West Hill School

ICT Security Policy

The purpose of the Policy is to protect the School's information assets from all threats, whether internal or external, deliberate or accidental.

Last Modified: Paul Gillon
10/03/2011

West Hill School ICT Security Policy

Contents

Document Control			
Version	Change	Author	Date
1.0	First Edition	Mrs L. Harrison Mr P. Gillon	March 2011

West Hill School ICT Security Policy

1. Introduction

1.1. The purpose of the Policy is to protect the School's information assets from all threats, whether internal or external, deliberate or accidental.

1.2. It is the policy of West Hill School to ensure that:

- information will be protected against unauthorised access
- confidentiality of information will be assured
- integrity of information will be maintained
- regulatory and legislative requirements will be met
- business continuity plans will be produced, maintained and tested
- ICT security training will be available to all staff

2. Policy Objectives

2.1. Against this background there are three main objectives of the ICT Security Policy:

- to ensure that equipment, data and staff are adequately protected against any action that could adversely affect the school;
- to ensure that users are aware of and fully comply with all relevant legislation;
- to create and maintain within the school a level of awareness of the need for ICT security to be an integral part of the day to day operation so that all staff understand the need for ICT security and their own responsibilities in this respect.

3. Application

3.1. The ICT Security Policy is intended for all school staff who are either controllers of the system or who are users and supporters of the school's administration and curriculum ICT systems or data. Pupils using the school's ICT systems or data are covered to a greater extent by the school's 'ICT Acceptable Use Guide' document.

3.2. For the purposes of this document the terms 'ICT' (or 'ICT system'), 'ICT data' and 'ICT user' are defined as follows:

- 'ICT' (or 'ICT system') means any device or combination of devices used for the storage or processing of data and includes: workstation (netbook, notebook, desktop/tower PC), PDA, cash till, server or any other similar device;
- 'ICT data' means any information stored and processed within the ICT system and includes programs, text, pictures and sound;
- 'ICT user' applies to any School employee, pupil or other authorised person who uses the school's ICT systems and/or data.

4. Roles and Responsibilities

4.1. The ICT Security Policy relies on management and user actions to ensure that its aims are achieved. Consequently, roles and responsibilities are defined below.

4.2. Governing Body

4.2.1. The governing body has the ultimate corporate responsibility for ensuring that the school complies with the legislative requirements relating to the use of ICT systems and for disseminating policy on ICT security and other ICT related matters. In practice, the day-to-day responsibility for implementing these legislative requirements rests with the Headteacher.

4.3. Headteacher

4.3.1. The Headteacher is responsible for ensuring that the legislative requirements relating to the use of ICT systems are met and that the school's ICT Security Policy, as may be amended from time to time, is adopted and maintained by the school. He/she is also responsible for ensuring that any special ICT security measures relating to the school's ICT facilities are applied and documented as an integral part of the Policy.

4.3.2. In practice, the day to day functions should be delegated to the 'ICT Network Manager', who must be nominated in writing by the Headteacher. This would take the form of an item in a job description.

4.3.3. The Headteacher is responsible for ensuring that the requirements of the Data Protection Act 1998 are complied with fully by the school. This is represented by an on-going responsibility for ensuring that the :

- registrations under the Data Protection Act are up-to-date and cover all uses being made of personal data and
- Registrations are observed with the school.

4.3.4. In addition, the Headteacher is responsible for ensuring that users of systems and data are familiar with the relevant aspects of the Policy and to ensure that the appropriate controls are in place for staff to comply with the Policy. This is particularly important with the increased use of computers and laptops at home. Staff should exercise extreme care in the use of personal data at home to ensure legislation is not contravened, in particular the Data Protection Act 1998.

4.4. ICT Network Manager

4.4.1. The 'ICT Network Manager' is responsible for the school's ICT equipment, systems and data and will have direct control over these assets and their use, including responsibility for controlling access to these assets and for defining and documenting the requisite level of protection. The ICT Network Manager will be an employee of the school.

4.4.2. The ICT Network Manager will administer the practical aspects of ICT protection and ensure that various functions are performed, such as maintaining the integrity of the data, producing the requisite back-up copies of data and protecting the physical access to systems and data.

4.4.3. In line with these responsibilities, the ICT Network Manager will be the official point of contact for ICT security issues and as such is responsible for notifying the Headteacher or Chair of Governors of any suspected or actual breach of ICT security occurring within the school. The Headteacher or Chair of Governors should ensure that details of the suspected or actual breach are recorded and made available upon request. The Headteacher or Chair of Governors must advise the Governing Body of any suspected or actual breach of ICT security pertaining to financial irregularity.

