ST PATRICK'S
Catholic College

‘Seek Ye First the Kingdom of God...’

Matthew 6.33

E-Safety Policy

Contents	Page(s)
Introduction	2
Roles and Responsibilities	3
e-Safety in the Curriculum	4
Password Security	5
Data Security	6
Managing the Internet safely	7
Managing other Web technologies	8
Mobile Technologies	9
Managing email	11
Safe Use of Images	12
Misuse and Infringements	13
Equal Opportunities	13
Parental Involvement	14
Writing and Reviewing this Policy	14
Acceptable Use Agreement: Staff, Governors and Visitors	15
Acceptable Use Agreement: Students	18
Flowcharts for Managing an e-Safety Incident	21
Incident Log	24
Smile and Stay Safe Poster	25
Current Legislation	26

Our e-Safety Policy has been written by the college, building on the Stockton-on-Tees LA guidance.

Introduction

Information and Communications Technology (ICT) in the 21st Century is 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, our school needs to build in the use of these technologies in order to support our young people to develop the skills to access life-long Learning and employment.

ICT covers a wide range of resources including web-based and mobile Learning. It is important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies students 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
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

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.

At St Patrick's Catholic College we understand the responsibility to educate our students 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.

Both this policy and the Acceptable Use Policy (for all staff, governors, visitors and students) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, web books, PDAs, tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, and portable media players, etc).

Roles and Responsibilities

The Head of Children's services and the Headteacher are both personally and legally responsible for the (e)safety of all members of the school community. Headteacher and governors have ultimate responsibility in ensuring that the policy and practices are embedded and monitored. The named e-Safety co-ordinator in our school is ***Mrs Michelle Booth*** who has been designated this role as a member of the senior Leadership team. All members of the school community have been made aware of who holds this post. It is the role of the e-Safety co-ordinator to keep abreast of current issues and guidance through organisations such as Stockton-on-Tees LA, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Leaders and Governors are updated by the Headteacher/ e-Safety 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 students (appendices), is there to protect the interests and safety of the whole school community. It is linked to the following school policies: child protection, health and safety, home-school agreements, PHSE, anti-bullying and Behaviour policy**.**

E-Safety skills development for staff

- Our staff receive regular information and training on e-Safety issues in the form of updates and inclusion within twilight and PD day programmes.
- New and trainee staff receive information on the school's acceptable use policy as part of their induction.
- All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community (see attached flowchart.)
- Departments, particularly ICT, are encouraged to incorporate e-Safety activities and awareness within their curriculum areas.

Managing the school e-Safety messages

We endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used.

- The e-Safety message is introduced to students at the start of each school year.
- e-Safety posters are prominently displayed throughout the school as part of our anti-bullying campaign
- The School's website has CEOP abuse icon for further information. All students have been trained how to use this tool.

E-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-Safety guidance to be given to students on a regular and meaningful basis. e-Safety is embedded within our curriculum and we constantly seek new opportunities to promote e-Safety.

- The school has a framework for embedding internet skills in ICT/ PHSE lessons
- The school provides opportunities within a range of curriculum areas to Learn about e-Safety.
- Educating students on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum.
- Students are aware of relevant legislation when using the internet such as data protection and intellectual property, which may limit what they want to do but also serves to protect them.
- Students are taught about copyright and respecting other people's information, images etc. through discussion, modelling and curriculum activities.
- Students are aware of the impact of on-line bullying and know how to seek help if they are affected by these issues. Students are 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 organisations such as CEOP.
- Students are taught to critically evaluate materials and Learn research skills through cross curricular work, discussions and via the ICT curriculum

Password Security

Password security is essential for staff, particularly as they are able to access and use student data. Staff must have secure passwords, which are not shared with anyone. Students are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and students are regularly reminded of the need for password security and to renew passwords

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-Safety Policy.

- Users are provided with an individual network, email and Learning Platform log-in username. Throughout their time in school students are expected to use a personal password and keep it private.

- Students are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.

- Any user whose password may have been compromised or if someone else has become aware of their password should report this to the ICT technical staff or an ICT teacher.

- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS system, email, remote access and 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 unattended or unlocked. The automatic log-off time for the school network is 50 minutes.

- ICT password policies are the responsibility of the ICT Network Manager and all staff and students 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.

