The Thomas Hardye School

A Policy for E-Safety in School

May 2013

Content

Background

New 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.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development/Monitoring/Review

This e-safety policy has been developed by:

- SDP for Child Protection
- Headteacher
- Management team
- SW Grid for Learning

Consultation with the whole school community has taken place through the following:

- School Staff: meetings
- Students: Student Voice
- Governors: meetings

- Parents and Carers: School website /newsletters
- Logs-of reported incidents
- SWGfl, logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of
- Students
- Parents / carers
- Staff

Schedule

This e-safety policy was approved by the Governing Body/Governors Sub-Committee on:	
The implementation of this e-safety policy will be monitored by the :	Management Team
Monitoring will take place at regular intervals:	Termly
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:	Once a year
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:	June 2014
Should serious e-safety incidents take place, the following external persons/agencies should be informed:	LA IC Manager, LA Safeguarding Officer, Police Commissioner's Office

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.

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 receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety as part of being the Safeguarding Governor. The role of the E-Safety Governor will include:

- regular meetings with the SDP
- to monitor e-safety incident logs
- to monitor filtering / change control logs
- reporting to Governors Education committee

Senior Management 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 SDPs for Child Protection and ICT manager
- The Senior Management team are responsible for ensuring that relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Senior Management team 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 Management Team will receive regular monitoring reports from the relevant staff
- The Headteacher and another member of the Senior Management 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.

E-Safety Coordinators:

- SDPs for Child Protection and ICT Manager
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT technical staff
- receives reports of e-safety incidents and creates a log of serious 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 Governors meetings
- reports regularly to Senior Management Team

ICT Manager

The Network Manager is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements outlined in the SWGfL Security Police and Acceptable Usage Policy and any relevant local Authority E-Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- SWGfL informed of issues relating to the filtering applied by the Grid
- that he keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator /

Headteacher / ICT Co-ordinator / Year Coordinator for investigation / action
- that any student misuse is logged on the students' network file
- that monitoring software / systems are implemented and updated as agreed in school policies

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
- they have read, understood and signed the school Staff Acceptable Use Policy
- they report any suspected misuse or problem to the E-Safety Co-ordinator
- digital communications with students (email / Virtual Learning Environment (VLE) should be on a professional level and only earned out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- 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
- they monitor ICT activity in lessons, extra-curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devises and that they monitor their use and implement current school policies with regard to these devises

Designated person for child protection

Is responsible for monitoring the potential for serious child protection issues to arise from:

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

Students:

- are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy (in student diaries), which they will be expected to sign before being given access to school systems.
- Follow the guidance on staying E-safe from students' diaries
- 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

Parent/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, website / VLE and information about national / local e-safety campaigns.

Parents and carers will be responsible for:
- endorsing (by signature) the Student Acceptable Use Policy
- accessing the school website/VLE/TH Direct student records in accordance with the school AUP

Policy Statements Education-students

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 will be provided as part of ICT / PHSE / other lessons and will be regularly revisited - this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages will be reinforced as part of pastoral activities
- 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 will 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 / internet will be posted in all rooms
- 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:

Letters, newsletters, web site, VLE
Parents evenings
The DASP Website
Reference to the SWGfL Safe website (nb the SWGfL "Golden Rules" for parents)

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:

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- The E-Safety Coordinator will receive regular updates through SWGfL / LA)
- This E-Safety policy and its updates will be presented to and discussed by staff in team meetings
- The E-Safety Coordinator will provide advice / guidance / training as required to individuals as required

Technical —infastructure /equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the ICT Manager and will be reviewed annually
- All users will be provided with a username and password by the ICT manager who will keep an up to date record of users and their usernames. Users will be required to change their password regularly.
- The "administrator" passwords for the school ICT system, used by the ICT Manager must also be

available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe)

- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by SWGfL In the event of the ICT Manager needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).
- Any filtering issues should be reported immediately to SWGfL.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- An appropriate system is in place for users to report any actual / potential e-safety incident to the Network Manager (or other relevant person).
- Appropriate security measures are in place 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 policy is in place for the provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system.
- An agreed policy is in place regarding the extent of personal use that users (staff/students/pupils/ community users) and their family members are allowed on laptops and other portable devices that may be used out of school.
- An agreed policy is in place that allows staff to /forbids staff from installing programmes on school workstations / portable devices.
- The school infrastructure and individual workstations are protected by up to date virus software.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- in lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- 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.
- 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 taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students / pupils 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. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will 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. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- 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 published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photos.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website
- Student's work can only be published with the permission of the student and parents or carers

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.

