** virus warnings should be sent to the Network Manager only. It is their responsibly to assess and notify everybody of virus warnings. A virus warning which comes from any other source should be ignored.

7. INTERNET

- 7.1 All Internet access is logged and recorded.

- 7.2 Reasonable private use of the internet is permitted but should be kept to a minimum and should not interfere with your work. Excessive private access to the internet during working hours may lead to disciplinary action and may, in certain circumstances, be treated by the College as gross misconduct.
- 7.3 The sites accessed by you must comply with the restrictions set out in these guidelines. Accessing inappropriate sites may lead to disciplinary action and may, in certain circumstances, be treated by the College as gross misconduct.
- 7.4 Copyright applies to all text, pictures, video and sound, including those sent by email or on the Internet. Files containing such copyright protected material may be downloaded, but not forwarded or transmitted to third parties without the permission of the author of the material or an acknowledgement of the original source of the material, as appropriate.
- 7.5 The amount of available disk space is finite and due care must be taken when downloading files.
- 7.6 Users must never engage in political discussions through outside newsgroups using the College's computer system.
- 7.7 In the interests of information security, the College restricts access to certain sites and prevents the downloading of certain types of file and content. You must not download, or attempt to download programs, viruses, hacking tools, copyrighted material (including music in any format – MP3, for example). Likewise, you must not access, or attempt to access, sites which offer or promote such downloads. If you are in any doubt at all, you should contact ICT Support.
- 7.8 It is a serious offence to attempt to bypass any filtering or security system. An example of this would be accessing or attempting to access proxy sites or anonymisers on the internet. Any such activity may lead to disciplinary action and may, in certain circumstances, be treated by the College as gross misconduct.
- 7.9 If you think you have a legitimate request to download something that is blocked by one of the College security systems, you should submit a request to the Network Manager who will evaluate the request and take the appropriate action.

8. LAPTOPS

8.1 Software

- 8.1.1 Laptops issued to staff remain the property of the College. Therefore, only software licensed to the College may be installed on these machines, unless authority has been sought from the Network Manager. All software and operating systems should be installed only by, or with the authority of, ICT Support.
- 8.1.2 Staff should advise ICT Support of any additional licensed software that they wish to use both at home and at the College. The user must supply ICT Support with the licensed media and licence details for installation purposes.
- 8.1.3 Any unlicensed or unauthorised software found on laptops will be removed and reported to the appropriate line manager.
- 8.1.4 Laptops that are used at home must not be used by other family members

8.2 Virus Protection

- 8.2.1 All laptops are installed with updated virus protection. However, laptops require connection to the College network to enable updates to the anti-virus software. These updates are released from the vendors as frequently as every hour. Connection to the network **must** take place at least once each month and preferably every week, particularly if the laptop is connected to the Internet away from the College.
- 8.2.2 All laptops have some restrictions in place. That is, the full functionality that would be expected from a personally owned computer will not be available. This to ensure the device remains fully operational and security procedures are in place in case of unauthorised access. Only in very rare cases will these restrictions be lifted and then only after an auditable request to ICT Support. However, the College reserves the right to revert back to a restricted configuration in the interests of security and stability of the laptop and the network.
- 8.2.3 The increased use and ownership of laptop computers has been accompanied by a rise in theft because they are easy to steal and open to opportunistic theft. Apart from the loss of the hardware there may be the loss of sensitive commercial information or personal data which is of a far higher monetary value than the laptop itself. Users of laptops must take all reasonable care to prevent theft or loss of, and damage to, laptops and the software and data stored thereon.
- 8.2.4. If a laptop is taken off site, it is the responsibility of the user to ensure that adequate insurance cover is in place.
- 8.2.5 All laptops should be marked with the College name, postcode and an asset number. In addition, the laptops should be marked with the Smart Water ® security system.
- 8.2.6 Any loss or damage must be reported to the appropriate bodies. i.e. theft must be reported to the police and the Network Manager. Damage or loss must be reported to the Network Manager.
- 8.2.7 All users are expected transport their laptop in an approved, fit for purpose carry case.
- 8.2.8 No food or drink should be consumed in the vicinity of any computer resources. Any damaged to the laptop caused by food or drink spillage must be reported immediately.
- 8.2.9 Under no circumstances must any student remove a College laptop from the College premises. Any laptop issued to a student is done so on the grounds that it remains on the College premises at all times.

9. PRINTING & COPYING

- 9.1 The College provides a broad spread of printing facilities. However, there is no automatic right to personal possession of a printer. All users have access to a pool of communal MFP (Multi Function Printer) devices, from which print jobs can be retrieved.
- 9.2 All printers, including the aforementioned MFP devices, are monitored by a central print accounting system. Individual user accounts may be subject to a printing and copying quota. This is a non-transferable, non-refundable monetary value.
- 9.3 Print and copy jobs will be “charged” against a student quota or a staff department/directorate based on how the job is submitted and processed. The charging scheme has been approved by senior management and details can be found in the Learning Resource Centre.

- 9.4 Any printing for personal use must first be cleared with the relevant manager or, in the case of students, with their personal tutor.
- 9.5 Managers and Directors will receive notification, on a monthly basis, of the printing and copying volumes for their department. This information will also be passed to the Finance Office for budget charging.
- 9.6 Students who use their quota can purchase additional credits from the LRC.
- 9.7 Any disputes regarding quota levels or budgetary charging should, in the first instance, be referred to the Network Manager who will check printer log files.
- 9.8 Large print or copy jobs should be directed to the large, high speed, robust MFP devices in Reprographics rather than burden the smaller, low volume printers in classrooms and offices.

10. *TELEPHONES (INCLUDING COLLEGE-OWNED MOBILE TELEPHONES)*

- 10.1 All telephone calls, incoming, internal, and outgoing are subject to processing by a logging system. This system records dates, times, duration, and source & destination telephone numbers.
- 10.2 Occasional personal use of telephones (including College-owned mobile telephones) is permitted for staff. However, this should not interfere with work and should not be excessive (See 4.6 above). Directors and Managers receive a weekly itemised report of calls for their department, and can view the information listed in 10.1 above.
- 10.3 Calls to premium and other high rate numbers, for example, Directory Enquiries, should be avoided. There are alternative methods of obtaining telephone numbers and these should be exhausted before using premium rate services.
- 10.4 Where personal use of a telephone (or fax machine) will incur a high cost, for example, international calls, this should be by arrangement with the appropriate line manager in advance of the call being made. The College reserves the right to charge for personal calls.
- 10.5 It is an offence to use a mobile telephone whilst driving, without a hands-free kit. Users of College-owned mobile telephones may also be subject to disciplinary action if found doing so.
- 10.6 All staff are expected to be allocated, and use, a voicemail box.