HIGHGATE WOOD SCHOOL
arts college

E-Safety Policy
2014

Background / Rationale

The internet and other digital and information technologies are powerful tools and provide many opportunities for teaching and learning. They help teachers, students, parents, carers and the wider school community collaborate together and communicate with each other. They can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Moreover, these technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. However, despite the clear benefits of communicational technologies, they also present risks. These dangers include:

- Access to illegal, harmful or inappropriate text, images, video and other on-line content.
- Unauthorised access to/loss of/sharing of personal information and the risk of "identity theft"
- Inappropriate communication / contact with others, including strangers and the risk of being subject to grooming by on-line predators.
- Cyber-bullying
- Failure to properly evaluate the quality, accuracy and relevance of information found on-line.
- Plagiarism and copyright infringement, including the illegal downloading of music, video and program files.
- The risks presented by viruses and malware.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Whilst it is possible to guard against some of these risks through the use of safeguards, including specialist software and through systems for filtering and monitoring, it is impossible to eliminate these risks completely. It is therefore essential, through good educational provision, to build resilience to the dangers to which users of new technologies may be exposed, so that they have the confidence and skills to face and deal with the risks that currently present themselves and the new risks that the constant development of digital technologies inevitably bring.

This e-safety policy will demonstrate how the school provides the safeguard manage and reduce e-safety risks, while also addressing wider educational issues in order to help young people (and their parents / carers) and their teachers to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by a working group made up of: the school's head of e-learning, teachers, support staff, admin staff, governors, parents and carers, students

Consultation with the whole school community has taken place through the following: Staff meetings, School Council, governors meeting, parents evening, school website / newsletters

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the Governing Body on:

11 February, 2014

The implementation of this e-safety policy will be monitored by the:

E-Safety Officer

Monitoring will take place at regular intervals:

Annually

The Governing Body / Governors Sub Committee will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:

Annually

The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:

Spring, 2015

Should serious e-safety incidents take place, the following external persons / agencies should be informed:

E-Safety Officer

The school will monitor the impact of the policy using:

Logs of reported incidents

Internal monitoring data for network activity:

Surveys / questionnaires of students, parents\carers and staff

Scope of the Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

The e-safety policy also includes consideration of all relevant legislation including legislation connected to Data Protection, Freedom of Information, Copyright and Piracy and Computer Misuse.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor

The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Officer
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors' committee.

Headteacher and Senior Leadership Team:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Officer.
- The Headteacher is responsible for ensuring that the E-Safety Officer and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Officer.
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. [1]

E-Safety Officer:

- leads the e-safety committee
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.

[1] See flow chart included in this policy

- provides training and advice for staff
- liaises with the Local Authority
- liaises with Managed Service Provider
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

The Managed Service Provider

The Managed Service Provider is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack[2]
- that the school meets the e-safety technical requirements outlined in the school's policy documents.
- that users may only access the school's networks through a properly enforced password protection policy
- that the use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Officer
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- have appropriate safeguards when accessing, saving, moving and using data that may be considered sensitive or personal.
- they have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the E-Safety Officer for investigation / action / sanction
- digital communications with students should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities

[2] In association with facilities provided by LGfL filtering and anti-virus provisioning

- students understand and follow the school e-safety and acceptable use policy
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Designated Child Protection Officers

Child Protection officers should be aware of the potential for serious child protection issues arising from:

- sharing and posting of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

E-Safety Committee

Members of the E-safety committee will assist the E-Safety Coordinator / Officer (or other relevant person, as above) with:

- the production / review / monitoring of the school e-safety policy / documents.

Students:

- are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to school systems
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters and a dedicated area of the school website. Parents and carers will be responsible for:

- endorsing (by signature) the Student Acceptable Use Policy

Community\Guest Users

Community and Guest users who access the school ICT systems will be expected to sign a Guest User AUP before being provided with access to school systems.

Policy Statements

Education – students / pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned e-safety programme is provided as part of the ICT curriculum at Key Stage 3 and registration sessions at Key Stage 4 and is regularly revisited – this covers both the use of ICT and new technologies in school and outside school
- Key e-safety messages are reinforced as part of a planned programme of assemblies and presentations
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students should be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems are displayed on log-on screens
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

- Relevant information in Insight magazine
- Through the school website e-safety pages – including helpsheets, publications and updates of key e-safety issues and advice.
- Parent information evenings

Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Officer will provide advice / guidance / training as required to individuals as required.