- Staff are aware of their responsibilities when accessing school data.
- The level of access to school or student data is determined by the Head teacher.
- Data can only be accessed and used on school computers or laptops in school.
- Any data which refers to sensitive information about students should not be openly transmitted across the internet via email – any such information should be password protected and/or initials only used to refer to any individual
- Staff can remotely access school files through a 2 form factor level security system when granted access by the IT department.
- Staff and students are responsible for files stored in their personal space on school servers and any personal storage devices brought into school. There must be no use of distribution of malicious files.

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. All use of the internet is logged and a weekly log is produced from the school proxy server. Whenever any inappropriate use is detected it will be followed up.

- St Patrick's Catholic College allows students to have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology.
- Staff are recommended to preview any sites to be used with students prior to use.
- Raw image searches are discouraged when working with students. Such sites are normally blocked for student use as part of the filtering service.
- 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. Parents will be advised to supervise any research through SMHW.
- All users are expected to observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- Documents must not be published by users on the internet which are defamatory or which may be intimidating, hostile or offensive to others on the basis of sex, race, colour, religion, national origin, sexual orientation or disability.
- Similarly, users must not accesses materials on the internet which may be objectionable on the above grounds as they would violate the terms of the signed Acceptable Use Agreement
- All users are expected to observe copyright of materials from electronic resources.

Infrastucture

- School internet access is controlled through One IT and school's in-house web filtering service. Our ICT Network Manager monitors Internet usage via web filtering portal on a regular basis and forwards any inappropriate use in line with the school's published policy to the e-Safety co-coordinator, Mrs Michelle Booth.
- St Patrick's Catholic College is aware of its responsibility when monitoring staff communication under current legislation and takes account of; 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 students are aware that school based email and internet activity can be monitored and explored further if required.
- The school does not allow students access to internet logs.
- The school uses the management control tool called NetSupport for controlling and monitoring workstations.
- If staff or students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-Safety co-ordinator or ICT technical staff.
- It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines.
- Students and staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software.
- The school anti-virus software is set to automatically check the contents of any personal storage media attached to the system. It will automatically quarantine any suspected virus or malware identified on the personal storage media.
- Students and staff are not permitted to download programs or files on school based technologies, nor should they use any software or hardware designed to subvert the integrity of the school network.
- If there are any issues related to viruses or anti-virus software, the ICT technical staff should be informed in person.

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. We recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students 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 students within school.
- All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Students 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.
- Students 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, email address, specific hobbies/ interests).
- Students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Students are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our students are asked to report any incidents of bullying via such web media to the school.
- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with students using the school Learning Platform or other systems approved by the Headteacher.

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, mobile and Smartphones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible 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.

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 student or parent/ carer using their personal device.

- Students are allowed to bring personal mobile devices/phones to school but must not use them at any point during the school day. At all times the device must be switched onto silent and remain out of sight.
- Such technology may be used however for educational purposes, as mutually agreed with the Headteacher. The device user, in this instance, must always seek 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 member 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.

School provided Mobile devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies such as phones, and laptops 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.

Managing email

The use of email within school is an essential means of communication for both staff and students. In the context of school, email should not be considered as being private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or student based, within school or international. We recognise that students need to understand how to style an email in relation to their age and good 'etiquette'.

- The school gives all staff and students their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and to avoid the risk of personal profile information being revealed.
- It is the responsibility of each user to keep their password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used to conduct any school business.
- Under no circumstances should staff contact students, parents or conduct any school business using personal email addresses.

- The school attaches a standard disclaimer to all email correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. This disclaimer should not be removed.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper. This is particularly important since such emails are not subject to the same internal scrutiny as letters on headed notepaper are prior to being sent.
- Staff sending emails to external organisations, parents or students are advised to cc. the Headteacher, senior leader or line manager.
- Students may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- All our students have their own individual school issued accounts.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette particularly in relation to the use of appropriate language, revealing personal details about themselves or others in e-mail communication, arranging to meet anyone without specific permission and virus checking attachments.
- Students must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Staff must inform the e-Safety co-ordinator/Headteacher if they receive an offensive e-mail.
- Students are introduced to email as part of the ICT Scheme of Work.
- ***All staff will be made aware of, and must sign, the Email Guidance Policy.***

Safe Use of Images

Taking of Images and Movies

Digital images are easy to capture, reproduce, transform and publish and, therefore are easy to misuse. It is not appropriate to take or store images of any member of the school community or public, without having first sought consent and considered the appropriateness of such images. The MIS contains an up-to-date record of parental/carer permission for the taking of images of our students, this record should be checked prior to taking images and in particular prior to publication of any images taken.

