

Acceptable User Policy for Pupils' Use of Hardware / Software at Leicester Grammar School

NB: The Acceptable User Policy refers to the use of hardware and software in school and to the use of the school's Virtual Learning Environment (VLE) outside of school.

CONDITIONS OF USE OF THE COMPUTING FACILITIES

Normal school rules for behaviour apply. In addition:

- Access must only be made via the pupil or staff member's (Users) authorised account and password, which must not be made available to any other person;
- Users must not walk away from their computer and leave it logged on;
- Activity that threatens the integrity of the school's ICT systems, or that attacks or corrupts other systems, is forbidden; this includes attempts to circumvent access controls to unauthorised areas;
- Users may not modify, change or in any other way alter, delete or add to system configurations, or software loaded on the system;
- Users must not move, open or tamper with any ICT equipment;
- Users must report all faults or damage to the computer system - including printers, PCs, or other peripherals - to staff on duty in the ICT suites immediately, who may be able to rectify minor faults; otherwise the Network Manager should be notified as soon as possible;
- Users must not send or take part in the preparation of text, graphics or audio material which is offensive, abusive, obscene or defamatory, or which may be unlawful; any material of this nature received must be reported immediately;
- Copyright of materials and intellectual property rights must be respected;
- Users must not plagiarise the work of others and present or submit it as their own;

- Users files may be examined and deleted if they pose a security threat to the system or misuse is suspected;
- Authorised school work must always take priority although legitimate private interests may be followed in the pupils' own time.

In addition, the following specific rules must be adhered to.

INFORMATION SECURITY

- You must take the appropriate steps to guard against unauthorised access to, alteration, accidental loss, disclosure or destruction of data.
- Under no circumstances should you divulge your password to anyone else nor should you gain access or attempt to gain access to information stored electronically which is beyond the scope of your authorised access level.
- You must, when selecting a password, endeavour to choose one which will not be obvious to another person. Passwords should be changed on a regular basis.

ELECTRONIC MAIL

The use of the e-mail system within the School is encouraged, as its appropriate use facilitates communication and improves efficiency. Used correctly, it is a facility that is of assistance to many employees. Its inappropriate use, however, causes many problems. This section sets out the School's view on the correct use of the e-mail system, and explains how this can be achieved, as well as the School's responses to its inappropriate use.

Monitoring

- The School reserves the absolute right to monitor pupils' use of any part of the network, including email usage.

Authorised Use

- Employees using the School's e-mail system or private emails, such as gmail or hotmail, should give particular attention to the following:
 - the standard of presentation: the style and content of an e-mail message must be consistent with the standards that the School expects from written communications
 - the extent of circulation: e-mail messages should only be sent to those for whom they are particularly relevant, and should not be sent people the pupil does not know or who might be upset by the email
 - the appropriateness of e-mail: e-mail should not be used as a substitute for face to face communication; "Flame-mails" (e-mails that are abusive) can be a source of stress and can damage working relationships, while hasty messages, sent without proper consideration, can cause unnecessary misunderstandings
 - the visibility of e-mail: if the message is confidential, the pupil must ensure that the necessary steps are taken to protect confidentiality
 - the individual concerned is liable for any defamatory information circulated either within the School or to external users of the system in school time; and
 - e-mail contracts: should not use the school network to buy or solicit any materials.

Unauthorised Use

The School will not tolerate the use of the e-mail system for any of the following:

- Any message that could constitute bullying or harassment (e.g. on the grounds of sex, race, age or disability)
- Excessive or inappropriate personal use, e.g. cartoons or chain letters
- On-line gambling
- Accessing pornography or other illegal or obscene material; and
- Downloading or distributing copyright information and/or any software available to the user.

NETWORK USE

- Network users will face action under the School's Disciplinary and Dismissal Procedure if found to:
 - any form of un-authorized game (i.e. video, images or audio files) on the school network.
 - access, possess, view or store pornography in any way. This also applies to any illegal or obscene material (i.e. information on the building of weapons etc). This includes using school laptops, workstations or any form of external storage device.
- Network users are responsible for the material they upload to the school network, which must be of a minimal size and relevant to school work, and must remove any material once it is no longer relevant or required.

INTERNET

The use of the Internet within this School is encouraged, as its appropriate use provides access to a wide range of useful information. Used correctly it is a facility which can be of valuable assistance to the School and to employees in the performance of their jobs. Its inappropriate use, however, causes many problems, ranging from excessive costs for the School to possible legal claims against the School.

Monitoring

- The School reserves the absolute right to monitor pupils' use of the network and the Internet.

Authorised Use

Access to the Internet is provided to employees for matters directly concerned with the business of the School. You should be aware that:

- leaving Internet access open while away from your chair means that unauthorised use may occur in the absence and be attributable to you

- spending long periods of the working day on the Internet may mean that normal work is not being done or other pupils are picking up an unequal share; and
- system records may be used to monitor your use of the Internet if it is felt to be inappropriate.

Unauthorised Use

The School will not tolerate the use of the Internet for any of the following:

- accessing / downloading pornography or other illegal or obscene material
- downloading software which has not been virus checked and approved e.g. games or free issue software;
- pupils' use of on-line services, personal communications, such as researching or booking holidays, on-line shopping¹, banking, chat-rooms; or creating and /or operating unauthorised personal web sites.

