

Eaton Bank School

Acceptable use of ICT Facilities Policy

Contents

1.0 Introduction

2.0 Purpose

3.0 Scope

4.0 Responsible Authorities

5.0 Policy Statements

5.1 General

5.2 Acceptable Use

5.3 Personal Use

5.4 Unacceptable Use

5.5 Prevention, Detection & Investigation of Misuse

6.0 Legislation

6.1 Computer Misuse Act 1990

6.2 Data Protection Act 1998

6.3 Libel

6.4 Copyright

7.0 Sanctions

1. Introduction

This document defines the Eaton Bank School's policy in respect of the acceptable use of its information and communications technology (ICT) facilities.

2. Purpose

The Network Manager is responsible, on behalf of Eaton Bank School, for minimising and containing potential risks to Eaton Bank School and its members, both operational and legal, from the consequences of the misuse of its ICT facilities. The purpose of this policy is therefore to state clearly both users' obligations in using these facilities and Network Manager's responsibility and authority in taking action to safeguard them.

3. Scope

This policy applies to all staff, students, contractors, consultants, authorised guests and other personnel at the Eaton Bank School and includes Acceptable Use, Personal Use and Prohibited Use of Eaton Bank School's ICT facilities, which encompass (but are not restricted to):

- network infrastructure, including (but not exclusively) the physical infrastructure whether cable or wireless, together with network servers, firewall, connections, switches and routers
- network services, including (but not exclusively) internet access, web services, email, wireless, messaging, telephony and fax services
- computing hardware, both fixed and portable, including (but not exclusively) personal computers, workstations, laptops, PDAs, servers, printers, scanners, disc drives, monitors, displays, keyboards, tablets and pointing devices
- software and databases, including (but not exclusively) applications and information systems, virtual learning and videoconferencing environments, language laboratories, software tools, information services, electronic journals & e-books

4. Responsibility

This policy is issued under the authority of the head teacher who as an employee of Eaton Bank School is responsible for enforcing sanctions where necessary to safeguard Eaton Bank School and its community.

The IT Infrastructure is managed by the Network Manager who is responsible for the prevention and detection of ICT misuse.

This policy is managed by the network manager who is responsible for investigating incidents of ICT misuse.

5. Policy Statements

5.1 General

It is the policy of Eaton Bank School:

- to provide a working environment that encourages access to knowledge and sharing of information.
- to maintain ICT facilities for teaching, learning and administrative purposes which provide access to its community for local, national and international sources of information.
- that ICT facilities will be used by members of its community with respect for the public trust through which they have been provided, and in accordance with prevailing laws and such regulations and policies established from time to time by Eaton Bank School.
- to ensure that Eaton Bank School is protected by holding users responsible for safeguarding passwords and access identities. Passwords and identities must not be shared.

5.2 Acceptable Use

It is the policy of Eaton Bank School:

- that Eaton Bank School's ICT facilities are provided in support of Eaton Bank School's teaching, learning, and administrative activities
- that they may be used for any purpose that is in accordance with the aims and policies of Eaton Bank School
- that only registered users (i.e. those holding valid 'Eaton Bank School' usernames and passwords) or those given permission by the Head Teacher, Deputy Head Teacher or Network Manager are permitted to use Eaton Bank School's ICT facilities.
- that users are expected to:
 - be prepared to confirm proof of identity. This must be shown when requesting any changes to a network account.
 - respect the published times of access to the facilities
 - respect the rights of others, and conduct themselves in a quiet orderly manner when using the open access facilities
 - comply with all valid regulations and legislation covering the use of Copyright and licensed material, including software, whether those regulations are made by law, or the originator of the material, or the distributor of the material or by any other legitimate authority
 - make all reasonable efforts to send data that is 'Virus Free', and to protect themselves from viruses and hacking attempts when connected to Eaton Bank School's network either on or off Campus. Eaton Bank School will not be held responsible for any damage to users' systems or information that occurs through such virus or hacking attacks.
 - conform to all other appropriate policies and guidelines determined by the NETWORK MANAGER (including netiquette guidelines), Eaton Bank School (including web page design guidelines), and externally .

5.3 Personal Use

- Eaton Bank School accepts that a member's Personal Use of Eaton Bank School's ICT facility is within the scope of Acceptable Use, subject to the provisos within this document. It is the policy of Eaton Bank School:
 - that provided that personal use is occasional and reasonable and does not interfere with, nor detract from an individual's everyday workload and commitments, nor with the effective functioning of Eaton Bank School or any part of it, and that it complies with all other terms of this Acceptable Use Policy then it will normally be tolerated
 - to reserve the right to withdraw access to ICT facilities for this category of use at any time.