4.4.4. It is vital, therefore, that the ICT Network Manager is fully conversant with the ICT Security Policy and maintains an up to date knowledge of best practice and follows the associated approved practices.

4.5. School Technician

4.5.1. The school technician is responsible for maintaining, repairing and proactively supporting the ICT System so that it can meet the requirements of the ICT Security Policy. The School Technician will respond to actions delegated by the school's nominated 'ICT Network Manager' in order to ensure that the ICT System can comply with the ICT Security Policy.

4.5.2. The school technician will also monitor the ICT System for breaches of security and inform the Headteacher.

4.6. Users

4.6.1. Users are those employees, pupils or authorised guests of the school who make use of the ICT system to support them in their work. All users of the school's ICT systems and data must comply with the requirements of this ICT Security Policy. The school has an ICT Acceptable Use Guide which summarises the responsibilities of users of the school's ICT systems.

4.6.2. Users are responsible for notifying the ICT Network Manager of any suspected or actual breach of ICT security. In exceptional circumstances, users may report any such breach directly to the Headteacher, Chair of Governors or to Tameside MBC Internal Audit department.

4.6.3. Users are responsible for the equipment they use including:

- Physical security
- Virus updates
- Operating system updates
- Security of data
- Their own passwords.

5. Management of the Policy

5.1. Sufficient resources should be allocated each year to ensure the security of the school's ICT systems and to enable users to comply fully with the legal requirements and policies covered in this policy. If insufficient resources are available to fully implement this policy, then the potential risks must be documented and reported to Governors by the Headteacher.

5.2. Suitable training for all ICT users and documentation to promote the proper use of ICT systems will be provided. Users will also be given adequate information on the policies, procedures and facilities to help safeguard these systems and related data. A record of the training provided through the school to each individual user will be maintained. Maintenance of this record should be the responsibility of the nominated 'ICT Network Manager'.

5.3. In addition, users will be made aware of the value and importance of such ICT systems and data, particularly data of a confidential or sensitive nature, and be made aware of their personal responsibilities for ICT security.

5.4. To help achieve these aims, the relevant parts of the ICT Security Policy and any other information on the use of particular facilities and techniques to protect the systems or data will be disseminated to users.

5.5. The Headteacher must ensure that adequate procedures are established in respect of the ICT security implications of personnel changes. Suitable measures should be applied that provide for continuity of ICT security when staff vacate or occupy a post. These measures as a minimum must include:

- a record that new staff have been issued with, have read the appropriate documentation relating to ICT security, and have signed the list of rules;
- a record of the access rights to systems granted to an individual user and their limitations on the use of the data in relation to the data protection registrations in place;
- a record that those rights have been amended or withdrawn due to a change to responsibilities or termination of employment.

6. Physical Security

6.1. Location Access

6.1.1. Adequate consideration should be given to the physical security of rooms containing ICT equipment (including associated cabling). As far as practicable, only authorised persons should be admitted to rooms that contain servers or provide access to data. The server rooms should be locked when left unattended. Ideally, such rooms should have a minimum of key pad access.

6.1.2. The ICT Network Manager must ensure appropriate arrangements are applied for the removal of any ICT equipment from its normal location. These arrangements should take into consideration the risks associated with the removal and the impact these risks might have.

6.2. Equipment siting

6.2.1. Reasonable care must be taken in the siting of computer screens, keyboards, printers or other similar devices. Wherever possible, and depending upon the sensitivity of the data, users should observe the following precautions:

- devices are positioned in such a way that information stored or being processed cannot be viewed by persons not authorised to know the information. Specific consideration should be given to the siting of devices on which confidential or sensitive information is processed or retrieved;
- equipment is sited to avoid environmental damage from causes such as dust & heat;
- users have been instructed to avoid leaving computers logged-on when unattended if unauthorised access to the data held can be gained. Clear written instructions to this effect should be given to users;
- users have been instructed not to leave hard copies of sensitive data unattended on desks.

6.2.2. The same rules apply when accessing the School's ICT System or ICT data away from school, e.g. at a User's home or visiting another school.

6.3. Inventory

6.3.1. The Headteacher, in accordance with the School's Financial Regulations, shall ensure that an inventory of all ICT equipment is maintained and all items accounted for at least annually.