- With the written consent of parents (on behalf of students) and staff, the school permits the appropriate taking of images by staff and students with school equipment.
- Staff are not generally permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on field trips. However with 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.
- Students are not generally permitted to use personal digital equipment, including 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 students device.

Consent of adults who work at the school

Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file. This links also to the Digital Photography & Images Policy.

Publishing students' images and work

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 Learning Platform
- 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, eg divorce of parents, custody issues, etc. ***Parents/ carers may withdraw permission, in writing, at any time.***

Students' names will not be published alongside their image and vice versa. E-mail and postal addresses of students will not be published. Students' 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.

Only the ICT technical support staff have authority to upload to the school website.

Storage of Images

- Images/ films of children are stored on the school's network and MIS system
- Students and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher
- Rights of access to this material are restricted to the teaching staff and students within the confines of the school network/ Learning Platform.
- The network manager has the responsibility of deleting/archiving the images when they are no longer required.

Webcams and CCTV

- The school uses CCTV for security and safety. The only people with access to this are the senior leaders in the school and lunchtime supervisory staff by agreement with a senior leader. Notification of CCTV use is displayed at the front of the school.
- We do not use publicly accessible webcams in school.
- Webcams in school are only ever used for specific learning purposes, e.g. monitoring a scientific experiment, never using images of children or adults.
- Misuse of webcam technology by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document)

Video Conferencing

- Permission is sought from parents/carers if their child is involved in video conferencing
- All students are supervised by a member of staff when video conferencing
- Approval from the Headteacher is sought prior to all video conferences within school.
- No part of any video conference would be 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 and the **Flowcharts for Managing e-Safety Incidents** should be followed (see appendix).

Inappropriate material

All users are made aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-Safety co-ordinator.
Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety 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 (see flowchart.)

Staff users are made aware of sanctions relating to the misuse or misconduct by posters displayed in the staffroom, discussion within staff training events, reminders at staff meetings/briefings and through induction programmes

Student users are made aware of sanctions relating to the misuse or misconduct by discussion within the ICT curriculum and wider curriculum including PSHE. Sanctions are listed as an appendix within this document and student sanctions are replicated within the School's Behaviour Policy

Equal Opportunities

Students with additional needs

The school seeks to create a consistent message with parents for all students and this in turn aids the establishment and future development of the schools' e-Safety procedures and rules. Staff know that some students require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

Where a student has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety. Internet activities are planned and managed to effectively support these students.

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting e-Safety both in and outside of school. We regularly consult and discuss e-Safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
- Parents are invited to a yearly training on e-safety delivered by a CEOP's trainer.
- 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 the school website)
- The school disseminates information to parents/carers relating to e-Safety where appropriate in the form of;
- Information and celebration evenings
- Posters
- Website/ Learning Platform postings
- Newsletter items
- Learning platform training

Writing and Reviewing this Policy

Review Procedure

There will be an on-going opportunity for staff to discuss, with the e-Safety coordinator, any issue of e-Safety that concerns them. ***This policy will be reviewed biannually*** and consideration given to the implications for future whole school improvement planning. The policy will also be amended if new technologies are adopted or there are National changes to the orders or guidance in any way.

Acceptable Use Agreement: Staff, Governors and Visitors

Are you connected to the network?

(1) You should understand fully if your laptop or desktop is configured to work on the school network or if it is not configured to work on the school network.

Laptop or Desktop(s) – Not configured to work on the school network

(2) Your laptop or desktop should not be connected to the school network.

(3) You should ensure anti-virus software is updated at least three times a week. (Laptops configured to connect to the network will update automatically). It would be prudent to make available your laptop when requested to help you ensure your virus software is up to date.

(4) You must NOT connect your laptop or desktop by network cable to the school network under any circumstance. You must consult the Network Manager if you wish a laptop or desktop to be connected to the network.

