Ingleby Manor Free School & Sixth Form
E-Safety Policy

Adopted:	15th September 2014
Reviewed date:	21st September 2016
Review Date:	21st September 2018

1 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, academies and free 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.

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
- E-mail 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 webbased 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 Ingleby Manor Free School**,** 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 Agreement (for all staff, governors, visitors and students) are inclusive of both fixed and mobile internet; technologies provided by the School (such as PCs, laptops, personal digital assistants (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, PDAs and portable media players, etc.).

2 Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the School, the Principal 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 Zoe Matthewman 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 Borough Council, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.
Senior Management and Governors are updated by the Principal/ 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 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 SMSC.

3 eSafety skills development for staff

- Our staff receive regular information and training on e-Safety issues in the form of staff training days, bulletins and e-mails.
- Details of the ongoing staff training programme can be accessed through the CPD coordinator
- New staff receive information on the School’s acceptable use policy as part of their induction.
- All staff have been 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.)
- All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas.

4 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 policy will be introduced to the students at the start of each School year.
- E-safety posters will be prominently displayed.

5 E-Safety in the Curriculum

- The School has a framework for teaching internet skills in cross-curricular and SMSC lessons □ The School provides opportunities within a range of curriculum areas to teach 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 the 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 activities.
- Students are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. Learning mentors, parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button.
- Students are taught to critical evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum

6 Password Security

- 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 log-in username. From Year 7 they 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.
- If Users think their password may have been compromised or someone else has become aware of their password, they must report this to Zoe Matthewman or a House Tutor
- Staff are aware of their individual responsibilities to protect the security and confidentiality of School networks and/or Learning Platforms, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.
- In our School, all ICT password policies are the responsibility of SPTA Core Team and all staff and students are expected to comply with the policies at all times.

7 Data Security

The accessing 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. They must not;

- access data outside of School, except when entering assessment data
- take copies of the data
- allow others to view the data
- edit the data unless specifically requested to do so by the Principal and/ or Governing Body.
- Leave open SIMS for students to view.
- Staff must always lock their workstations when leaving the classroom.
- No student should be allowed to use the classroom PC.
- Staff passwords should always be kept safe and never shared with others.

8 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 internet access in the School 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.
- Raw image searches are discouraged when working with students.
- If internet research is suggested for independent study, students will be accessing specific sites that have been authorised via the SPTA's Firewall. If a school tablet is used at home, internet searches are diverted through the SPTA servers and as such will give appropriately restricted access, however, we recommend that parents supervise any further research and ask that that any concerns are communicated to the School.
- 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.

9 Infrastructure

- Ingleby Manor Free School has a monitoring solution via the onsite Smoothwall software, where webbased activity is monitored and recorded.
- School internet access is controlled through the School's web filtering service. This is the responsibility of ICT support and SPTA core team.
- Ingleby Manor Free 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 students are aware that School based e-mail and internet activity can be monitored and explored further if required.
- The School does not allow students access to internet logs.
- The School uses management control tools 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.
- It is the responsibility of the School, 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. It is not the School's responsibility to install or maintain virus protection on personal systems. If students wish to bring in work on removable media it must be given to the teacher for a safety check first.
- Students and staff are not permitted to download programs or files on School based technologies without seeking prior permission from the ICT technician.
- If there are any issues related to viruses or anti-virus software, ICT support should be informed

10 Managing other Web 2 technologies

Web 2/ social networking sites, if used responsibly both outside and within an educational context, can provide easy to use, creative 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 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, IM/ e-mail address, specific hobbies/ interests).
- Our 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 to the School.
- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with students using the VLE or other systems approved by the Principal.
- Staff are advised to not have links to previous students for a minimum of 15v years after leaving that education establishment.
- Staff are advised not to engage with social media links with parents.
- Staff must not discuss school matters or bring school into disrepute via web2 technologies/social media.

11 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, PDAs, gaming devices, mobile and smart phones 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.

12 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 unless in extreme emergencies (off site trips etc.)
- Students are allowed to bring personal mobile phones to School on the understanding that they remained switched off during school hours (8.30-4.30) and are kept securely in school bags.

- The School is not responsible for the loss, damage or theft of any personal mobile device.

13 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, laptops and PDAs for offsite visits and trips, only these devices should be used.
- Where the School provides a laptop for staff, this device may only be used to conduct School business in or outside of School.

14 Managing e-mail

The use of e-mail within most academies and free schools is an essential means of communication for both staff and students. In the context of School, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between School's on different projects, be they staff based or pupil based, within School or international. We recognise that students need to understand how to style an e-mail in relation to their age and good 'netiquette'. In order to achieve ICT level 4 or above, students must have experienced sending and receiving e-mails.

- The School gives all staff their own e-mail account to use for all School business. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk 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 e-mail histories can be traced. This should be the account that is used for all School business.
- Under no circumstances should staff contact students, parents or conduct any School business using personal e-mail addresses.
- The School requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the School. The responsibility for adding this disclaimer lies with the account holder.
- 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.
- Staff sending e-mails to external organisations, parents or students are advised to cc. the Principal or their line manager.
- Students may only use School approved accounts on the School system and only under direct teacher supervision for educational purposes.
- All students have their own individual School issued account.
- The forwarding of chain letters is not permitted in School.
- All e-mail 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 e-mail communication, or arrange to meet anyone without specific permission, 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/ line manager) if they receive an offensive e-mail.
- Students are introduced to e-mail as part of the cross-curricular ICT work in School

15 Safe Use of Images

15.1 Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. 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 students) and staff, the School permits the appropriate taking of images by staff and students with School equipment.
- Staff are not 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 the express permission of the Principal, 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 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 Principal, images can be taken provided they are transferred immediately and solely to the School's network and deleted from the students device.

