

## **Guidelines for Use of IT Facilities**

### **Scope**

1. These guidelines cover the use of ETC International College-owned or licensed IT facilities, including computers, peripherals, networks, software and data, and also IT facilities owned by other organisations or privately owned which are directly attached to the ETC data network, physically or by wireless connection, or which use for data transfer telephone lines serving ETC. These are all referred to as "College IT facilities" for the purpose of these guidelines.

2. The guidelines lay down obligations applying to all users of College IT facilities, and to staff and students of the College using other IT facilities to communicate with or otherwise use College IT facilities. They supplement, and in some cases reiterate, English law relating to the use of IT facilities. Breach of these guidelines constitutes a breach of College regulations and in some cases may constitute a disciplinary issue or a matter that may lead to criminal proceedings.

### **Control of IT facilities**

4. The College reserves the right to exercise control over all activities on its IT facilities and networks, including monitoring of systems and electronic communications and access to external electronic resources. The reasons for undertaking such monitoring include: to establish the existence of facts, to ascertain compliance with regulatory or self-regulatory practices or procedures or to ascertain or demonstrate standards which are or ought to be achieved (quality control and training), to prevent or detect crime, to investigate or detect unauthorised use of telecommunication systems or, to secure, or as an inherent part of, effective system operation.

5. This monitoring is permitted within the terms allowed by the Regulation of Investigatory Powers Act (RIPA) 2000 and The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. These Regulations constitute formal notice that communications may be intercepted for reasons allowed within these Acts.

### **Authorisation**

6. To use any IT facilities at the College you must have authorisation to use those specific facilities. This authorisation is granted by the department owning the facilities. (In these Guidelines, "department" means academic department, centre or administrative section, such as, for example, "the Academic department").

7. In addition, if the facilities are controlled by a central computing account and password, you must be registered with the Computing Service and have your own central computing account and password, or you must be using a special computing account set up for teaching purposes and which you have been temporarily authorised to use. The central computing account and password is usable throughout the College. (An example of an IT facility which does not require a computing account is a self access terminal. Permission to use such terminals is granted as part of the general authorisation to use the Library.)

8. If you are an authorised user of an active computing account and password, you are thereby permitted to use the central IT user services run by the Computing Service.

10. Computing accounts and passwords are granted to individuals, or in certain cases to groups of individuals. You must not use, or attempt to gain access to, the computing account belonging to another individual or group of individuals. In the case of an individual account, you must not disclose your password to any other person nor allow another person to use your account. If you are a member of a group with a group account, you must not disclose the password to any person outside the group nor allow any person outside the group to use the account. As an exception, a head of department may grant a staff member the right temporarily to use the account of another individual or group with the agreement of the latter, for example in an individual's absence.

### **Use of facilities**

11. You may use College IT facilities for purposes related to College work or study, and for a limited and reasonable amount of personal use. Such use is a privilege and not a right and must not inhibit or interfere with the use by others for College purposes.

12. You must not use College IT facilities for outside work, whether paid or unpaid, or for non-College activities which generate income, except by explicit permission of a head of department, and in the case of central facilities the Operations and Facilities Manager.

13. You must not use College IT facilities to engage in any unlawful activity, or to infringe College Regulations.

14. You must not use College IT facilities without permission. This includes using computers and networks, or accessing, copying, reading, or storing software, databases, messages or data. You must not attempt to gain unauthorised access to any College IT facilities, or use College facilities to gain unauthorised access to other IT facilities.

15. You must not deliberately or recklessly act in a way which directly or indirectly causes disruption to others' use of College IT facilities, or so use College IT facilities to disrupt the use of IT facilities elsewhere.

16. You must not knowingly download, transmit, store, generate or use any program, tool or virus designed to damage or disrupt or in any other way interfere with the functioning of IT facilities, unless explicitly authorised to do so as part of your College work, and you must take sufficient care to minimise the risk of doing this inadvertently. If you suspect you have a virus then you must take action to eliminate it.

17. You must not alter computer material on College IT facilities without permission of the owner or licence holder. This includes systems software, other software, configurations, databases, messages, data files, web pages or web sites. Likewise you must not use College IT facilities to alter computer material elsewhere without permission.