7. Legitimate Use

7.1. The school's ICT facilities must not be used in any way that breaks the law or breaches Council standards.

7.2. Such breaches include, but are not limited to:

- making, distributing or using unlicensed software or data;
- making or sending threatening, offensive, or harassing messages;
- creating, possessing or distributing obscene material;
- Unauthorised personal use of the school's computer facilities.

7.3. Private Hardware & Software

7.3.1. Dangers can occur from the use of unlicensed software and software infected with a computer virus. It is therefore vital that any private software permitted to be used on the school's equipment is acquired from a responsible source and is used strictly in accordance with the terms of the licence. The use of all private hardware for school purposes must be approved and recorded by the ICT Network Manager.

7.4. ICT Security Facilities

7.4.1. The school's ICT systems and data will be protected using appropriate security arrangements outlined in the rest of Section 7. In addition consideration should also be given to including appropriate processing controls such as audit trails, input validation checks, control totals for output, reports on attempted unauthorised access, etc.

7.4.2. For new systems, it is recommended that such facilities be confirmed at the time of installing the system. Information on the range of such facilities can be sought from the School's ICT Services Team.

7.5. Authorisation

7.5.1. Only persons authorised by the ICT Network Manager, are allowed to use the school's ICT systems. Written authorisation outlines the extent to which an ICT User may make use of the ICT System.

7.5.2. Failure to establish the limits of any authorisation may result in the school being unable to use the sanctions of the Computer Misuse Act 1990. Not only will it be difficult to demonstrate that a user has exceeded the authority given, it will also be difficult to show definitively who is authorised to use a computer system.

7.5.3. Where ICT systems are available for use, messages should be displayed to users warning against unauthorised use of the system. This may take the form of warnings displayed by the ICT system itself, the use of wall displays or other display suitable to that environment.

7.5.4. Access eligibility will be reviewed continually, including remote access for support. In particular the relevant access capability will be removed when a person leaves the employment of the school. In addition, access codes, user identification codes and authorisation rules will be reviewed whenever a user changes duties.

7.5.5. Failure to change access eligibility and passwords will leave the ICT systems vulnerable to misuse.

7.6. Passwords

7.6.1. The level of password control will be defined by the ICT Network Manager based on the value and sensitivity of the data involved, including the possible use of “time out” passwords where a terminal/PC is left unused for a defined period.

7.6.2. Passwords for staff users should be changed at least termly and should not be re-used. They should be a minimum of 8 characters, including a mix of letters and numbers.

7.6.3. Passwords should be memorised and not written down.

7.6.4. Passwords or screen saver protection should protect access to all ICT systems. The BIOS (the first code run by a PC when powered on) area of ICT devices should be protected with a password to restrict unauthorised access.

7.6.5. A password must be changed if it is affected by a suspected or actual breach of security or if there is a possibility that such a breach could occur, such as:

- when a password holder leaves the school or is transferred to another post;
- when a password may have become known to a person not entitled to know it.

7.6.6. The need to change one or more passwords will be determined by the risk of the security breach.

7.6.7. Users must not reveal their password to anyone. Users who forget their password must request the ICT Network Manager issue a new password.

7.7. Security of the network

7.7.1. Only devices approved by the Network Manager should be permitted to be connected to the network, either through wired or wireless connectivity.

7.7.2. Where devices are connected to the network using wireless, the wireless network should be secure; as a minimum this should be done using WPA encryption (note that WEP encryption is no longer consider robust). Open Access Wireless Access Points must not be connected to the school’s network. As the school network connects to the Tameside MBC corporate network, Network Managers will be asked to remove unsecured access points where this comes to the attention of Tameside MBC staff due to the risk this poses to the wider corporate network and other schools.

7.7.3. Where encryption is applied to wireless networks, encryption keys should be kept secure and known only to the Network Manager and technical staff. A policy for the regular change of encryption keys should be in place.

7.8. Encryption

7.8.1. As a minimum, all devices of the ICT System that are portable should be fully encrypted to meet the current standards outlined by Becta (see http://www.tamesideschoolssupport.net for further information). Devices subject to encryption may include:

- Laptops
- PDAs
- Smartphones/Blackberries
- USB Pen drives/Memory cards

7.8.2. Where technology prevents the use of encryption (e.g. SD Memory Cards used in Digital Cameras) then all data should not be stored on these devices longer than one day.

7.8.3. When using encryption systems that require a password to access the system, the same guidance for passwords outlined in Section 7.6 applies.

7.9. Filtering of the Internet

7.9.1. Access to the internet for children should be filtered using an approved system. In Tameside MBC all schools connected through the Wide Area Network have their internet filtered using a Becta accredited filtering solution (see http://www.tamesideschoolssupport.net for current details).