Laptops or Desktop(s) – Configured to work on the school network

(5) Your school laptop should not be used on the internet at home.

(6) You will need to connect your laptop to the network at least once a day to ensure all security patches are up to date. The update is automatic; you only need to log on, wait for 10 minutes and log off. If you take a computer attendance register using your laptop, then these updates will occur whilst using the electronic register.

(7) Your laptop should not be connected to any other network (wired or wireless) at home or elsewhere under any circumstance.

All Laptops and Desktops in the school

(8) You should never install software on any school laptop or school desktop computer. You need to complete a technical request form if installation of software is required. Software can only be installed if the license is made available.

(9) For your protection and the protection of the network you should never allow a student to use your own user account, SIMS account or email account.

(10) You should never allow a student to use the internet if his/her own account does not work. Accounts might not work because: the student's Internet or email account is disabled due to infringements; not enable because the student has not brought in an Internet/email/network letter; the student has forgotten his/her own username or password.

(11) You should never allow a student to use your laptop or desktop to take the electronic register.

(12) If an investigation were required to determine the cause of a network issue, it would be prudent to make available your laptop to identify the problem if requested.

(13) When a software audit is being carried out, it would be prudent to make available your laptop to ensure your laptop configuration adheres to St. Patrick's format.

(14) You should not upload material to shared areas, which infringes Copyright. You should seek advice if required. Unfortunately where an infringement is detected, resources will be removed from shared areas and access to upload is removed.

(15) The Internet and email at school should be only used for schoolwork. Logs of all activity will be recorded and accessed if required at a future date to help resolve any issues.

(16) if you use an external hard drive, any form of memory stick, CD/DVD or any other storage media to copy files (of any description) onto your laptop or any computer in the school, you should ensure the computer it came from is virus free.

(17) If you allow a student to use your laptop or school PC you should ensure he/she uses his/her own network account, SIMS account and email account.

(18) If you have your laptop or desktop computer you must always log off/lock the computer to protect your files and the integrity of the network.

(19) If you have your laptop at school it must be left in a secure area.

(20) You should ensure that your laptop has been security marked in the event that your laptop is lost or stolen.

(21) When transporting your laptop from the school to home, or vice versa, you must ensure it is not left unattended (e.g. in your car), as the school insurance does not cover the theft of your laptop if left unattended.

(22) If you bring in a device such as a hand held computer or mobile phone you must ensure that the wireless network settings are disabled when in school, if the wireless device conforms to 11a, 11b, or 11g. If you are not sure what this means you should seek advice when you bring in such a device.

(23) You should not allow any student under any circumstance to remove or replace cables from a PC, usually at the back of the PC. These can include a keyboard, mouse, power cable, monitor, etc…. Students are allowed to plug in and remove a USB stick or cable for a digital camera.

(24) Each member of staff should sign an agreement to indicate he/she has understood the school policy.

Full Name: ___________________________________ Department: __________________

Signed: _________________________ Date: __________________

Acceptable Use Agreement: Students

RULES FOR ALL STUDENTS AT ST PATRICK'S CATHOLIC COLLEGE

1) Students bringing in content (files, pictures, etc.) on USB sticks or on any other media storage devices, or sending files via the email or the Internet from outside school must ensure that virus protection is installed on the PC. Please see the IT staff if you require advice on antivirus software.

2) The Internet should only be used for school related work and should not attempt to access unsuitable material from the Internet.

3) Do not attempt to log on to the St Patrick's network, e-mail, VLE or to any other computer system with another person's account. You must not under any circumstances allow other students to use your username and password.

4) Students must understand that any e-mail going out from the school will carry St. Patrick's address. Do not give out personal information about yourself in an e-mail, including your home address, unless given permission by a teacher.

5) Students must act responsibly when using the school email or the VLE. Do not send e-mails with any material that is inappropriate or use offensive or threatening language in e-mails. If you receive an email containing material of a violent, dangerous, abusive, or inappropriate content, always report such messages to a member of staff.

6) Students can only save content and electronic documents on the school network that are appropriate and related to school use. Do not attempt to save or download any other type of file, for example, software, games, illegal music, etc.

7) Do not attempt to install any software on the computers. Students are only permitted to access software installed by the school.

