

2 Introduction

- 2.1 This document gives specific guidance on the acceptable use of IT facilities (computers, printers, scanners, cameras, and like devices used for the creation, storage, transmission and manipulation of information) that form part of the Kingston College Network.
- 2.2 These regulations cover all students, and staff using College's IT facilities.

3 Why Have an Acceptable Use Policy?

- 3.1 Kingston College's Acceptable Use Policy for its Network has been created to:
- Ensure that all users have reasonable access to the facilities and encourage the responsible use of all its IT resources. Discourage practices that degrade the usability of network resources. Maintain the image and reputation of the Kingston College as a responsible provider of education and training.
 - Protect the security, reliability, and privacy of Kingston College's systems and network and the systems and network of others, consistent with the relevant policies of the Kingston College.
 - Safeguard the privacy and security of individual users, consistent with the relevant policies of Kingston College.

4 General Guidance

- 4.1 IT users shall not by any wilful, deliberate, reckless or unlawful act interfere with the work of another user or jeopardise the integrity of data networks, computing equipment, systems programs, or other stored information.
- 4.2 Authorised IT users are expected to treat as privileged any information which may become available through the use of such facilities and which is not obviously intended for unrestricted dissemination. Such information shall not be copied, modified, disseminated, or used, either in whole or in part, without the permission of the appropriate person or body.
- 4.3 *Staff are responsible for all User Accounts allocated to them. Passwords must not be disclosed to anyone. If a password is suspected of being having been discovered by another person, it must be changed immediately.* IT users are responsible for ensuring that they have logged out effectively from any machine used. It is the responsibility of the IT user to ensure that the data in his/her account(s) is protected.

Policy Title:	Acceptable Use of ILT Resources - Annex	Staff Member Responsible:	Director of ILT
Version:	Final July 2008	Review Due:	July 2011

Acceptable Use of ILT Resources Policy Annex



- 4.4 Reasonable precautions will be taken to ensure the reliability of the College Network servers, but no guarantee of the correct functioning of program(s) or equipment is given.
- 4.5 All data held on College Network servers will be protected by a back up procedure. This will usually means that data is backed up every night (Monday to Friday). All users are advised to hold a copy of all their files on removable media. No responsibility is accepted for the protection of any data held on local hard drives.
- 4.6 All computers on the College Network have a virus protection system installed. IT users must not interfere with the operation of this system.
- 4.7 The holding or distribution of computer files containing obscene or offensive material will be treated as a serious breach of these conditions unless explicitly authorised as part of an academic study.
- 4.8 College's Internet access is provided by JANET. You are also required to abide by the JANET Acceptable Use Policy for all Internet related communication and services.
- 4.9 IT users are not allowed to take into any computer suite, any form of entertainment which may interfere with other users. The taking of food and drink into these areas is not permitted. All mobile phones should be switched off before entering an IT area. Unreasonable behaviour (for example using facilities for games, chats, etc. when others cannot access a system to carry out study related work) will not be tolerated.
- 4.10 The College reserves the right for an appointed person authorised by Senior Management Team to copy and examine any files or information resident on the College Network.
- 4.11 It is prohibited for any unauthorised devices to be attached to the College Network. In order to protect the systems associated with the College Network, security measures exist to prevent switches, hubs, and wireless access points to be connected to the network.
- 4.12 IT users are prohibited to remove any computer-related devices including cabling from the College cabling infrastructure. Non-College machines can be connected to the infrastructure using the 'Guest' wireless which is available in most areas of the College, and dedicated 'Guest' physical network ports wherever available e.g. Café 100.

Policy Title:	Acceptable Use of ILT Resources - Annex	Staff Member Responsible:	Director of ILT
Version:	Final July 2008	Review Due:	July 2011

Acceptable Use of ILT Resources Policy Annex

4.13 IT users are expected to use the College IT facilities for College related activities. Limited personal use is allowed, provided that it does not prevent others from pursuing their legitimate work. The use of IT facilities for significant personal financial gain or any unlawful activity (such as storing obscene material) will be considered a serious offence.

5 Electronic Mail

5.1 When using E-mail IT users should be aware that:

5.2 E-mail is generally insecure. Anything sent may be read by others. Therefore never disclose anything confidential, such as passwords or credit card numbers, in an e-mail message.

5.3 The individual is responsible for all messages sent from a system using his/her network and e-mail accounts.

5.4 If an e-mail is sent that includes information that should not be disclosed to anyone other than the recipients, make this clear in the message.

5.5 Offensive or abusive e-mails or propagate chain mail must not be sent. Statements made in e-mail messages are considered to be "in permanent form" for the purposes of the Defamation Act 1996 and so you could be held responsible for any libellous statements made in an e-mail. The aspect of copyright must also be considered, especially when attachments consist of an extract of another person's work.

5.6 Be aware that attachments may contain viruses. Always save an attachment and ensure that your virus scan program has checked it before opening it.

6 Publishing Information on the Internet

6.1 If, as an IT user, you are responsible for providing information on any of the web pages hosted on a College server or on behalf of the College (e.g. Internet/Intranet) then you must ensure that you do not include or facilitate access to information that violates any College policy or existing legislations. In particular do not:

- Breach anyone's copyright.
- Publish obscene material.
- Publish material likely to incite racial hatred.
- Breach the data protection act.
- Make a libellous statement.

Policy Title:	Acceptable Use of ILT Resources - Annex	Staff Member Responsible:	Director of ILT
Version:	Final July 2008	Review Due:	July 2011

Acceptable Use of ILT Resources Policy Annex

- 6.2 IT users are not allowed to use the College's name, logo, mark, statements or images and must not make suggestions or statements that claim or imply any representation of the College when publishing information on personal (non-College controlled) websites.
- 6.3 IT users are not allowed to use web pages hosted on College servers for commercial purposes.
- 6.4 It is expected that IT users will use their ability to access the Internet wisely, taking into full account the reason for their membership of the College.

7 Software

- 7.1 In general, systems and applications software (and many databases and datasets) are only licensed for use on the systems upon which they can be found. Unauthorised copying of such items is commonly known as 'piracy' and is an offence under the Copyright, Designs and Patents Act 1988.
- 7.2 No attempt should be made to copy software or databases/datasets from the College or other computer systems.
- 7.3 If software from the College is obtained for use at home, proper procedures as set out in the relevant licence must be followed.

8 Data Protection

- 8.1 Legislation under the Data Protection Act 1984/1998 is quite extensive and a full explanation of its implications is beyond the scope of this document. However, it is generally concerned with access to, and treatment of, personal information on individuals. Hence, if work is undertaken on a College computer which involves information relating to individuals that has not been de-personalised, it is very important that this is discussed with the College's designated staff responsible for the Data Protection within the institution.

9 Suspected Breaches of the IT Regulations

- 9.1 Any person believed to be in breach of one or more of the above rules shall be reported to the Deputy Principal of the College. Proceedings may be initiated under either or both of the College disciplinary procedure and any appropriate legislation.

Policy Title:	Acceptable Use of ILT Resources - Annex	Staff Member Responsible:	Director of ILT
Version:	Final July 2008	Review Due:	July 2011