7.9.2. It is the responsibility of the ICT Network Manager to monitor the effectiveness of filtering at the school and report issues to Tameside MBC.

7.9.3. Where breaches of internet filtering have occurred, the ICT Network Manager should inform the Headteacher and assess the risk of continued access.

7.10. Backups

7.10.1. In order to ensure that essential services and facilities are restored as quickly as possible following an ICT system failure, back-up copies of stored data will be taken at regular intervals as determined by the ICT Network Manager, dependent upon the importance and quantity of the data concerned.

7.10.2. Where programs and data are held on the Council's systems or other multi-user system, data security and restoration is covered by Tameside MBC procedures.

7.10.3. Data essential for the day to day running and management of the school should be stored on the school's network.

7.10.4. Backups contain data that must be protected and should be clearly marked as to what they are and when they were taken. They should be stored away from the system to which they relate in a restricted access fireproof location, preferably off site.

7.10.5. Instructions for re-installing data or files from backup should be fully documented and security copies should be regularly tested to ensure that they enable the systems/relevant file to be re-loaded in cases of system failure.

7.11. Operating System Patching

7.11.1. The ICT Network Manager will ensure that all machines defined as part of the ICT System are patched up to date according to those releases distributed by the manufacturers of the operating systems. A record should be maintained of all machines running operating systems that can be patched along with each machine's patch status.

7.12. Virus Protection

7.12.1. The school will use appropriate Anti-virus software for all school ICT systems.

7.12.2. All Users should take precautions to avoid malicious software that may destroy or corrupt data.

7.12.3. Teachers who have laptops which are taken away from school and may spend periods of days and/or weeks disconnected from the school's network, must take the necessary steps to ensure anti-virus protection software on their laptop is updated as soon as possible after a period of time off the network. The ICT Network Manager will have a documented procedure to explain this.

7.12.4. The school will ensure that every ICT user is aware that any device in the ICT system (PC, laptops, netbook, PDA, cash till) with a suspected or actual computer virus infection must be disconnected from the network and be reported immediately to the ICT Network Manager who must take appropriate action, including removing the source of infection.

7.12.5. The governing body could be open to a legal action for negligence should a person suffer as a consequence of a computer virus on school equipment.

7.12.6. The school's internet link is provided by Tameside MBC, procured through a 3rd party. The terms of this connection retain a sanction to remove the connection from the whole Tameside estate if significant viral activity is detected by that 3rd party provider. As such, the school will be notified by Tameside MBC if this is where the viral activity arises from. The ICT Network Manager is responsible for the treatment of any virus problems within an agreed period from notification by Tameside MBC. The authority reserves the right to disconnect a school that fails to comply with a notification order to protect the access for all other schools.

7.12.7. Any third-party laptops not normally connected to the school network must be checked by the ICT Network Manager for viruses and anti-virus software before being allowed to connect to the network.

7.12.8. The school will ensure that up-to-date anti-virus signatures are applied to all servers and that they are available for users to apply, or are automatically applied, to PCs or laptops.

7.13. Disposal of Waste

7.13.1. Disposal of waste ICT media such as print-outs, floppy diskettes and magnetic tape will be made with due regard to the sensitivity of the information they contain. For example, paper will be shredded if any confidential information from it could be derived.

7.13.2. The Data Protection Act requires that adequate mechanisms be used when disposing of personal data.

7.14. Disposal of Equipment

7.14.1. The Data Protection Act requires that any personal data held on a part of the ICT system subject to disposal to be destroyed.

7.14.2. Prior to the transfer or disposal of any ICT equipment the ICT Network Manager must ensure that any personal data or software is obliterated from the machine if the recipient organisation is not authorised to receive the data. Where the recipient organisation is authorised to receive the data, they must be made aware of the existence of any personal data to enable the requirements of the Data Protection Act to be met. Normal write-off rules as stated in Financial Regulations apply. Any ICT equipment must be disposed of in accordance with WEEE regulations.

7.14.3. It is important to ensure that any copies of the software remaining on a machine being relinquished are legitimate. Care should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently. The school should maintain a regularly updated asset register of licenses and should indicate when licenses have been transferred from one part of the ICT system to another.

7.15. Repair of Equipment

7.15.1. If a machine, or its permanent storage (usually a disk drive), is required to be repaired by a third party the significance of any data held must be considered. If data is particularly sensitive it must be removed from hard disks and stored on floppy disk or other media for subsequent reinstallation, if possible. The school will ensure that third parties are currently registered under the Data Protection Act as personnel authorised to see data and as such are bound by the same rules as school staff in relation to not divulging the data or making any unauthorised use of it.