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 deuces, ensuring that they are properly "logged-off at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

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
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person - in accordance with the school policy, 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 / carers (email, VLE etc) must be professional in tone and content. These communications may only take place on official 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

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User Actions		Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images		X
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation		X
	adult material that potentially breaches the Obscene Publications Act in the UK		X
	criminally racist material in UK		X
	pornography	X	
	promotion of any kind of discrimination	X	
	promotion of racial or religious hatred	X	
	threatening behaviour, including promotion of physical violence or mental harm	X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute	X	
Using school systems to run a private business		X	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfLand/or the school		X	
Uploading, downloading or transmitting commercial software or any copy righted materials belonging to third parties, without the necessary licensing permissions		X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer/ network access codes and passwords)		X	
Creating or propagating computer viruses or other harmful files		X	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet		X	
On-line gambling		X	
Use of social networking sites		X	

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.

An inappropriate website is accessed unintentionally by student/staff:

1. Play the situation down; don't make it into a drama.
2. Report to the headteacher/ e-safety Co-ordinator and decide whether to inform parents of any students who viewed the site.
3. Inform the ICT support team and who will ensure the site is filtered
4. ICT support team should contact SWGfL

An inappropriate website is accessed intentionally by a student:

1. Refer to the acceptable use policy that was signed by the student, and apply agreed sanctions.

2. Notify the parents/carer of the student.
3. Inform the ICT support team who will ensure the site is filtered if need be.
4. ICT support team should contact SWGfL

An adult uses an organisation's ICT equipment inappropriately.

1. Ensure you have a colleague with you; do not view the misuse alone.
2. Report the misuse immediately to the headteacher/ e-safety Co-ordinator and ensure that there is no further access to the PC/ laptop.
3. If the material is offensive but not illegal, the headteacher/ e-safety Co-ordinator should then:

    - Remove the PC to a secure place.
    - Complete an e-safety serious incident log
    - Instigate an audit of all ICT equipment by the ICT support team to ensure there is no risk of others accessing inappropriate materials.
    - Identify the precise details of the material.
    - Take appropriate disciplinary action (contact Personnel/Human Resources).

4. In an extreme case where the material is of an illegal nature:
    - Remove the PC to a secure place
    - Complete an e-safety serious incident log
    - Contact the local police and follow their advice.

A bullying incident directed at a student occurs through email or mobile phone technology.

1. Advise the student not to respond to the message.
2. Refer to the Year Co-ordinator who will and apply appropriate sanctions (referring to TH policies including e-safety)
3. Secure and preserve any evidence.
4. Inform the sender's email service provider.
5. Notify parents/carers of the students involved.
6. Consider delivering a parent/carer workshop for the community.
7. Inform the police if necessary.
8.

Malicious or threatening comments are posted on an internet site about a student or member of staff.

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Inform the e-safety Co-ordinator. Endeavour to trace the origin and inform police as appropriate.

You are concerned that a child's safety is at risk because you suspect someone is us ing communication technologies (such as social networking sites) to make inappropriate contact with the child.

1. Report to and discuss with the SDP for child protection and contact parents/carers.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP (Child Exploitation and Online Protection Centre): www.ceop.gov.uk
4. Consider the involvement of police and Children's Services.

Appendices

Can be found on the following pages:

THE THOMAS HARDYE SCHOOL

ICT Acceptable Use Policy for Students

Introduction

The following document is divided into three sections as follows:

1. The SMART Rules.
2. The Quick Guide.
3. Full Policy Document.

1. SMART Rules

S Safe - Keep safe by being careful not to give out personal information, such as your full name, email address, telephone number, home address, photos or school name, to people you have only had contact with online. Set strong privacy settings on social networking sites

M Meeting: Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or guardians' permission and even then only when they can be present.

A Accepting: Accepting emails, instant messages, or opening files, pictures or texts from people you don't know or trust can lead to problems; they may contain viruses or nasty messages!

R Reliable: Information you find on the Internet may not be true, or someone online may be lying about who they are.

