

# **SCARISBRICK HALL SCHOOL**

## **E-SAFETY AND ACCEPTABLE ICT USE POLICY**



### **Rationale**

ICT in the 21<sup>st</sup> Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the every day lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

ICT covers a wide range of resources including: web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children are using both inside and outside the classroom include:

- websites;
- VLEs;
- email and Instant messaging;
- chat rooms and social networking;
- blogs and wikis;
- video broadcasting;
- music downloading;
- gaming;
- mobile / smart phones with text, video and/or web functionality;
- other mobile devices with web functionality.

We need to take advantage of new technologies in our everyday teaching:

- the Internet provides instant access to a wealth of up-to-the minute information and resources from across the world, which would not ordinarily be available;
- the use of e-mails enables improved communication and facilitates the sharing of data and resources;
- Virtual Learning Environments (VLEs) provide students with a platform for personalised and independent learning.

Unfortunately, with this can come concerns such as:

- students might inadvertently access content of an unsavoury, distressing or offensive nature on the Internet or receive inappropriate or distasteful emails;
- students might receive unwanted or inappropriate emails from unknown senders, or be exposed to abuse, harassment or 'cyber-bullying' via email, text or instant messaging, in chat rooms or on social-networking websites, such as MySpace, Bebo, Facebook, Twitter etc.;
- Chat rooms provide cover for unscrupulous individuals to groom children.



At Scarisbrick Hall School we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

The purpose of an e-safety Policy is to ensure that we minimise the risks of the misuse of technology. We endeavour to embed eSafety messages across the curriculum whenever the Internet and / or related technologies are used. The eSafety policy will be introduced to the pupils at the start of each school year.

### **Development Process**

Policy written	February 2010
Initial discussion with Directors	
Approval of Policy by Directors	
Next major review	February 2012
Pupil involvement	Through Mentor groups, PSCHE and ICT
Parents' consultation	VLE
Staff involvement	Continuous application / review

### **Location and dissemination**

A copy of this policy can be found in the Staff room and on the VLE.

### **The content of the policy and its relationship to other policies**

This policy should be considered in conjunction with other written policies on ICT, Anti-Bullying, Support Learning, Child Protection, Behaviour and Discipline and PSCHE. The contents of this policy apply to all staff and pupils at Scarisbrick Hall School .

### **Links with outside agencies**

This policy has been written in accordance with BECTA guidelines and focuses on each individual technology available within the school and outlines the procedures in place to protect students and the sanctions to be imposed if these are not adhered to.

### **Social and Educational Benefits to be derived from the understanding and use of e-technologies**

- children and young adults are equipped with skills for the future;
- the Internet provided instant access to a wealth of up-to-date information and resources from across the world, which would not otherwise be available;
- the Internet helps to improve children's and/or young adults' reading and research skills;
- email and the use of some networking areas helps to foster and develop good social and communication skills.

The school feels that the benefits far outweigh the risks involved so long as users are made aware of the issues and concerns and receive ongoing education in choosing and adopting safe practices and behaviours.

Scarisbrick Hall is committed to educating staff, parents and pupils concerning the benefits and risks of technology. The school has links with CEOP who play a role in delivering sessions at the School to make sure that all pupils are aware of the dangers and pitfalls of new and emerging technologies.



### **Procedures for the use of a Shared Network**

Password security is essential for staff and pupils. Staff are expected to have secure passwords, which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. From Year 5 pupils are expected to use a personal password.

The following procedures should be adhered to:

- users must access the network using their **own** logons and passwords;
- users must respect confidentiality and attempts should not be made to access another individual's personal folder on the network without permission;
- if a user thinks a password may have been compromised or someone else has become aware of it he/she must report this to the e-learning Co-ordinator;
- software should only be installed by the Network Manager;
- removable media will be scanned for viruses before being used on a machine connected to the network;
- machines must never be left 'logged on' and unattended. If a machine is to be left for a short while, it must be 'locked' ( **Ctrl + alt + del followed by 'lock computer'** )
- machines must be 'logged off' correctly after use.

### **Procedures for the use of the Internet and email**

The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material, which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

The use of email within schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits and we recognise that pupils need to understand how to style an email in relation to their ages and good 'netiquette'.

All use of the VLE is logged and the logs are randomly and regularly monitored.