8) Students can print files appropriate for and related to educational use in the school. Ask a teacher before you print out any information from the Internet that you are unsure about.

9) School ICT facilities must be used in a responsible manner and do not attempt to 'fix' equipment yourself (e.g. PC, Laptops, Printers). Students should report any faults or misuse of school facilities immediately to the ICT staff.

10) Students must understand that failure to comply with these rules will leadd to a temporary ban on the Internet and/or network account. However, serious violations will be dealt by senior management following the school behaviour policy procedure.

11) Without a signed form, both the student's Internet account and network account will be suspended. If they have been suspended, these accounts will be reactivated when the student and parent/guardian have returned the signed form.

(12) When using Social networking sites at home, such as, but not limited to, Facebook, students should understand the following:

• bullying in any form is totally unacceptable at St Patrick's Catholic College. Using social networking sites to bully students will not be tolerated. Social networking has no boundary, crossing over into the school.

• be aware that placing personal information onto a social networking site, such as your name, home address, telephone number etc. can be visible to anyone in the world. When using social networking sites at home the school advises parents or guardians to ensure that the settings of the account are set to friends only.

• be very careful what information is placed onto a social networking site. For example, not saying when you might be going on holiday. This type of information would be an advertisement on when your home might be empty.

• understand that the person you are speaking to on a social networking site may not be the person he/she says they are.

• be aware when uploading photos of yourself, such as in school uniform, which could be used by others to identify the school you attend and put you in a vulnerable position.

• understand the school advises that students should not arrange through a social networking site or other online, digital or analogue communication system to meet someone. The person they are communicating with may not be the person he/she says they are.

• understand that uploading text/photos/videos onto a social networking or other type of site that you would not want your parent or guardian to see should NOT be uploaded. Text/photos/videos can be copied and distributed by other people and once on the web cannot be easily removed.

Pupil,

As a school user of the Internet, I agree to comply with the rules on its use. I will use the school network in a responsible way and observe all the restrictions explained to me by the school.

Pupil's signature _____________________

Date: ___/___/___

Parent,

As the parent or legal guardian of the pupil signing above, I grant permission for my son or daughter to use electronic mail and the Internet. I understand that pupils will be held accountable for their own actions. I also understand that some material on the Internet may be objectionable and I accept responsibility for setting standards for my son or daughter to follow when using the Internet.

Parent's signature ______________________________

Date: ___/___/___

Pupil's name __________________________________

Form/class ____________________________________

Committing an Illegal Act - Did You Know? (Staff Version)

1. Receiving unsolicited emails that may contain potentially illegal material (either as an attachment or in a URL) is not an illegal offence

2. If you receive potentially illegal material you could easily commit an illegal act - **do not open the material or personally investigate**

3. Opening an attachment or URL that proves to hold illegal content **is an illegal act** and is classed as possession of illegal material

4. Showing anyone else illegal material that you have received **is an illegal act**

5. Printing a copy of the offensive email to report it to someone else **is an illegal act** and is classed as producing illegal material

6. Printing a copy of the material to give to someone else **is an illegal act** and is classed as distributing illegal material