T Tell: Tell your parents, guardian or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

You can report online abuse to the police at: www.thinkyouknow.co.uk and you can report anything you are not happy about to anyone you feel you trust. This could be a teacher, guardian, parent or someone else's parent. Tell someone.

2. The Quick Guide: Student Use of Computers and Mobile Devices

-You may only log on as yourself. Do not give your password to anyone else.
- Be aware that the School can check your computer files and which sites you visit at any time.
- Do not use bad language, bully or try to access inappropriate material on line.
- iPods, mobile telephones and/or other mobile devices must be switched off and out of sight during lessons and whilst on the school premises unless permission has been given by a teacher to use them.
- You are not to record, video or photograph anything during lessons unless the teacher requests that you do so.
- You must not wear earphones when walking around the site at any time.
- Do not attempt to bypass school web filters.
- Do not give out your personal details online and never arrange to meet a stranger.
- Respect copyright and do not plagiarise work.

Any breach of this policy will result in appropriate disciplinary action.

3. Student Computer Acceptable Use Policy

The use of the latest technology is actively encouraged at Thomas Hardye School but with this comes a responsibility to protect students, staff and the School from abuse of the system.

All students, therefore, must adhere to the Policy set out below. This Policy covers all workstations, laptops, mobile telephones and other electronic devices within the School, irrespective of who is the owner.

All students are expected to behave responsibly on the School computer network, as they would in classrooms and in other areas of the School.

i) Personal Safety

-Always be extremely cautious about revealing personal details and never reveal a home address, telephone number or email address to strangers.
-Always inform your teacher or another adult if you have received a message or have visited a website that contains inappropriate language or makes you feel uncomfortable in any way.
-Do not play with or remove any cables that are attached to a School computer.
-Always be yourself and do not pretend to be anyone or anything that you are not on the Internet.
-Do not arrange to meet anyone you have met on the Internet; people are not always who they say they are.
-If in doubt, ask a teacher or another member of staff.

2. System Security

-Do not attempt to go beyond your authorised access. This includes attempting to log on as another person, sending e-mails whilst masquerading as another person or accessing another person's files. Attempting to log on as staff is unacceptable and may result in the loss of access to systems and other serious sanctions. You are only permitted to log on as yourself.
-Do not give out your password to any other student; if you do and they do something wrong logged on as you, you will be held responsible. If you suspect someone else knows your password, change it immediately. This password should be changed at least once a term and be at least 6 characters long.
-Do not alter School hardware in any way.
-Do not eat or drink whilst using the computer.

3. Inappropriate Behaviour

'Inappropriate Behaviour' relates to any electronic communication whether email, blogging, tweeting, social networking, texting, journal entries or any other type of posting/uploading to the Internet.

-Do not use indecent, obscene, offensive or threatening language.
-Do not post or send information that could cause damage or disruption.
-Do not engage in personal, prejudicial or discriminatory attacks.
-Do not harass another person. 'Harassment' is persistently acting in a manner that distresses or annoys another person.
-Do not knowingly or recklessly send or post false, defamatory or malicious information about a person.
-Do not post or send private information about another person without their prior agreement.
-Bullying of another person either by email, online or via texts will be treated with the highest
-Do not access, or post, material that is profane or obscene, or that encourages illegal acts, violence or discrimination towards other people.
-If you mistakenly access such material, please inform your teacher or another member of staff immediately or you may be held responsible.
-Do not attempt to use proxy sites on the Internet.
-Do not take or post a photo of another student or member of staff without their permission.

4. Email

-You should check your School email at least once a day during term time for new messages.
-Do not reply to spam mails as this will result in more spam. Delete them and inform the IT support office.
-Do not open an attachment from an unknown source. Inform the IT support office as it might contain a virus.
-All emails sent from the School reflect on the School name so please maintain the highest standards.
-Do not use email (including web mail) during lessons unless your teacher has given permission.
-Do not send any files above 10mb by mail. Please ask the IT support office if you require this temporarily to be lifted.
-Do not send or forward annoying or unnecessary messages to a large number of people, e.g. spam or chainmail.
-Do not join mailing lists without the prior permission of IT support.

5. Plagiarism and Copyright

-Plagiarism is taking the ideas or writings of others and presenting them as your own. Do not plagiarise works that you find on the Internet or anywhere else.
-You should respect copyright. Breaking copyright law occurs when you reproduce a piece of work. You should request permission from the copyright owner. This includes music files and the copying of CDs, downloading of films from illegal sites and other such formats.