The following procedures are in place:

- all users must sign an Acceptable Use Agreement before access to the Internet and email is permitted in the school;



- Parental or Carer consent is requested in order for students to be allowed to use the Internet or email;
- users must access the Internet and email using their own logon / password and not those of another individual. Passwords must remain confidential and no attempt should be made to access another user's email account. If you feel your account details are known by others you should change your password immediately;
- the Internet and email must be used in a reasonable manner adhering to the professional judgement of the supervising teacher;
- students must be supervised at all times when using the Internet and email in school;
- procedures for Safe Internet use and sanctions are applicable if rules are broken;
- accidental access to inappropriate material is to be reported to the relevant Headteacher and a note of the offence recorded and acted upon;
- Internet and email filtering software is installed to restrict access, as far as possible, to inappropriate or offensive content and to reduce the receipt of 'spam', junk or unwanted correspondence. This is to be reviewed and updated regularly;
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that Parents recheck these sites and supervise this work;
- Internet and email use will be monitored regularly in accordance with the Data Protection Act;
- users must be careful when they disclose any information of a personal nature in an email or on the Internet. This includes mobile and home phone numbers, addresses, or anything else which might allow them to be identified;
- all emails sent should be courteous and the formality and tone of the language used appropriate to the reader. Sanctions, appropriate to the case, will be imposed on any users who break this code;
- the forwarding of chain letters is not permitted in school;
- bullying, harassment or abuse of any kind via email will not be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code;
- if users are bullied, or offensive emails are received, this must be reported immediately to a trusted adult or member of staff within the school. Emails received should not be deleted, but kept for investigation purposes;
- staff sending emails to external organisations, parents or pupils are advised to cc. the Headteacher or e-learning co-ordinator.

### **Managing other Web 2 technologies**

Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.



- At present, the school endeavours to deny access to social networking sites to pupils within school;
- all pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are;
- pupils are taught to avoid placing images of themselves on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once on line;
- pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are;
- our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals;
- pupils are encouraged to be wary about publishing specific and detailed private thoughts online;
- our pupils are asked to report any incidents of bullying to the school;
- **staff may only create blogs, wikis or other web 2 spaces in order to communicate with pupils using the VLE.**

**To ensure that sites are used appropriately we also encourage all parents and guardians to consider the following guidelines that are recommended by CEOP. The following guidance can be found at the CEOP website**

<https://www.thinkuknow.co.uk/parents/faq/socialnetworking/>

- Encourage them only to upload pictures that you as their parents / carer would be happy to see – anything too sexy to be passed round the dinner table should NOT make it on to the web. It's also not a good idea to post pictures which can identify the school which your child attends since this could help someone locate them.
- Tell your children not to post their phone number or email address on their homepage.
- Help your child to adjust their account settings so that only approved friends can instant message them. This won't ruin their social life – new people can still send them friend requests and message them, they just won't be able to pester them via Instant Messenger (IM).
- Check if your child has ticked the “no picture forwarding” option on their social networking site settings page – this will stop people sending pictures from their page around the world without their consent
- Encourage them not to give too much away in a blog. Friends can call them for the address of the latest party rather than read about it on their site.

Ask them to show you how to use a social networking site - getting involved will empower them to share the experience with you.



## **File transfers**

Files may be taken home or brought into school using the following methods:

- attached to emails using student's individual email accounts;
- bringing pen drives these will be checked by the network software when placed in a computer in the network. Data will then be transferred to / from student areas.

The school uses special filtering software, which prevents students from accessing most unsuitable sites and it also records every attempt students make to hit a site, whether successful or not, when and where he/she did it and who he/she is – every action under a password is recorded.

## **Mobile technologies**

Many emerging technologies offer new opportunities for teaching and learning including personalised learning. Many existing mobile technologies such as portable media players, mobile and smart phones are familiar to children outside of school too. They often provide Internet access and thus open up risk and misuse associated with communication and Internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately

Use any mobile or digital technologies 3G or mobile Internet services in any way to intimidate, threaten or cause harm to others will not be tolerated. Moreover, mobile technologies should not be used to access inappropriate materials or encourage activities that are dangerous or illegal.

Scarisbrick Hall School understands the benefit of mobile tablet devices to enhance learning. These devices will be treated the same way as a laptop and are subject to the same conditions outlined in this policy. The School has access to a secure wireless network and we therefore encourage parents and guardians to deactivate the 3g capabilities of tablets before they are brought into school. Each manufacturer provides clear guidance how to make devices safer e.g. <http://support.apple.com/kb/HT4213>

## **Procedures for the use of cameras, Video equipment and webcams**

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

Therefore:

- permission must be obtained from a student's parent or carer before photographs or video footage can be taken **with school equipment**;
- **staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips**;
- **pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others in school. However with the**



**express permission of the Headteacher, images can be taken on school trips, provided the permission of the parents of all pupils on the trip is sought and granted;**

- photographs and/or video footage can be downloaded and stored into an appropriate area under the guidance of the Network Manager;
- pupils and staff are not permitted to use personal portable media for storage of images (e.g. USB Flash Drives) without the express permission of the Headteacher;
- any photographs or video footage must be deleted immediately once no longer needed;
- webcams in school are only ever used for specific learning purposes;
- students and staff must conduct themselves in a polite and respectful manner when representing the school in a video conference or when corresponding via a webcam. The tone and formality of the language used must be appropriate to the audience and situation;
- all pupils are supervised by a member of staff when video conferencing;
- approval of the Headteacher is sought prior to all video conferences within the school;
- the school uses CCTV for security and safety, Notification of CCTV use is displayed in specific areas of the school.