15.2 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.

15.3 Publishing pupil's images and work

On a child's entry to the School, parents/guardians 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 (Sharepoint)
- 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 the person with parental responsibility to be valid.

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. No photos should be uploaded to website or put in any publications without prior checking with the main office.

15.4 Storage of Images

- Images/ films of children are stored on the School's network
- 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 Principal
- Rights of access to this material are restricted to the teaching staff and students within the confines of the School network/ Learning Platform.

15.5 Webcams and CCTV

- The School uses CCTV for secure and safe access. The only people with access to this are the Office Manager and SLT.
- Webcams in the School and cameras on our iboards will only ever be used for specific learning or training purposes.
- Misuse of a webcam or camera by any member of the School community will result in sanctions (as listed under the ' inappropriate materials' section of this document)
- Consent is sought from parents/carers and staff on joining the School, in the same way as for all images.

15.6 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 students are supervised by a member of staff when video conferencing
- All students are supervised by a member of staff when video conferencing with end-points beyond the School.
- The School keeps a record of video conferences, including date, time and participants.
- Approval from the Principal 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.

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be DBS checked.
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

16 Misuse and Infringements

16.1 Complaints

Complaints relating to e-Safety should be made to the e-Safety co-ordinator or Principal. Incidents should be logged.

16.2 Inappropriate material

- All users are 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 Principal/ Governors, immediate sanctions, possibly leading to exclusion/dismissal and involvement of police for very serious offences
- Users are made aware of sanctions relating to the misuse or misconduct through inductions (staff), ICT sessions (students).

17 Equal Opportunities

17.1 Students with additional needs

The School endeavours to create a consistent message with parents for all students and this in turn should aid establishment and future development of the School's' e-Safety rules. However, staff are aware that some students may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety. Internet activities are planned and well managed for these children and young people.

17.2 Parental Involvement

- Parents/ carers and students are actively encouraged to contribute to adjustments or reviews of the School e-Safety policy by accessing the policy via the School website.
- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to School.
- 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 e-Safety where appropriate in the form of; □ Information and celebration evenings
- Posters
- Website/ Learning Platform postings
- Newsletter items
- Learning platform training

18 Writing and Reviewing this Policy

18.1 Approval and Review Procedure

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

This policy will be reviewed every year and consideration given to the implications for future whole School development planning. The Education Advisory Board will assess its implementation and effectiveness. The policy will be promoted and implemented throughout the School.

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

Signed ____ *Mr D Willard* **(Principal)**

Date ____

Signed ____ *Mr M Thorpe* **(Chair of EAB)**

Date ____

Ingleby Manor
School & Sixth Form

Acceptable Use Agreement: Staff, Governors and Visitors

Ingleby Manor Free School Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as e-mail, 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. I will only use the School's e-mail / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal or Governing Body.

- 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 students and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to students.
- I will only use the approved, secure e-mail system(s) for any School business.
- 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.
- I will not install any hardware of software without permission of the ICT technician.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of students and/ or staff will only be taken, stored and used for professional purposes in line 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 Principal.
- 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 Principal.
- 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 students 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 ……………………………......................................Ingleby Manor Free School & Sixth Form

Ingleby Manor
School & Sixth Form

Acceptable Use Agreement: Students

Ingleby Manor Free School Acceptable Use Agreement / e-Safety Rules

- I will only use ICT systems in School, including the internet, e-mail, 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/ Learning Platform with my own user name and password.
- I will follow the School's ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my School e-mail address.
- I will make sure that all ICT communications with students, 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 students and/ or staff will only be taken, stored and used for School purposes in line with School policy and not be distributed outside the School network without the permission of the Head teacher.
- I will ensure that my online activity, both in School and outside School, will not cause my School, the staff, students 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 or the Police may be contacted.

<u>Dell Tablet Devices</u>

As a School we are keen to promote individual tablet device usage as we believe these devices will aid learning and promote progress. Below is an outline of our expectations for their day to day care.

- All students will be issued with an 8" Dell Tablet to support their learning
- Each device will have a heavy duty cover – this must not be removed
- Devices should be treated with respect and care taken to avoid damage
- Devices can be taken home but must be charged ready for use the next day
- If a device is accidentally damaged the School will, within reason, seek to repair within 5 days
- If a student repeatedly mistreats the device leading to multiple instances of damage then the School reserve the right to retain the device on site and only issue during lesson time
- If a student repeatedly leaves the device at home then the School reserves the right to retain the device on site to ensure it can be used for learning when needed
- If a device is deliberately damaged the School reserves the right to charge the cost of repair or replacement.

Dear Parent/ Carer

ICT including the internet, learning platforms, e-mail and mobile technologies have become an important part of learning in our School. We expect all students to be safe and responsible when using any ICT. It is essential that students are aware of e-Safety and know how to stay safe when using any ICT. Students are expected to read and discuss this agreement with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their class teacher or Sarah Gill (School e-Safety coordinator).

Please complete the bottom section of this form and return it to the School for filing.

Pupil and Parent/ carer signature

We have discussed this document and ……………………………………..........(pupil name) agrees to follow the e-Safety rules and to support the safe and responsible use of ICT at Ingleby Manor Free School & Sixth Form.

Parent/ Carer Signature …….…………………….……………………….

Pupil Signature……………………………………………………………….

Form …………………………………. Date ………………………………

Relevant Legislation

Acts relating to monitoring of staff e-mail

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 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. Academies should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

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 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 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.