E-Safety Policy

Committee with oversight for this policy – Behaviour and Safety	
Policy to be approved by the Headteacher	
Policy last reviewed by the Committee	N/A
Policy last ratified by the Headteacher	3 November 2016
Policy / Document due for review	November 2019

Ravenor Primary School
e-Safety Policy

Contents

Our e-Safety Policy has been written by the school, building on Ealing's model policy (with acknowledgement to Hertfordshire Grid for Learning, LGfL, SWGfL and Bristol City Council, and Becta guidance.

Introduction

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

Information and Communications Technology 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 and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting (Audio Sharing)
- Video Sharing
- Music Sharing / Downloading
- Gaming
- Mobile / Smart phones with functionality including: text, video, web, audio, music , global positioning (GPS)
- Other mobile devices with similar functionality (tablets, laptops, gaming devices)

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

Ensuring children and young people are aware of the risks associated with the use of technologies, and can adopt safer behaviours, is vital in safeguarding them against cyber-bullying and grooming.

At Ravenor Primary School, we understand the responsibility to educate our pupils on e-Safety 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.

This policy relates to both fixed and mobile Internet technologies provided by the school, and technologies owned by pupils, parents and staff, but brought onto school premises.

Roles and Responsibilities

This is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and

practices are embedded and monitored. The named e-Safety co-ordinator in our school is Craig Jones who has been designated this role as Computing Co-ordinator. All members of the school community have been made aware of who holds this post. It is the role of the co-ordinator to keep abreast of current issues and guidance through organisations such as Ealing LA, CEOP (Child Exploitation and Online Protection), UKCCIS, and Childnet.

Senior Management and Governors are updated by the Head/ co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and particularly to the curricular for PHSE and SRE.

Skills / awareness development for staff

- Our staff receive regular information and training on e-Safety issues in the form of CPD training sessions.
- New staff receive information on the school's acceptable use policy as part of their induction.
- All staff has been made aware of their individual responsibilities relating to the safeguarding of children within the context of and know what to do in the event of misuse of technology by any member of the school community (see attached flowchart.)
- All staff is expected to incorporate activities and awareness within the Computing and PSHE curriculum areas.

Managing the school e-Safety messages

- We endeavour to embed messages across the curriculum whenever the Internet and/or related technologies are used. This is particularly reinforced in PSHE, SEAL, and RSE lessons in relation to cyber-bullying and to grooming.
- The policy will be introduced to the pupils at the start of each school year.
- Posters will be prominently displayed in each classroom.
- The school uses and Security software (LGFL) *this* system reminds users of their obligations as a condition of logging in.

Computing in the Curriculum

Computing and online resources are increasingly used across the curriculum. We believe it is essential for guidance to be given to the pupils on a regular and meaningful basis. Is embedded within our curriculum and we continually look for new opportunities to promote.

- The school has a framework for teaching in Computing / PHSE lessons using a range of resources provided by EGFL.

- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum
- PSHE and SEAL lessons provide the opportunity to discuss issues relating to cyber-bullying and Internet grooming (e.g. through respect for others and appropriate / positive relationships) these lessons can equip pupils with the knowledge to keep safe from harm.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staffs 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, not even with their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read ***and sign*** an Acceptable Use Agreement to demonstrate that they have understood the school's Policy.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- If a user thinks their password may have been compromised or someone else has become aware of their password they are expected to report this to Craig Jones.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left logged on.
- Due consideration should be given when logging into the Learning Platform / Managed Learning Environment to the browser/cache options (shared or private computer)
- In our school, all ICT password policies are the responsibility of Craig Jones and all staff and pupils are expected to comply with the policies at all times.

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously. The school follows Becta guidelines (published autumn 2008)

- Staff are aware of their responsibility when accessing school data. Level of access is determined by the HT

- Any data taken off the school premises must be encrypted whether in a laptop or USB device.
- Data can only be accessed and used on school computers or laptops. Staff are aware they must not use their personal devices for accessing any ***school/ children/ pupil*** data
- The school network is back up internally / using a secure remote back up facility provided by the LGfL.

Managing the Internet

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. In our school access to the Internet is via the London Grid for Learning. Internet is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- The school maintains students will have supervised access to Internet Resources (where reasonable) through the school's fixed and mobile internet technology
- Staff will preview any recommended sites before use with students.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested. These will have been checked by the teacher. Where possible links from the school learning platform will be provided,
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Infrastructure

- Ealing Local Authority has a monitoring solution via the London Grid for Learning. Upon request, web-based activity can be monitored and recorded.
- School Internet access is controlled through the LGfL's web filtering service.
- Ravenor Primary School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and pupils are aware that school based email and Internet activity can be monitored and explored further if required.
- The school does not allow pupils access to Internet logs.
- The school uses management control tools for controlling and monitoring workstations.

- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator.
- The offending URL will be reported to the LGfL.
- Sophos Anti-Virus protection is provided by the LGfL and is set to automatically update on all school machines. This is the responsibility of (network manager / technical support company (Flexitech).
- Pupils and staff are not permitted to download programs or files on school equipment without seeking prior permission from the network manager and ICT Coordinator.

Managing other Communication & Networking technologies

The Internet includes a wide range of communication and networking tools & sites. Children need to be educated about appropriate ways of communicating and about the risks of making personal information too easily available. If used responsibly both outside and within an educational context it 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 denies access to social networking sites to pupils within school. (Such as Facebook, Myspace and Bebo).
- 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 (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- 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.
- Pupils are asked to report any incidents of bullying to the school.
- Pupils are introduced to a variety of Internet communication tools within the safe context of the school learning platform / London MLE.
- Staff understand that it is highly inappropriate to use social networking sites and other personal communication tools to communicate with pupils and / or parents (e.g.: Facebook, MySpace, Twitter, email etc). Staff is expected to use the tools within the school learning platform / MLE.

- Staff understand that it may be considered a disciplinary offence if they mention on social networking sites; issues concerning students / parents / carers / other staff associated with the school.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies (such as portable media players, gaming devices, Smart phones, etc) are familiar to children outside of school. Allowing such personal devices to access the school network can provide immense benefits in collaboration, but also create risks associated with misuse, inappropriate communications, etc. Emerging technologies will be examined for educational benefit and the risk assessed before such use of personal devices is facilitated in school. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

- 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.
- Under exceptional circumstances Year 6 pupils are allowed to bring personal mobile devices/phones to school but these must be locked away during the day and must not be used for personal purposes within lesson time.
- Technology may be used, for educational purposes, as mutually agreed with the Headteacher. The device user, in this instance, must always ask the prior permission of the bill payer.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the school community is not allowed.
- Permission must be sought before any image; video or sound recordings are made on these devices of any member of the school community.
- Capturing images & video is not allowed by students / staff unless on school equipment and for educational purposes.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School provided Mobile devices (including phones)

- The sending of inappropriate text messages between any members of the school community is not allowed.
- Permission must be sought before any image; video or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies (e.g.: phones, laptops, etc) for offsite visits and trips, only these devices should be used.

- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

For the purposes of this document "the school" means the "School site"

Managing email

The use of email within most 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 including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and be aware of what constitutes good 'netiquette'. In order to achieve ICT level 4 or above, pupils must have experienced sending and receiving emails.

- The school gives all staff an individual LGfL StaffMail account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and that of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. Staff LGfLmail should used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- Email sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending emails to external organisations, parents or pupils are advised to cc. the Headteacher, line manager or designated office account.
- LGfL StaffMail and LondonMail are subject to mail scanning.
- All email users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive message and keep the offending message(s) as evidence.
- Staff must inform (the eSafety co-ordinator/ line manager) if they receive an offensive email.

Safe Use of Images / Video

Taking of Images and Video

Digital images / video are easy to capture, reproduce and publish and, therefore, easily 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.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images / video by staff and pupils with school equipment.
- Staff are not permitted to use personal devices, (e.g.: mobile phones and cameras), to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.
- Pupils are not permitted to use personal devices, (e.g.: mobile phones and cameras), to record images of the others, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the pupils device.
- Images of pupils are deleted when pupils leave the school.

Consent of adults who work at the school

- Permission to use images / video of all staff who work at the school is sought on a regular basis and a copy is located in the personnel file
- Parents must seek permission to take photos / video school events, and must agree to NOT post images / video on the Internet.
- Parents are requested NOT to video school performances. Video are captured ONLY by school staff and are stored on the LGfL VideoCentral secure service and made available on the school website / MLE.

Publishing pupil's images and work

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

- On the school web site
- On the school's Learning Platform / MLE
- In the school prospectus and other printed publications that the school may produce for promotional purposes
- Recorded/ transmitted on a video or webcam
- In display material that may be used in the school's communal areas
- In display material that may be used in external areas, i.e. exhibition promoting the school
- General media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This 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, custody issues, etc. Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Pupils' names will not be published alongside their image and vice versa. Email and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Video is only streamed from the LGfL VideoCentral service set to private.
Only the Web Manager has authority to upload to the public website.

Storage of Images / Video

- Images/ video of children are stored on the school's network and London MLE provided by Fronter.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/ Learning Platform / MLE.
- Images / video of pupils are deleted when pupils leave the school.

Webcams and CCTV

- The school uses CCTV for security and safety. The only people with access to this are site/facilities managers and members of the senior management team. Notification of CCTV use is displayed at the front of the school.
- We do not use publicly accessible webcams in school other than for special projects such as nature cams which are streamed to the web.
- Webcams in school are only ever used for specific learning purposes, (e.g.: monitoring hens' eggs) Images of children / adults ever never broadcast.
- Misuse of a webcam by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document)
    - Webcams can be found with network manager. Notification is given in this/these area(s) videoed by webcams by signage.
    - Consent is sought from parents/carers and staff on joining the school, in the same way as for all images.