On a child's entry to the school, all parents / carers will be asked to give permission to use their child's work / photos in the following ways:

- on the school web site;
- on the school's VLE;
- in the school prospectus and other printed publications that the school may produce for promotional purposes;
- in display material that may be used in the school's communal areas;
- general media appearances.

The consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents. Parents/ carers may withdraw permission, in writing, at any time.

#### **Procedures for using mobile phones, iPods**

- the school allows staff to bring in personal mobile phones and devices for their own use. **Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device;**
- the school is **not** responsible for student's mobile phones, pen drives, MP3 Players or iPods being damaged, lost or stolen. Items are brought into school at the owner's risk;
- if a mobile phone or iPod is activated in school without permission, it will be confiscated immediately, recorded and kept in a safe, locked place as per the mobile phone policy. Repeat occurrences will result in the student's privilege being withdrawn;
- this technology may be used, however for educational purposes, as mutually agreed with the Headteacher. The device user, in this instance, must always ask permission of the bill payer;

- the sending of inappropriate text messages between any members of the school community is not allowed;
- permission must be sought before any image or sound recordings are made on these devices of any member of the school community;
- users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.



### **Procedures for using personal PDAs and Games consoles**

- the use of personal PDAs and games consoles will not be permitted in school at any time. (tablet devices that enhance learning are except from this statement)

### **Procedures to ensure the safety of the school website**

- it is the responsibility of the designated member of staff, to approve all content and images to be uploaded onto the website prior to it being published;
- the website is checked every term to ensure that no material has been inadvertently posted, which might put students or staff at risk;
- copyright and intellectual property rights are respected;
- permission is obtained from parents or carers before any images of students can be uploaded onto the website;
- names are not used to identify individuals portrayed in images uploaded onto the website. Similarly, when a student is mentioned on the website, photographs which might enable this individual to be identified must not appear;
- when photographs to be used on the website are saved, names of individuals should not be used as file names.

### **If a student breaks any of the rules the following may happen:**

- a temporary ban on the use of all computer facilities at school until a discussion takes place with the Mentor and Head teacher;
- a ban, temporary or permanent, on the use of the Internet facilities at school;
- appropriate punishment within the school's disciplinary system;
- a letter informing parents what you have done;
- any other action decided by the Head teacher and Directors of the school.

Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the Police:

- Images of child abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative)
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist or anti-religious material
- Violence and bomb making

- Illegal taking or promotion of drugs
- Software piracy
- Other criminal activity



### **Wider Agency Support**

Scarisbrick Hall School fully embraces guidelines and support from the following organistaions;

- CEOP
- Thinkuknow
- Virtual Global Taskforce
- UKCCIS

### **Equal Opportunities**

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the school's eSafety rules.

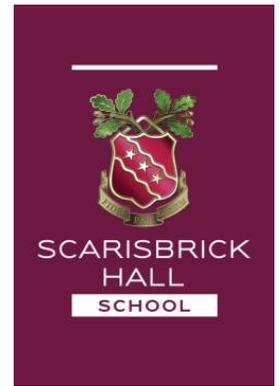
However staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety.

### **Future developments**

The procedures in this policy will be subject to ongoing review and modification in order to keep up with advances in the technology at the school. It may be that staff / students might wish to use an emerging technology for which there are currently no procedures in place. The use of emerging technologies will be permitted upon completion and approval of a risk assessment, which will be used to inform future policy updates.

# **SCARISBRICK HALL SCHOOL**



## **Acceptable Use Agreement: Staff, Directors and Visitors**

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Board of Directors.

- I will only use the school's email / Internet / Intranet / VLE and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Directors.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on the MIS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Directors.
- I will not install any hardware or software without permission of the Directors
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

### **User Signature**

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature ..... Date .....

Full Name .....(printed)

Job title . . . . .

# **SCARISBRICK HALL SCHOOL**

## **Acceptable Use Agreement: Pupils - Primary**



- ✓ I will only use ICT in school for school purposes.
- ✓ I will only use my own school email address when emailing.
- ✓ I will only open email attachments from people I know, or who my teacher has approved.
- ✓ I will not tell other people my ICT passwords.
- ✓ I will only open/delete my own files.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- ✓ I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ✓ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.