18. In general, systems and application software that is installed or otherwise available within the College is protected by licence agreements. You must not use such software unless you have permission to use it under College licence agreements. You must not copy software which is installed

or otherwise available unless you have explicit permission or own a licence which permits you to do that.

19. You must treat as confidential any information to which you gain access in using College IT facilities and which is not on the face of it intended for unrestricted dissemination. You must not copy, modify or disseminate such information without explicit permission from an authorised person. The ability to read or alter information held on a computer system does not imply permission to do so.

20. Any information about living individuals must be held in accordance with College policy and the responsibilities as a Data User under the Data Protection Act 1998. Further guidance is available on these responsibilities is given on the Records Management website or from the College Records Manager.

21. In order to ensure effective running of IT services, or to manage costs, the College from time to time imposes controls on the use of systems. An example is the use of firewalls in some areas of the College. You must not attempt to circumvent such controls.

22. You must not use College IT facilities to create, transmit, store, download or display any offensive, obscene, indecent or menacing images, data or other material, or any data capable of being resolved into such material. (There are certain exceptions for academic purposes, which require the explicit authorisation of a head of department).

23. You must not use College IT facilities to defame, harass, offend or hinder another person, by creation, transmission, storage, download or display of materials, or by other means.

24. You must not send an email or message that does not correctly identify you as the sender, or which appears to originate from another person, or otherwise attempt to impersonate another person. You must not send unsolicited emails to a large number of recipients, without proper authorisation to do so, or unless the recipients have indicated an interest in or consented to receiving such email.

25. You must not use College IT facilities to create, access, store or transmit material in a way which infringes a copyright, trade mark, or other intellectual property right.

26. You must not cause damage to College-owned IT facilities, or move or remove such facilities without authorisation. Any damaged or faulty facilities should be reported to that repairs can be made.

27. In using central facilities you must observe rules or guidelines issued from time to time by Information Systems Services.

28. Open access computing laboratories are open long hours, some of them around the clock. To help keep them in working condition, you must not cause litter or damage, and must not bring food or drink into the laboratories or consume it there, except by prior arrangement with the Computing Service. You must not smoke in the laboratories.

29. You must vacate computers in open access laboratories promptly when the laboratory is being

closed, at the start of a booked teaching or demonstration session, or at other times when requested by an authorised member of staff.

30. Computers are not allowed to be reserved by individuals, except with the agreement of the Director, the Principal, the Director of Studies or the Operations and Facilities Manager.

31. You must not use laboratory computers for non-work purposes if the laboratory is full and any user is waiting for a machine.

32. Certain work stations in open access laboratories have special facilities to support disabled users. You must vacate such a work station should somebody with a requirement to use its resources need it.

33. You must not attempt to change or reconfigure the operating system or other software on open access laboratory computers.

#### Web servers and websites

34. A web server set up on College IT facilities must be authorised by a head of department, or by the Operations and Facilities Manager, and the server must be registered with Information Systems Services. (Web servers with restricted access, authorised and set up as part of IT course work or research, are exempt from the preceding provision.) The person setting up or registering the server is responsible for ensuring that the server is well-managed, and that its content and management complies with these guidelines.

35. Third party or guest web sites may be hosted on College IT facilities only with the agreement of the Operations and Facilities Manager and must be registered with Information Systems Services by a College staff member or student. The person registering the site is responsible for ensuring that its content and management complies with these guidelines.

#### **External guidelines**

36. You must comply with all relevant external guidelines and laws which affect your use of College IT facilities, including:

The Computer Misuse Act 1990.

The Data Protection Act 1998.

The Copyright, Designs & Patents Act 1988

The Copyright (Computer Programs) Regulations 1992

#### **Infringements**

37. If a student of the College is found to infringe these guidelines, his or her computing account may be suspended by the Operations and Facilities Manager and a report made to the Principal and the Director of Studies.

38. If a member of the College staff is found to infringe these guidelines, his or her computing account may be suspended by the Operations and Facilities, acting on behalf of the Principal, and a report made to the Principal, the Director and Director of Studies.

39. If an authorised user who is neither a student nor a staff member of the College is found to infringe these guidelines, his or her authorisation will be revoked and computing account withdrawn by the Operations and Facilities Manager.

40. If material accessible via the College network, including a web site or server, is suspected to be in violation of these guidelines, then access to the material, or to the systems hosting the material, may be suspended by the Operations and Facilities Manager pending an investigation.