Training – Governors

Governors will be invited to take part in e-safety training/awareness sessions.

This may be offered in a number of ways:

- Attendance at training provided by the Local Authority , the National Governors Association and or other relevant organisation.
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

The school, the Local Authority and the Managed Service Provider will work together to ensure:

- The school ICT systems is managed in ways that ensure that the school meets the e-safety technical requirements outlined in the Acceptable Usage Policy and any relevant Local Authority\School E-Safety Policy and guidance.
- The system of Unified Sign On from LGfL that allows users access to the school network, school email and the MLE is correctly and effectively used, so that users are able to logon to the network, school email and the MLE with their own (unified) username and password that is linked to their status in the MIS (Sims.net).
- Users have clearly defined access rights to school ICT systems, including remote access. Details of the network access rights available to groups of staff users will be recorded in the permissions grid.
- The WebScreen filtering service provided by LGfL is appropriately set up and managed to provide filtering for all internet access, including access through personal devices connected to the school's wireless network. The enhanced filtering service provided by RM's SmartCache is in place for all access through equipment connected to the CC4 network. Any changes or alterations to the filtered list are monitored and available for review.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Servers, wireless systems and cabling are securely located and physical access restricted and appropriate security measures are in place (schools may wish to provide more detail) to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data
- An agreed process is in place for the provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system.
- An agreed process is in place for the installation on the network of executable files and computer programs, for the saving of media files and other copyright material, and for the storage of files and other material on users' home drives and shared network drives.

- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see School Personal Data Policy Template in the appendix for further detail)
- The school infrastructure and individual workstations are protected by up to date virus software and that there is an appropriate and comprehensive back-up routine, with safe storage of back-up tapes and a disaster recovery plan.

Curriculum

General

E-safety should be embedded in all areas of the curriculum and staff should reinforce e-safety messages wherever possible.

- Students should be taught in all lessons to be critically aware of the materials / content they access on-line (and elsewhere) and be guided to validate the accuracy of information
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet (and elsewhere).

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

Staff should inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.[3]
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs that include students intended for publication (on a website, or elsewhere) should be selected carefully and will comply with good practice guidance on the use of such images. Students' full names must not be associated with their image when published on-line.

[3] See agreement on use of pictures

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

In accordance with these requirements and the school's Data Protection policy staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Take particular care when transferring data between devices, moving data from the network or accessing the network remotely that they have taken appropriate precautions (including using data encryption) to maintain the security of that data.

Communications

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users need to be aware that email communications may be monitored
- Users should immediately report, to a teacher (if a student) or their line manager or e-safety officer, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents / must be professional in tone and content. These communications may only

take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.

- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

Unsuitable / inappropriate activities

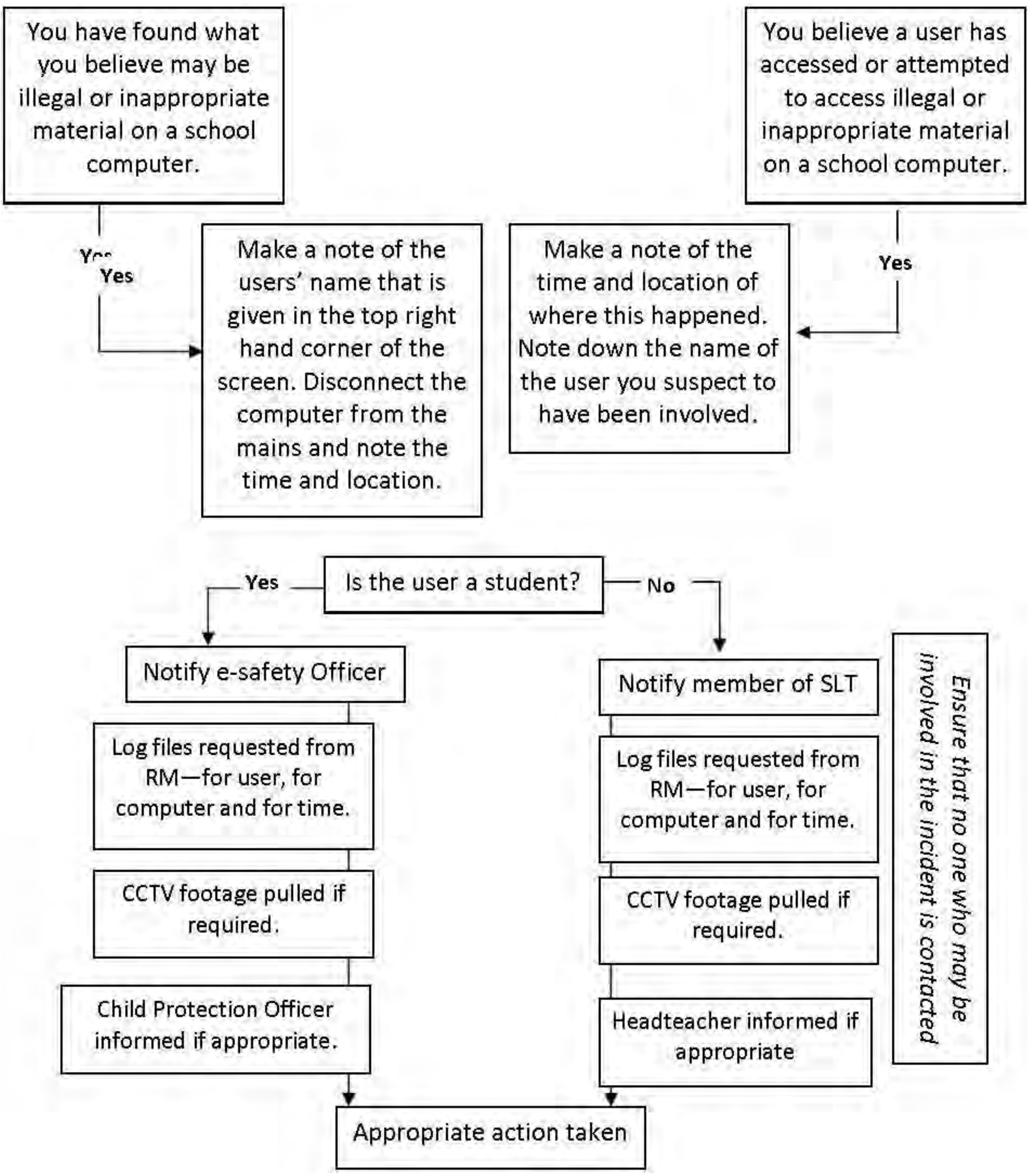
Some internet activity, eg accessing material that is illegal, would obviously be banned from school and all other ICT systems. Other activities eg Cyber-bullying could lead to criminal prosecution and would also be banned as a matter of course. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to below are inappropriate in a school context and that users should not engage in these activities in school or outside school when using school equipment or systems except with the expressed permission of the Headteacher.

- Use of school systems to run a private business
- Creating of propagating viruses or malware
- Engaging in hacking or attempting to breach computer security settings
- Non-educational on-line gaming
- On-line gambling
- On-line trading
- File sharing that is in breach, or risks being in breach, of copyright and licensing agreements.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. In these instance the processes outline in the flow chart below should be followed.


You have found what you believe may be illegal or inappropriate material on a school computer.
Yes
Make a note of the users' name that is given in the top right hand corner of the screen. Disconnect the computer from the mains and note the time and location.
You believe a user has accessed or attempted to access illegal or inappropriate material on a school computer.
Yes
Make a note of the time and location of where this happened. Note down the name of the user you suspect to have been involved.
Is the user a student?
Yes
No
Notify e-safety Officer
Log files requested from RM—for user, for computer and for time.
CCTV footage pulled if required.
Child Protection Officer informed if appropriate.
Notify member of SLT
Log files requested from RM—for user, for computer and for time.
CCTV footage pulled if required.
Headteacher informed if appropriate
Ensure that no one who may be involved in the incident is contacted
Appropriate action taken

Appendix 1

Legal Framework

Below is a listing of the legislative framework under which this E-Safety Policy has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

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.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

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.

Protection of Children Act 1978

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 a 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). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

The new grooming offence 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 fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

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. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.