6. Privacy

-All files and emails on the system are the property of the School. As such, system administrators and staff have the right to access them if required.
-Do not assume that any email sent on the Internet is secure.
-All network access, web browsing and mails on the School system are logged.
-If you are suspected of breaking this Policy, your own personal laptop/device and mobile telephone can be searched by staff.
-The School reserves the right to randomly search the Internet for inappropriate material posted by students and to act upon it.

7. Software

-Do not install any software on the School system.
-Do not attempt to download programmes from the Internet onto School computers.
-Do not knowingly install spyware or any sort of hacking software or device.

8. Sanctions

-Sanctions will vary depending on the severity of the offence; they will range from a warning or withdrawal of Internet use, to suspension or expulsion.
-A breach of the law may lead to the involvement of the police.

9. General and Best Practice

-Think before you print; printing is expensive and consumes resources which is bad for the environment.
-Priority must be given to students wishing to use the computers for School use.
-Always log off your computer when you have finished using it. Do not lock the computer so that others cannot use it.
-Always back up your work if you are not saving it on the School system. Work saved on the School system is backed up every night for you, but be careful if you only have a copy of your work on a memory stick.
-Avoid saving or printing sizeable files (eg. above 5mb); if in doubt ask a member of IT support.
-Passwords should be alpha numeric, ie. contain both letters and numbers.

-Observe Health and Safety Guidelines; look away from the screen every 10 minutes to rest your eyes and make sure your chair is positioned and adjusted to the correct height to the desk.
-Housekeep your email regularly by deleting old mail.
-If a web page is blocked that you feel you have a legitimate use for, please ask IT support and it can instantly be unblocked if approval is given.
-If you are leaving the School, please ensure you have saved any files or email you wish to keep to a
memory stick or CD to take home, as these files will be deleted.
-If in doubt, ask a member of the IT support office.

10. Mobile Phones / Mobile Devices

-Do not use a mobile telephone or other mobile device during lessons unless you have the teacher's permission.
-Mobile telephones should be switched off and kept out of sight while you are on the school premises unless you have the permission of a teacher.
-Do not take photos or videos with any device during lessons unless the member of staff has given permission.
-Do not take photos of people without their permission.
-Bullying by text or any other method will be treated in the same severe manner as any other form of bullying.
-Do not attempt to hack into someone else's device via Bluetooth or any other method.

11. Music/Video Players (eg, iPods)

-The use of such devices is banned during lessons unless the teacher has given permission.
-Do not connect such a device to the School network/School computers.
-Do not break copyright laws by swapping illegal music/video files.

✂.....

Please return to Dr T Ennion, Assistant Headteacher

ICT Acceptable Use Policy for Students

I have read and understood and agree to comply with the Student ICT Acceptable Use Policy.

Student Name:.....College:.....Tutor Group:.....

Student Signature:..... Date:.....

Parent/Guardian Name:.....

Parent/Guardian Signature:.....Date:.....

Thomas Hardye School
Frog Acceptable Use Policy

The school uses the Frog learning platform to support teaching and learning. In addition to the ICT acceptable use policy, students should comply with the following code of conduct when using Frog:

- Frog is for Learning. All activities undertaken on Frog must conform to this expectation.
- Usernames and passwords must be suitably complex and not shared with any other user.
- Keep your password private – if you think someone else knows it, get it changed. IT support will help you change it.
- Do not enter Frog using anyone else's details
- Consider the long-term implications of any content posted or saved on Frog (or anywhere on line).
- Discussion forum contributions should be in support of learning and not defamatory or use inappropriate language in any form. Teachers, support staff and members of the Frog Student Voice will monitor discussion forums.
- Do not upload or post inappropriate, offensive or illegal content to Frog or other online spaces – there are no private areas on Frog.
- Student activity on Frog outside of normal school hours is subject to all of the guidance contained in this acceptable use policy and will also be monitored in the same way as activity during school hours.

Sanctions
Failure to comply with the terms of this Acceptable Use Policy may result in disciplinary action. This can include written warnings, withdrawal of access privileges, detentions and, in extreme cases, temporary or permanent exclusion from the school. The school also reserves the right to report any illegal activities to the appropriate authorities.