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences
- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school.
- All pupils are supervised by a member of staff when video conferencing
- All pupils are supervised by a member of staff when video conferencing with end-points beyond the school.
- The school keeps a record of instances of video conferences, including date, time and participants.
- Approval from the Headteacher is sought prior to all video conferences within school.
-
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.

- No part of any video conference is recorded in any medium without the written consent of those taking part.

Misuse and Infringements

Complaints

Complaints relating to e-Safety should be made to the e-Safety co-ordinator or Headteacher. Incidents should be logged (see Incident Log in Appendix) and process should be followed (see Flowchart in Appendix)

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences
- Users are made aware of sanctions relating to the misuse or misconduct as part of the ICT induction lesson at the beginning of each school year (first lesson). Access rights will be removed for individuals who misuse access. Specific sites are available and vetted as part of the LA and school firewall settings.

Equal Opportunities

Pupils with additional needs

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 schools' 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. Internet activities are planned and well managed for these children and young people.

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting both in and outside of school while appreciating the benefits provided by technologies generally. We regularly consult and discuss with parents/ carers and seek to promote a wide understanding about the link between and safeguarding.

- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- The school disseminates information to parents relating to eSafety where appropriate in the form of;

- Information and celebration evenings
- Posters
- Newsletter items
- Leaflets

Writing and Reviewing this Policy

Staff, parent and pupil involvement in policy creation

- Staff and pupils have been involved in making/ reviewing the policy through analysis of pupil questionnaires, school council, staff meetings, parent information sessions and governor meetings.

Review Procedure

There will be an on-going opportunity for staff to discuss with the coordinator any issue of e-Safety that concerns them.

This policy will be reviewed every 12 months and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

This policy has been read, amended and approved by the staff and Headteacher.

Acceptable Use Agreement: Staff, Governors and Visitors

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 Claire Meade the school e-Safety coordinator.

- I will comply with the ICT system security protocols and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils, parents and staff are compatible with my professional role, and never via personal email / phone accounts / social networking profiles.
- I will not discuss school issues on social networking sites / web-blogs.
- I will not give out to pupils, my own personal contact details, such as mobile phone number and personal email address.
- I will only use the approved, secure email system(s) and MLE tools for communications related to my professional role.
- I am aware that communicating with students / pupils via private email / SMS and social networking sites may be considered a disciplinary matter.
- I will ensure that personal data (such as data held on SIMS) 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 Governing Body and will be encrypted.
- I will not install any hardware or software without permission of the ICT leader
- I will not browse, download, upload or distribute any material of a pornographic, offensive, illegal or discriminatory nature. **I understand that to do so may be considered a disciplinary matter, and in some cases a criminal offence.**
- Images & videos of pupils and / or staff will only be taken, stored on school equipment and will only be used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images & video will not be distributed outside the school network / MLE without the permission of the parent/ carer, member of staff 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 or the school 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 . . . . . .

Responsible Internet Use - KS2

These rules help us to be fair to others and keep everyone safe.

- I will ask permission before using the Internet.
- I will work under the 'Pupil user' on my school network.
- I will only connect to the school network using my own username.
- I will only look at or delete my own files.
- I understand that I must not bring software or disks into school without permission from my teacher.
- I will only visit approved websites as instructed by an adult.
- I will not use Internet Chat or Internet Messaging or visit Chat rooms/websites.
- I understand that I must never give my home address or phone number, or arrange to meet anyone.
- If I see anything I am not happy with, or receive messages I do not like, I will tell an adult immediately.
- I understand that the school may check my computer files and the Internet sites I visit.
- I understand that if I break these rules, I may not be allowed to use the Internet or computers.

Responsible Internet Use – FS & KS1

- We will ask an adult before we visit a website
- We only use the internet when an adult is with us.
- We can click on the buttons or links when we know what they do.
- We can search the Internet with an adult.
- We always ask if we get lost on the Internet.

Incident Log (suggested format)

'School name' eSafety Incident Log

Details of ALL eSafety incidents to be recorded by the eSafety Coordinator. This incident log will be monitored termly by the Headteacher, Member of SLT or Chair of Governors. Any incidents involving Cyberbullying should be recorded on the 'Integrated Bullying and racist Incident Record Form 2'

Date & time	Name of pupil or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons

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.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
http://www.hmso.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.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts relating to eSafety
Racial and Religious Hatred Act 2006
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.

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

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)
06/01/2012 - 21 -
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 the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

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

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.

Keeping Children Safe in Education DfE September 2016.