5.4 Unacceptable Use

It is the policy of Eaton Bank School to prohibit the use of its ICT facilities when used or attempted to be used intentionally in contravention of the general principles outlined in 5.1 above.

The activities prohibited under this policy include (but are not restricted to) those listed below. In particular, users must not:

1. cause the good name & reputation of Eaton Bank School or any part of it to be damaged or undermined.

2. create or transmit (other than in the course of properly supervised research where this aspect of the research has the explicit approval of Eaton Bank School's official processes for dealing with relevant ethical issues) any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.
3. access, create, change, store, download or transmit material which Eaton Bank School may deem to be threatening, defamatory, abusive, indecent, obscene, racist or otherwise offensive.
4. place links to websites which have links to, or displays pornographic and inappropriate material, facilitate illegal or improper use, or to bulletin board which are likely to publish defamatory materials or discriminatory statements; or where copyright protected works such as computer software or music are unlawfully distributed.
5. generate excessive noise, cause annoyance, inconvenience or needless anxiety to, or to violate the privacy of, anyone else.
6. allow the ICT facilities to be damaged or contaminated by food, drink or smoking materials.
7. interfere with the legitimate use by others of the ICT facilities, or interfere with or remove computer printout or media belonging to others.
8. send unwanted, e-mail, chain letters, hoax virus warnings, pyramid letters or similar schemes using Eaton Bank School e-mail system.
9. falsify E-mails to make them appear to have been originated from someone else.
10. make use and possess, distribute, sell, hire or otherwise deal with any unauthorised copies of computer software for any purpose without the license of its owner;.
11. install any software that is not licensed to Eaton Bank School and /or install without authorisation software licensed to Eaton Bank School on any of Eaton Bank School's computer systems under any circumstances;
12. transmit unsolicited unauthorised commercial or advertising material.
13. use the ICT facilities for commercial , social or group distribution activities unless permission has been formally granted by the NETWORK MANAGER;
14. gain unauthorised personal commercial benefit.
15. gain unauthorised access to facilities or services via Eaton Bank School network.
16. allow others to gain such unauthorised access, either wilfully by disclosing user names or passwords or neglectfully by failing to log out of the system, thereby permitting unauthorised use of an Eaton Bank School account.
17. disseminate any material which may incite or encourage others to carry out unauthorised access to or unauthorised modification of Eaton Bank School's or others' computer facilities or materials.
18. introduce and transmit material (including, but not restricted to, computer viruses, Trojan horses and worms) designed to be destructive to the correct functioning of computer systems, software, networks and data storage, or attempt to circumvent any precautions taken or prescribed to prevent this.
19. attempt to circumvent Eaton Bank School's firewall systems, or use file-sharing systems (sometimes known as P2P or peer-to-peer).
20. change, damage, dismantle, corrupt, or destroy (or cause to be changed, damaged, dismantled, corrupted or destroyed) any network component, equipment, software or data, or its functions or settings, which is the property of Eaton Bank School.

21. cause any of Eaton Bank School's ICT services to be overloaded, impaired, disrupted, curtailed or denied (other than in compliance with the direct instruction of the Network Manager).
22. connect any non approved computer network equipment (including wireless access points) to Eaton Bank School network without first gaining the written permission of the Network ;
23. set up any network services (e.g. web servers, e-mail services etc) unless formally sanctioned by the Network Manager.
24. register any domain name which includes the name of Eaton Bank School or any name which may mislead the public into believing that the domain name refers to Eaton Bank School.
25. use equipment (including mains leads) which has not first been PAT Safety tested (Portable Application Tested) by Eaton Bank School approved staff. Such equipment must display an up to date PAT label.
26. continue to use any item of networked hardware or software after the Network Manager has requested that use ceases because of its causing disruption to the correct functioning of Eaton Bank School ICT facilities, or for any other instance of Unacceptable Use.
27. fail to comply with any action directed by the Network Manager to prevent or respond to any threats to the correct functioning of Eaton Bank School ICT facilities;
28. contravene any local rules and guidelines for using Eaton Bank School ICT facilities outside Eaton Bank School.
29. create or transmit material that infringes the copyright of another person or institution, or infringe the Copyright laws of the UK and other countries.
30. interfere with the legitimate activities of other users covered within the principles outlined in Section 5.2 of Acceptable Use.
31. otherwise act against the aims and purposes of Eaton Bank School as specified in its rules, regulations, policies, and procedures adopted from time to time.
32. contravene applicable laws and prevailing regulations and policies applied by relevant bodies external to Eaton Bank School.