Thomas Hardye School

ICT Acceptable Use Policy for Staff

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

☐ I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites**.**

☐ School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

☐ I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

☐ I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with eight or more characters, does not contain a dictionary word and is only used on one system).

☐ I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

☐ I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely. *Staff should not carry personal, sensitive or confidential information on data sticks or laptop hard drives (for example, sensitive data on students, staff or parents, from SIMS). When off-site, such data should only be accessed using the secure VMWare remote desktops.* Any images or videos of students will only be used as stated in the school image use policy and will always take into account parental consent.

☐ I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones). Where possible I will use the School Learning Platform or VMWare remote desktops to access sensitive information when off the school site (see above). I will protect the devices in my care from unapproved access or theft.

☐ I will avoid printing sensitive information on students, staff or parents unless absolutely necessary, and then only using a printer located in a staff base.

☐ I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

☐ I will respect copyright and intellectual property rights.

☐ I have read and understood the school e-Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

☐ I will report all incidents of concern regarding children's online safety to the Designated Child Protection Coordinator (Kaye Chittenden) and/or the e-Safety Coordinator (Tim Ennion) as soon as possible.

☐ I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to Tim Ennion, the e-Safety Coordinator, as soon as possible.

☐ I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the ICT Support Team as soon as possible.

☐ My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.

☐ My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.

☐ I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role or the school into disrepute.

☐I will promote e-Safety with the students in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

☐ If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the e-Safety Coordinator (Tim Ennion) or the Head Teacher.

☐ I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the school's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff ICT Acceptable Use Policy.

Signed: ……..... Print Name: …… Date: ……

Accepted by: …….. Print Name: ……..…….

Thomas Hardye School

Online Safety – Guidance and Protocols for Teachers and Support Staff

Web 2.0 has created many new methods of instant communication which allow great opportunities for educators both in and out of the school environment. Social networking sites such as Facebook and Twitter provide opportunities for teachers to link online with like-minded people sharing ideas and information, as well as providing another forum for communication with students.

It must be remembered that online communication is often informal. It lacks the non-verbal clues of face-to-face conversations and it is without the formal protocols of traditional written communication. It is therefore easy to respond and publish before the time has been taken to consider fully the implications of that communication.

Those working in schools should be aware that publication of private and personal information in any online forum cannot be controlled, nor can the use of that information be monitored. Information you publish may be altered, copied and republished on other sites and in other formats. Injudicious publication of personal information can provide opportunities for dishonest or opportunistic individuals to manipulate information without the knowledge of the author.

It is also important to be aware that some people may associate your online activity with your school or with your post in school. Employment disputes involving the use or misuse of the internet are becoming more common. Potential employers are known to check candidates by entering their names into search engines.

In the light of these statements the following guidance should be considered:

1. Remember that activities online can affect your life offline.
2. Take great care when commenting upon school activities in any online forum; if in any doubt check with a senior member of staff before publishing.

Social Networking Sites

3. Do not post in any forum, information or photographs which you would not feel comfortable sharing with a stranger. Do not post anything which could be embarrassing.
4. If using a networking site, ensure that you know and use the security/privacy controls. Do not allow anyone other than close friends, access to personal information.
5. If you wish to use a networking site for communication with students, set one up specifically for this purpose. Be clear about your reasons and goals for doing so.
6. Use a neutral picture of yourself as your profile image.
7. Protect the privacy of friends, family and colleagues in the same way you safeguard your own personal information.
8. Be careful about accepting “friends” if you do not know enough about them.

Email

9. Although there are no protocols for emails, maintain an acceptable formality for the work place.
10. If using email for communication with students or parents, only use the school email and not your personal address. Where possible send emails to the student’s school address.
11. Consider using messaging or forum facilities on Frog as an alternative to an email conversation.
12. If you receive emails which you consider to be inappropriate, keep a copy and if necessary share it with your line manager or Headteacher.
13. Remember that emails may be requested as part of records held on a student.

The Thomas Hardye School Acceptable Use of Digital Images

The use of digital / video images plays an important part in learning activities. Students / Pupils and members of staff may use school digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons. Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names. Parents are requested to sign the permission form below to allow the school to take and use images of their children.

Permission Form

Parent/Guardian Name: ……

Student Name: ……

As the parent/ carer of the above student, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at, or of, - school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Signed:……Date:……

The Thomas Hardye School
Filtering Policy

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school. As a part of the South West Grid for Learning (SWGfL) schools and connected organisations automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the ICT Manager.