COMPUTER SOFTWARE

You have a duty to take all reasonable steps to ensure you do not spread computer viruses. It is your responsibility to ensure that you have up to date virus checking software on your home computer, before you transfer documents to and from the School by any electronic means including using memory sticks, flash drives, pen drives, or any portable memory devices.

Virus protection software is maintained and periodically updated by the School. It is mandatory that you re-boot your P.C. at the end of the day with the anti virus software to ensure that no viruses are present. You must not make 'pirate' copies of School owned software. This not only breaks School rules, it is an illegal practice.

Use of Internet and E-mail

In addition the following conditions of use apply:

- E-mail and Internet access must only be used for educational purposes²;

¹ Under certain circumstances, staff members and sixth form pupils may use the system for this form of personal use. Please see specific statements below.

- Pupils will access personal e-mail from the school system, in their own time only;
- Files attached to e-mails occupy bandwidth, which may degrade performance; they also pose a potential security risk, therefore pupils must seek permission before they send or open attachments;
- In-coming e-mail will be regarded as public. E-mail will be screened for viruses and may be examined for unacceptable content;
- Messages sent using the school domain name should be regarded in the same way as messages written on school headed paper;
- The forwarding of chain letters will be banned, as will the use of public chat rooms;
- Newsgroups are only available to staff and to senior pupils with specific permission;

The downloading of files occupies bandwidth and may degrade performance, also the loading of any executable files violates the conditions of use of computing facilities, permission must be sought from the network manager for exceptional need for this facility.

DATA PROTECTION

The School's use of the data protection act is in line with that laid out by law, i.e. The Data Protection Act 1998³ is concerned with the processing of computerised and manual information about living individuals (personal data) and gives rights of access to the individuals who are the subject of that information. Further, the Act places certain obligations on the School's [The Organisation's] data user, in respect of the personal information it processes or causes to be processed on its behalf by third parties.

- A data user must notify the Information Commissioner of any use of personal data from a third party unless covered by the exclusions in the Act.
- The Organisation must complete a notification covering all personal data presently held, specifying:

² Please see specific exceptions below.

³ http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1

- a general description of security measures
- the purposes for which the data is used
- a description of the data and the data subjects
- the sources and disclosures applicable to the information comprising the data; and
- the countries outside the European Economic Area to which the data is transferred (overseas transfers).
- Notification has to be updated as and when changes occur in any of the 'registrable particulars'.
- The holding and processing of un-notified data, which is covered by the Act, is a criminal offence and is subject to unlimited fines. The School, therefore, must operate within the terms of its notification.
- The School or any member of the school must:
 - not access, process or disclose any personal data other than is necessary, within the terms of the School's notification, to carry out the role for which you are employed; and
 - understand that any change in 'purposes, description, sources, disclosures, overseas transfers' of the personal data under its control may require an amendment to what has been notified.

In addition, the following specific rules and sanctions apply to the use of computers outside of lesson times when using public computer facilities, e.g. during free, lunch and break periods in the library.

CODE OF PRACTICE FOR ICT USE IN NON-LESSON PERIODS AT LEICESTER GRAMMAR SENIOR SCHOOL

This document is in addition to the Acceptable User Policy, which is designed for all computer use. This code is designed specifically for computer use during non-lesson times, and provides more unambiguous guidance and sanctions. This code is not meant to supersede the Acceptable User policy, but provide guidelines for staff administering ICT equipment and software.

N.B. All computer use is supervised and monitored throughout the day.

- Pupils must respect the furniture, hardware and software in the school's computing areas, or those temporarily being used for the use of computers. If they are found tampering with either, they will be referred to either the Head of ICT or, in the most extreme cases, to the Headmaster.
 - Pupils tampering with computers will be banned from the computer facilities for two weeks, receive an evening detention, and have their accounts blocked
 - Pupils tampering with software, or downloading software, will have their accounts blocked, and receive an after-school detention
 - In addition, those found damaging either software, furniture or hardware will be billed for the damage
- Pupils must tuck in their chairs after using a computer, and leave the computer and surrounding area in the way that they found it
- Sixth formers may use the computer room A6 or the library in private study periods, after booking or asking permission to do so. However, they must

treat both rooms with respect, and adhere to the normal code of conduct in these rooms

- Pupils are not allowed to eat in the school's computing areas, or use the computers if they have dirty hands. Pupils must also not leave litter in any part of the school's computing areas
 - Pupils found leaving litter or eating in a computer room will be banned from these areas for half a term
- In the library, computers may be booked in advance for use at break and lunchtime.
 - Bookings can only be made for the current day
 - Bookings can only be made by members of the library staff
- All computers must be logged-off at the end of each session.
 - Pupils leave computers logged-on at their own risk, and at the risk to their data
- Pupils must change their passwords at least every six months
 - Pupils who do not change their passwords do so at their own risk
 - Pupils who allow others to use their accounts for illegal activity will receive the same punishment as a person who breaks the code of practice using their own accounts
- At the end of a school day, the pupils must shut down their own computers
- Pupils must not play games on the school's computers at any time – unless they are designed and programmed by the pupil in a supervised session
 - Pupils found playing games will be logged off of their session on the computer and have to leave the room

- If pupils log back on after being logged off, their accounts will be blocked, and they will be given an account without internet or N: drive access.
- During break and lunch periods, sixth formers may use the computers in A6 for suitable non-academic purposes (e.g. emailing friends, or browsing allowable non-academic websites).
 - If there are no computers for those pupils wanting to do academic work, pupils doing non-academic work must give up their computers.