5.5 Prevention, Detection & Investigation of Misuse

Monitoring may take place, with the prior permission of students, to facilitate academic and pastoral care by ensuring that students not using electronic systems vital for study are identified and encouraged to do so and thereby not fall behind in their studies.

Monitoring may take place periodically within the guidelines set down by the Regulation of Investigatory Powers Act (RIPA) 2000.

Eaton Bank School retains the right under the RIPA Act to access all information held on its information and communications facilities to monitor or intercept any system logs, web pages, E-mail messages, network account or any other data on any computers system owned by Eaton Bank School. This will be for the purposes of preventing, detecting or investigating crime or misuse, ascertaining compliance with regulatory standards and Eaton Bank School policies, or to secure effective system operation.

Eaton Bank School reserves the right to inspect and validate any items of Eaton Bank School owned computer equipment connected to the network. Any other computer equipment connected to Eaton Bank School's network will be deemed unauthorised and will be removed unless previously authorised for connection to the Eaton Bank School network by the NETWORK MANAGER.

It is the policy of Eaton Bank School:

- to publish its Acceptable Use Policy and to promote this to all users of Eaton Bank School Network
- to provide advice to staff and students, on request, on matters relating to acceptable use
- to take swift and effective action within existing disciplinary and / or legislative frameworks against anyone found to be intentionally misusing the information and communications facilities;

In all cases where there is the potential for Eaton Bank School's ICT facilities to be misused, it is Eaton Bank School's policy to:

- record the identity of the individual using the specific facility at any given time;
- retain these records for not less than three calendar months, and shall make them available to those senior staff appointed by Eaton Bank School to investigate complaints of misuse;
- destroy these records after twelve calendar months unless required in connection with a specific investigation;

6. Legislation

6.1 Computer Misuse Act 1990

It is a criminal offence (Computer Misuse Act 1990) to gain unauthorised access to a computer system to make any unauthorised modification of computer material (including the introduction of a computer virus) or to interfere with any computing system provided in the interests of health and safety. For more information see

http://www.hms0.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

6.2 Data Protection Act 1998

The Data Protection Act 1998 regulates the storage of personal information (i.e. any information that can be identified as relating to a particular person or person(s) on computer systems. Before storing any such information on Eaton Bank School computer system, you must notify the NETWORK MANAGER in writing. It is everyone's responsibility to ensure that any such information complies with the law. For more information regarding Data Protection see <http://www.dataprotection.gov.uk>

6.3 Libel

Libel is a civil wrong, which in proven cases, may incur substantial compensation. It is very complicated and therefore one of the easiest laws to contravene through ignorance. Facts concerning individuals or organisations must be accurate, verifiable and views or opinions must not portray their subjects in any way that could damage their reputation. Users must check with the NETWORK MANAGER before publicly displaying any contentious material. Web pages and E-mail messages are regarded as published material.

6.4 Copyright

The Copyright laws of the UK and other countries must not be infringed. Downloading material from the Internet carries the risk of infringing copyright. This applies to files, music, films, TV programmes, documents and software, which must be licensed. Material illegally copied in this country or elsewhere and then transmitted to another country via the Internet, will also infringe the copyright laws of the country receiving it.

Copyright, Design and Patents Act 1998 is applicable to all types of creations, including text, graphics and sounds by an author or artist. This will include any that are accessible through Eaton Bank School's computer systems.

Any uploading or downloading of information through on-line technologies which is not authorised by the copyright owner will be deemed to be an infringement of her/his rights.

Users must not make, transmit or store an electronic copy of copyright material on Eaton Bank School's computing services without the permission of the owner.

7. Sanctions

Where misuse of ICT facilities has been identified, the matter will be investigated under Eaton Bank School's appropriate disciplinary procedure. As an officer of Eaton Bank School, the NETWORK MANAGER or his / her nominee has the authority to investigate cases of alleged misuse and where applicable to apply sanctions directly, or to refer individuals to senior Eaton Bank School staff for disciplinary action.

Any misuse which is in contravention of the law and/or which involves the intentional access, creation, storage or transmission of material which may be considered indecent or obscene (other than in the course of specified research where this aspect of the research has the explicit approval of Eaton Bank School's official processes for dealing with relevant ethical issues) will be regarded as an act of gross misconduct.

Staff and/or student disciplinary procedures will be used to apply any necessary sanctions.

Where there is evidence of a criminal offence, the issue will be reported to the Police for them to take action. Eaton Bank School will co-operate with the Police and other appropriate external agencies in the investigation of alleged offences.

"Eaton Bank School is grateful to the Director of the Information Systems Division at the University of Salford for allowing use of policies developed for the University as a basis for the policies developed for Eaton Bank"