Dear Parent/ Carer

**Re: ICT Acceptable Use Agreement**

ICT including the internet, VLE, email and mobile technologies, etc have become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT. It is essential that pupils are aware of eSafety and know how to stay safe when using ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact me.

Yours sincerely

✂-----

**SCARISBRICK HALL SCHOOL  
ICT ACCEPTABLE USE AGREEMENT**

**Parent/ carer signature**

We have discussed this and .....(child name) agrees to follow the eSafety rules and to support the safe use of ICT at Scarisbrick Hall School.

Parent/ Carer Signature .....

Pupil's signature .....

Form ..... Date .....

# **SCARISBRICK HALL SCHOOL**

## **Acceptable Use Agreement:** **Pupils – Key Stages 3 and 4**



- I will only use ICT systems in school, including the internet, email, digital video, mobile technologies, etc. for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the school network/ VLE with my own user name and password.
- I will follow the schools ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school email address.
- I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- Images of pupils and/ or staff will only be taken, stored and used for school purposes inline with school policy and not be distributed outside the school network without the permission of the Headteacher
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring into disrepute.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted.

# **SCARISBRICK HALL SCHOOL**

## **AGREEMENT FORM FOR LAP TOP USERS**



This agreement is intended to set out the expectations of the pupil and parent in order to ensure that laptops are only used to support the learning process and ensure the best education of the pupil.

### **Pupil**

I will:

- keep the laptop in a suitable, secure and lockable case and keep it in a secure place;
- abide by the eSafety rules;
- agree to allow immediate and unrestricted access to all files and folders on the laptop to any members of staff should I be requested to do so;
- not play games, videos or any software unrelated to the task in hand;
- not use the webcam on the laptop;
- not allow other pupils to use the laptop;
- make a backup of all my work on the hard drive and on my pen drive;
- take responsibility for printing out my work and handing it in at the correct time;
- not store work belonging to another pupil;
- not permit the copying of any work onto the laptop;
- never have any indecent images or videos or any content that may offend others on the laptop;
- ensure that the laptop has adequate antivirus software installed and kept up to date.

Signed: ..... Date:.....

### **Parent**

I will:

- ensure that the laptop has suitable carrying case and all items are clearly named;
- agree to random checks being made by a member of staff;
- ensure that there is a compatible printer always available at home;
- regularly check that the laptop contains no material of a dubious nature;
- provide all necessary hardware, software, batteries etc.

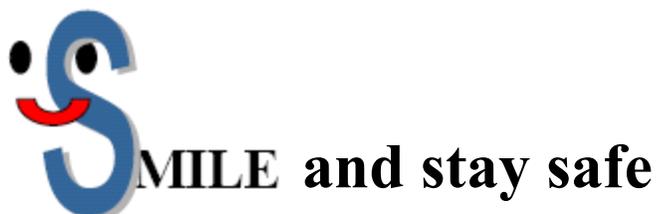
I have insured the laptop against loss, theft and damage and understand that my son/daughter takes full responsibility for it, and that the school takes no responsibility for it.

Signed: ..... Date: .....



# Smile and Stay Safe Poster

E-Safety Rules to be displayed next to all PCs in school



**S**taying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

**M**eeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

**I**nformation online can be untrue, biased or just inaccurate. Someone online may not be telling the truth about who they are - they may not be a 'friend'

**L**et a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

**E**mails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply



## **Current Legislation**

### **Acts relating to monitoring of staff email**

#### **Data Protection Act 1998**

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

<http://www.hmsso.gov.uk/acts/acts1998/19980029.htm>

#### **The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000**

<http://www.hmsso.gov.uk/si/si2000/20002699.htm>

#### **Regulation of Investigatory Powers Act 2000**

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

<http://www.hmsso.gov.uk/acts/acts2000/20000023.htm>

#### **Human Rights Act 1998**

<http://www.hmsso.gov.uk/acts/acts1998/19980042.htm>

### **Other Acts relating to eSafety**

#### **Racial and Religious Hatred Act 2006**

It is 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.

#### **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. Schools should already have a copy of “*Children & Families: Safer from Sexual Crime*” document as part of their child protection packs.

For more information  
[www.teachernet.gov.uk](http://www.teachernet.gov.uk)



### **Communications Act 2003 (section 127)**

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

### **The Computer Misuse Act 1990 (sections 1 – 3)**

Regardless of an individual’s motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another person’s password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

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

### **Malicious Communications Act 1988 (section 1)**

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

### **Copyright, Design and Patents Act 1988**

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone’s work without obtaining their author’s permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else’s material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

### **Public Order Act 1986 (sections 17 – 29)**

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



### **Protection of Children Act 1978 (Section 1)**

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

### **Obscene Publications Act 1959 and 1964**

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

### **Protection from Harassment Act 1997**

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

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