

HILLS ROAD SIXTH FORM COLLEGE

Acceptable Use by Students of College IT Facilities

Non substantive changes approved by Principal:

April 2016

Post of member of staff responsible:

Director of Digital Strategy

Date of equality impact assessment:

May 2010

1.0 Purpose

This policy is designed to ensure the maximum availability of College computers, that hardware and software perform reliably, that unnecessary support work is minimised and that the requirements of the law are met.

2.0 Forbidden Activities

- 2.1 The use of the College network, which includes the WiFi connection, in a way that may affect the integrity of the College IT facilities.
- 2.2 The use of College network to breach copyright laws.
- 2.3 The use of College network in a way that disrupts other users' legitimate activities.
- 2.4 The use of College network extensively for any purpose not connected with College activities.
- 2.5 The use of College network for illegal or "disreputable" purposes.

3.0 Policy details

The following guidance illustrates how the above rules will be interpreted. It is not exhaustive and students should note that sanctions will be taken where, in the view of the College, an activity falls within the forbidden list whether or not it is listed below.

3.1 Specific Restrictions

Students should refrain from:

- 3.1.1 Sending general e-mails to mailing lists without permission from the teacher/tutor concerned.
- 3.1.2 Using the IT facilities to advertise non-College events or items.
- 3.1.3 Doing anything that could be construed as cyber-bullying.
- 3.1.4 Playing games on any College IT equipment.
- 3.1.5 Storing or distributing games using a College Account.

- 3.1.6 Accessing inappropriate materials such as pornographic, racist or offensive material.¹
- 3.1.7 Eating or drinking near computers.
- 3.1.8 Installing software on College computers.
- 3.1.9 Using other people's computer accounts or allowing others to access your account.
- 3.1.10 Moving, opening or otherwise tampering with computer equipment.
- 3.1.11 Leaving yourself logged-on to any of the College computers.
- 3.1.12 Using College computers or the College WiFi connection for non-academic activities which generate heavy network traffic, especially those which interfere with others' legitimate use of IT facilities and/or which incur financial costs.

3.2 Contractual and Legal Restrictions

- 3.2.1 The College uses Ja.Net, the Joint Academic Network, as an Internet provider. In common with other ISPs they issue a code of conduct that the College must follow. In particular, students should be careful when sending emails outside College to ensure that they do not have the appearance of SPAM i.e. unsolicited bulk email.
- 3.2.2 Students should be aware of copyright restrictions and ensure that they comply with them in using or storing electronic materials.
- 3.2.3 A most serious view will be taken of the creation, storage or dissemination of material, words, images or programs, that could be deemed to either break laws or to have the potential to break laws of the United Kingdom.

3.3 College's Rights

- 3.3.1 The College reserves the right to examine and delete any files that may be held on its computer systems.
- 3.3.2 The College reserves the right to monitor* activities of students while using College IT facilities.

*To clarify the term "monitoring": computer usage will only be "monitored" when there is a reason to do so. This will be because some problem or transgression has been reported or otherwise detected. It will not occur randomly. The nature of the monitoring will be restricted to investigation of the problem or transgression and will not be extended in scope. The results of the monitoring will be treated as appropriately confidential. Monitoring should be interpreted as:

- visual inspection
- the use of software to see in real time the activities and screen displays on a computer
- the examination of computer logs and other reports to determine activities in the past

¹ 3.1.6 This access is already restricted by the IT network internet filter. All major categories of inappropriate material are blocked to network users.

- enabling the creation of logs recording significant events on the College computers.

Note that systematic monitoring is needed for routine housekeeping and this may trigger active monitoring of an individual student as part of investigating a problem.

4.0 Penalties

Any breaches of this policy will be dealt with in line with the College referral and disciplinary procedures and the Disciplinary Policy² where appropriate.

Linked Statements, Policies and Procedures:

College Policy and Procedures for Use in Cases of Inappropriate and Serious Misconduct by full-time 16-19 students
Student Code of Conduct

Further Guidance:

For further guidance, please contact:
Jonathan Sansom (Director of Digital Strategy)
Paul Rowan (IT Operations Manager)

² College Policy and Procedures for Use in Cases of Inappropriate and Serious Misconduct by full-time 16-19 students