7. Within 4 simple steps you could easily break the law 4 times. Each is a serious offence

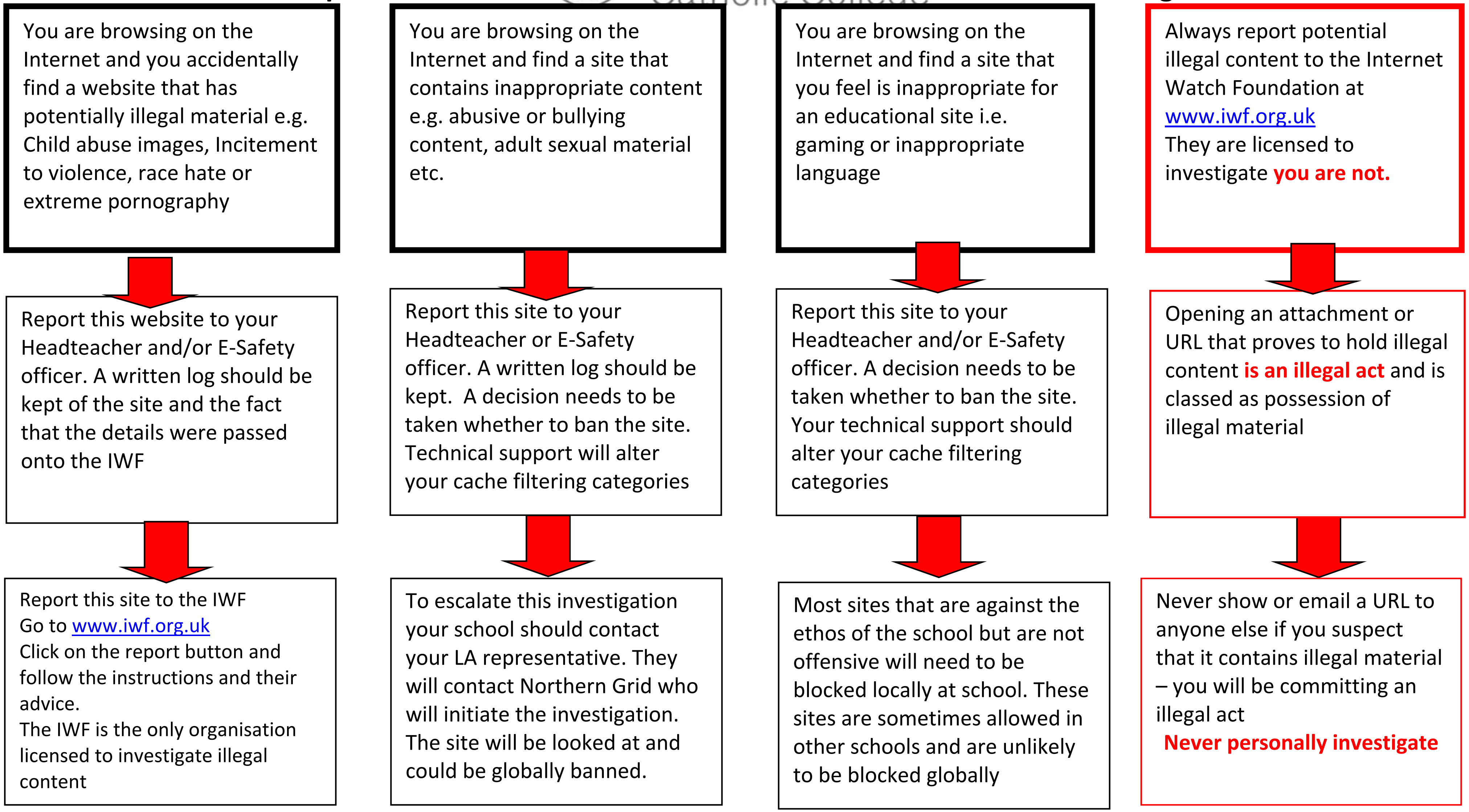
8. Never open unsolicited URLs or attachments. If you are suspicious that the content could be illegal report it and log that you have received it

9. Always report potential illegal content to the Internet Watch Foundation at www.iwf.org.uk They are licensed to investigate **you are not.**

Never personally investigate. If you open illegal content accidentally, report it to the Headteacher and IWF. Go to the IWF website and click on the report button. **Do not copy and paste the URL, write it down and type it into the reporting screen. This prevents accidental opening**. Once the email has been logged and reported to the IWF delete it from your inbox. If you are unsure, contact the IWF for advice on 01223 237 700. **The Internet Watch Foundation only deals with illegal content please see their website for information and advice. Please note this guidance only relates to illegal content not inappropriate.**

ST PATRICK'S
Catholic College

What to do with Suspicious Web Browsing – Staff Version



You are browsing on the Internet and you accidentally find a website that has potentially illegal material e.g. Child abuse images, Incitement to violence, race hate or extreme pornography

Report this website to your Headteacher and/or E-Safety officer. A written log should be kept of the site and the fact that the details were passed onto the IWF

Report this site to the IWF
Go to www.iwf.org.uk
Click on the report button and follow the instructions and their advice.
The IWF is the only organisation licensed to investigate illegal content

You are browsing on the Internet and find a site that contains inappropriate content e.g. abusive or bullying content, adult sexual material etc.