8. Security Incidents

8.1. All suspected or actual breaches of ICT security shall be reported to the ICT Network Manager or the Headteacher in their absence, who should ensure a speedy and effective response to be made to an ICT security incident, including securing useable evidence of breaches and evidence of any weakness in existing security arrangements. They must also establish the operational or financial requirements to restore the ICT service quickly.

8.2. The Audit Commission’s Survey of Computer Fraud and Abuse 1990 revealed that over 50% of incidents of ICT misuse are uncovered accidentally. It is, therefore, important that users are given positive encouragement to be vigilant towards any suspicious event relating to ICT use.

8.3. It should be recognised that the school and its officers may be open to a legal action for negligence if a person or organisation should suffer as a consequence of a breach of ICT security within the school where insufficient action had been taken to resolve the breach.

9. ICT Acceptable Use Guide

9.1. The school's ICT Acceptable Use Guide applies to all school staff, students and third parties who use either or both of these facilities. The policy covers the use of email, the Internet, services accessed through the Internet and local file and network usage. The conditions of use are explained in the policy. All school staff accessing these facilities must be issued with a copy of the 'ICT Acceptable Use Guide' and other relevant documents and complete the user declaration attached to the policy. For all students, the school will ensure that the relevant 'ICT Acceptable Use Guide' document is issued and the consent form is completed by pupils and their parents. In addition, copies of the 'ICT Acceptable Use Guide' document and consent form will be issued to all visitors.

10. Personal Use

10.1. The School has devoted time and effort into developing the ICT Systems to assist you with your work. It is, however, recognised that there are times when you may want to use the Systems for non-work related purposes, and in recognising this need the School permits you to use the Systems for personal use.

10.2. You must not use the systems for personal use during working hours. You must not allow personal use of systems to interfere with your day to day duties. Any non-job related use of the systems during working hours may be subject to disciplinary action.

10.3. You must not use School software for personal use unless the terms of the licence permit this and you are responsible for checking the licensing position. Microsoft Office and Internet Explorer are licensed for personal use.

10.4. Use of the systems should at all times be strictly in accordance with the provisions of paragraph 9.1 above. You must pay all costs associated with personal use at the School's current rates e.g. cost of paper.

10.5. You are responsible for any non-business related file which is stored on your computer.

10.6. When accessing the internet for non-work purposes you may only view web pages and download .pdf files.

11. Disciplinary Implications

11.1. Breaches of this policy may result in disciplinary action up to and including dismissal. They may also result in you being prosecuted under the Computer Misuse Act 1990, and may lead to prosecution of the School and the individual(s) concerned and/or civil claims for damages.

12. Appendix - Legal issues relevant to the use of ICT and communications equipment

This section is designed to inform users of potential legal issues relevant to the use of electronic communications. It is not professional advice.

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and changes occur frequently.

Criminal Justice Act 2003

Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Sexual Offences Act 2003

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as “Sexting”). **A person convicted of such an offence may face up to 10 years in prison.**

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.
It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff etc. fall in this category of trust).
Any sexual intercourse with a child under the age of 13 commits the offence of rape.
N.B. Schools should already have a copy of “Children & Families: Safer from Sexual Crime” document as part of their child protection packs.
More information about the 2003 Act can be found at www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment.
This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Data Protection Act 1998

The Act requires anyone who handles personal information to notify the Information

Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1 — 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to:

Gain access to computer files or software without permission (for example using someone else's password to access files);
Gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
Impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using his or her "work" without permission.

The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.
It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 — 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act
2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Regulation of Investigatory Powers Act 2000
The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications)
Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Criminal Justice and Immigration Act 2008
Section 63 offence to possess "extreme pornographic image"
63 (6) must be "grossly offensive, disgusting or otherwise obscene"
63 (7) this includes images of "threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead" must also be "explicit and realistic".
Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006

Education and Inspections Act 2006 outlines legal powers for schools which relate to Cyberbullying/Bullying:

Headteachers have the power “to such an extent as is reasonable” to regulate the conduct of pupils off site. School staff are able to confiscate items such as mobile phones etc. when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying policy

Telecommunications Act 1984

The transmission of an obscene or indecent image from one computer to another via a ‘public telecommunications system’ is an offence under section 43 of this Act. For traditional mail, the same sort of offence is created under the Post Office Act 1953.