They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems. To ensure that there is a system of checks and balances and to protect those responsible, changes to the SWGfL/school filtering service must be reported to a second responsible person: Senior Link Manager

All users have a responsibility to report immediately to the ICT Manager any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.
Education/Training /Awareness

Students will be made aware of the importance of filtering systems through ICT lessons. They will also be warned of the consequences of attempting to subvert the filtering system. Staff users will be made aware of the filtering systems through: signing the AUP
Parents will be informed of the school's filtering policy through the Acceptable Use agreement and through e-safety awareness sessions / newsletter etc.

Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the ICT Manager who will decide whether to make school level changes. (If it is felt that the site should be filtered (or unfiltered) at SWGfL level, SWGfL should be emailed at filterina@swafl.org.uk with the URL.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School E-Safety Policy and the Acceptable Use agreement.

Audit/Reporting Logs of filtering change controls and of filtering incidents will be made available to:

- the Senior Link Manager
- E Safety Coordinators

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

The Thomas Hardye School
Password Security Policy

Introduction

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system

A safe and secure usemame / password system is essential if the above is to be established and will apply to all school ICT systems, including email and Virtual Learning Environment (VLE).

Responsibilities

The management of the password security policy will be the responsibility of the ICT Manager
All users (adults and students) will have responsibility for the security of their usemame and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Awareness

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's e-safety policy and password security policy
- through the Acceptable Use Agreement

Students will be made aware of the school's password policy:

- in ICT lessons
- through the Acceptable Use Agreement
-

Policy Statements

All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the ICT Manager.

All users will be provided with a usemame and password by the ICT Manager.

The following rules apply to the use of passwords:

- the password should be a minimum of 6 characters
- the account should be "locked out" following six successive incorrect log-on attempts
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
-

The "administrator" passwords for the school ICT system, used by the ICT Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe).

Thomas Hardye School E-Safety
Serious Incident Log

Date	
Name of perpetrator(s)	
Position	Student Staff
Reason for Investigation	

	Primary Investigating Witness	Secondary Investigating Witness (if applicable)
Name		
Position		
Signature		

Name and location of computer used for investigation

Website(s) address	Reason why content is causing concern

Action proposed or taken

Thomas Hardye School
E-Safety Charter

Name of School:
Name of Local Authority:

We are working with staff, pupils and parents/ carers to create a school community which values the use of new technologies in enhancing learning, encourages responsible use of ICT, and follows agreed policies to minimise potential e-safety risks.

Our School Community

Discusses, monitors and reviews our e-safety policy on a regular basis. Good practice suggests the policy should be reviewed annually or at most every two years.

Supports staff in the use of ICT as an essential tool for enhancing learning and in the embedding of e-safety across the whole school curriculum.

Ensures that pupils are aware, through e-safety education, of the potential e-safety risks associated with the use of ICT and mobile technologies, that all e-safety concerns will be dealt with sensitively and effectively; that pupils feel able and safe to report incidents; and that pupils abide by the school's e-safety policy.

Provides opportunities for parents/carers to receive e-safety education and information, to enable them to support their children in developing good e-safety behaviour. The school will report back to parents / carers regarding e-safety concerns. Parents/carers in turn work with the school to uphold the e-safety policy.

Seeks to learn from e-safety good practice elsewhere and utilises the support of the LA SWGfL and relevant organisations when appropriate.

Chair of Governors: ……
Headteacher ……
Student Representative: ……..

Legislation

Schools should be aware of the legislative framework under which this E-Safety Policy template and guidance 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.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

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.

Computer Misuse Act 1990

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 Harrassment 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 OffencesAct2003

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 orwebcams, 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 fell 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.

Useful Links

DASP Website
http://www.dasp.org.uk
SWGFL
http://www.swgfl.org.uk/
British Education and Communication Training Agency
http://schools.becta.org.uk/index.php?section=is
CBBC
http://www.bbc.co.uk/cbbc/help/safesurfing/
Child Exploitation and Online Protection Centre
http://www.ceop.gov.uk/
THINKUKNOW
http://www.thinkuknow.co.uk/
The DCSF have now produced Resources for e-safety in Secondary schools at:
http://www.nationalstrategiescpd.org.uk/course/view.php?id=244