Report this site to your Headteacher or E-Safety officer. A written log should be kept. A decision needs to be taken whether to ban the site. Technical support will alter your cache filtering categories

To escalate this investigation your school should contact your LA representative. They will contact Northern Grid who will initiate the investigation. The site will be looked at and could be globally banned.

You are browsing on the Internet and find a site that you feel is inappropriate for an educational site i.e. gaming or inappropriate language

Report this site to your Headteacher and/or E-Safety officer. A decision needs to be taken whether to ban the site. Your technical support should alter your cache filtering categories

Most sites that are against the ethos of the school but are not offensive will need to be blocked locally at school. These sites are sometimes allowed in other schools and are unlikely to be blocked globally

Always report potential illegal content to the Internet Watch Foundation at www.iwf.org.uk
They are licensed to investigate **you are not.**

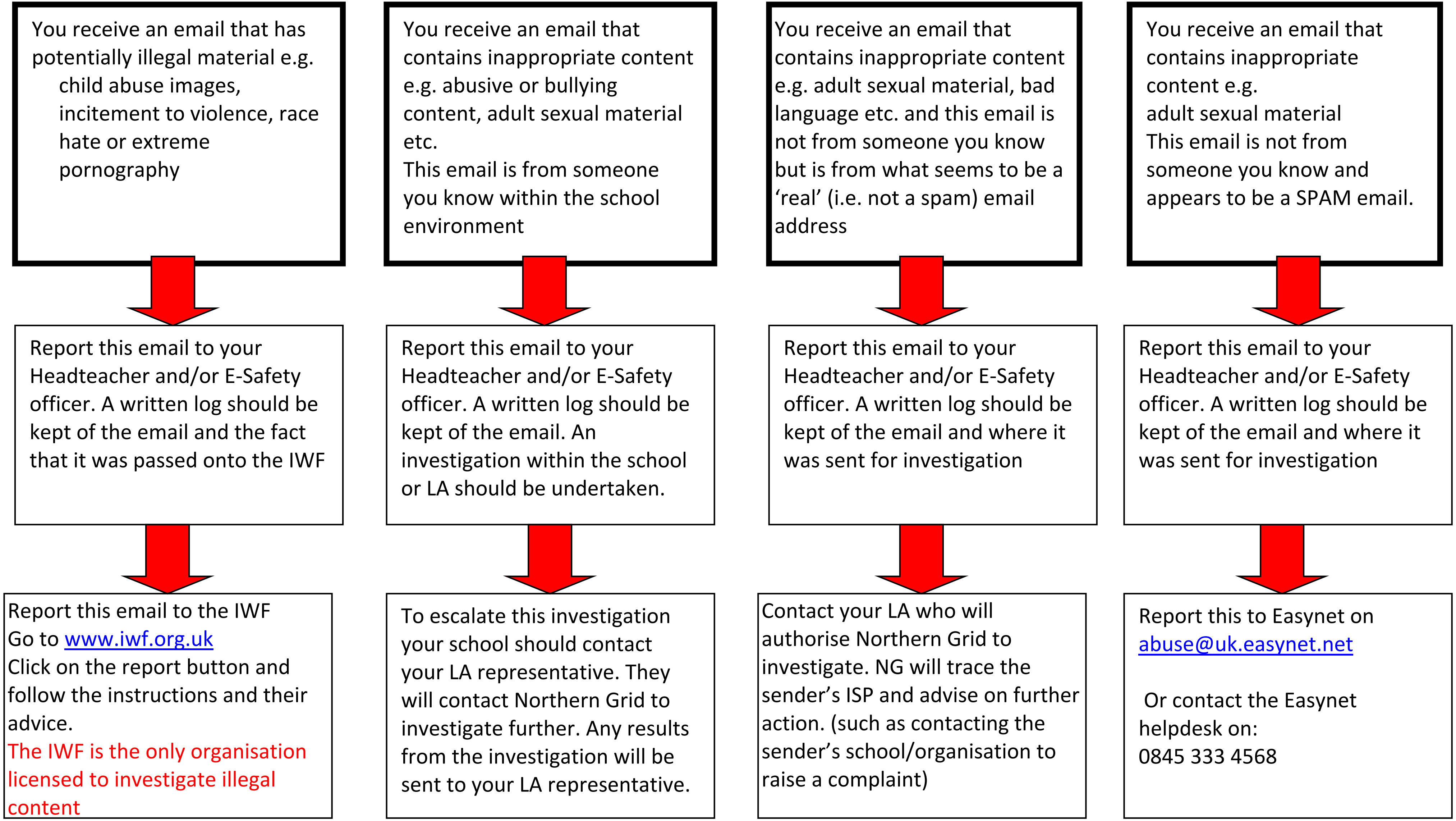
Opening an attachment or URL that proves to hold illegal content **is an illegal act** and is classed as possession of illegal material

Never show or email a URL to anyone else if you suspect that it contains illegal material – you will be committing an illegal act
Never personally investigate

Never personally investigate. If you open illegal content accidentally report it to the Headteacher and IWF. Go to the IWF website and click on the report button. **Do not copy and paste the URL, write it down and type it into the reporting screen. This prevents accidental opening**. Once the site has been logged and reported to the IWF delete it from your PC. If you are unsure, contact the IWF for advice on 01223 237 700. **The Internet Watch Foundation only deals with illegal content please see their website for information and advice. Please note this guidance only relates to illegal content not inappropriate.**

ST PATRICK'S
Catholic College

What to do with Suspicious Email – Staff Version



You receive an email that has potentially illegal material e.g.
child abuse images, incitement to violence, race hate or extreme pornography

Report this email to your Headteacher and/or E-Safety officer. A written log should be kept of the email and the fact that it was passed onto the IWF

Report this email to the IWF
Go to www.iwf.org.uk
Click on the report button and follow the instructions and their advice.
The IWF is the only organisation licensed to investigate illegal content

You receive an email that contains inappropriate content e.g. abusive or bullying content, adult sexual material etc.
This email is from someone you know within the school environment

Report this email to your Headteacher and/or E-Safety officer. A written log should be kept of the email. An investigation within the school or LA should be undertaken.

To escalate this investigation your school should contact your LA representative. They will contact Northern Grid to investigate further. Any results from the investigation will be sent to your LA representative.

You receive an email that contains inappropriate content e.g. adult sexual material, bad language etc. and this email is not from someone you know but is from what seems to be a 'real' (i.e. not a spam) email address

Report this email to your Headteacher and/or E-Safety officer. A written log should be kept of the email and where it was sent for investigation

Contact your LA who will authorise Northern Grid to investigate. NG will trace the sender's ISP and advise on further action. (such as contacting the sender's school/organisation to raise a complaint)

You receive an email that contains inappropriate content e.g.
adult sexual material
This email is not from someone you know and appears to be a SPAM email.

Report this email to your Headteacher and/or E-Safety officer. A written log should be kept of the email and where it was sent for investigation

Report this to Easynet on
abuse@uk.easynet.net

Or contact the Easynet helpdesk on:
0845 333 4568

In all cases secure the email in a folder and only delete when the investigation has been completed or you are advised to do so.

In the case of potential illegal material do not show the content of this email to anyone but report it to your Headteacher and take the advice of the Internet Watch Foundation.

Do NOT always presume that the sender's email address is telling you the truth – Spammers can and do fake other's email addresses. If you are unsure how to proceed please contact the Northern Grid for Learning on 0191 4611844

ST PATRICK'S
Catholic College

E-Safety Incident Log

Details of all e-Safety incidents will be recorded by the e-Safety co-ordinator. This log will be monitored termly and reported to the School Improvement Committee of the Governing Body. Any incidents involving Cyberbullying will be additionally recorded and reported on the separate Bullying or Racist Recording Forms.

Date and Time	Name of Student or member of Staff	Male or Female	Room and Device	Details of Incident (including evidence base)	Actions and Reasons for those actions

Smile and Stay Safe Poster

e-Safety Rules to be displayed in all areas of the school

SMILE AND STAY SAFE

Staying safe means keeping your personal details private, including your full name, phone number, home address, photos or school. Never reply to requests for ASL (age, sex, location)

Meeting 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.

Information 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'

Let 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.

Emails, downloads, MSN 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.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (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 e-Safety

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.

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 persons 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 them 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 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.

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 last two occasions, that violence will be used against them, 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.

Approved by Governors initially:	October 2012
Reviewed:	June 2017
Review approved by Governors:	July 2017