All Saints Catholic College

E- Safety Policy

Approved by Governors: 19th June 2017

Date to be next reviewed: June 2018

Introduction

At All Saints, our mission statement states ‘ We are a Catholic community dedicated to providing an excellent education to all of our pupils so that they fulfil their ambitions and exceed their expectations.
We work together as a family through mutual respect so that everyone succeeds academically and grows spiritually.’
In regard to this, we will endeavour to ensure that our students are safeguarded and protected in all aspects of their education but allowed to utilise and embrace the latest technology.
This policy should be read in reference to :

- The Child Protection (Safeguarding) Policy
- The Anti Bullying Policy

Rationale

This policy provides guidance on e-safety for All Saints Catholic College. The focus of the policy is to ensure that existing policies are applied to the digital environment. This policy is reviewed annually in line with current e-Safety guidance.

e-Safety is defined as all fixed and mobile technologies that children and young people may encounter, now and in the future, which allows them access to content and communications that could raise e-safety issues or pose risks to their wellbeing and safety.

Safeguarding children and young people, including e-safety, is everyone’s responsibility; e-safety is not a responsibility for just ICT staff. It needs to be considered as part of the overall arrangements in place that safeguard and promote the welfare of children and young people.

e-Safety covers any issues relating to any communications using the Internet, mobile phones or other electronic communications technologies that can pose risks to a person’s well-being or safety.

General statement

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at

any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any ICT authorised staff member will be happy to comply with this request.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the email or voicemail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

The Policy

Acceptable Use Policy

All students, parents and staff are expected to read and sign the Internet Safety statement located in the pupil journal. This statement identifies what is expected from the pupils with regards the acceptable, safe and responsible use of on-line technologies. All Saints Catholic College students and parents sign the statement at the start of an academic year.

This policy has been updated with reference to the document 'Keeping children safe in education' (Sept 2016).

Acceptable Use Agreement: Pupils - Secondary

- I will only use ICT systems in school, including the internet, email, digital video, and mobile technologies for school purposes
- I will not download or install software on school technologies
- I will only log on to the school network, other systems and resources 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 email address
- I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use
- I will not 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
- I am aware that when I take images of pupils and/ or staff, that I must only store and use these for school purposes in line with school policy and must never distribute these outside the school network without the permission of all parties involved. This includes school breaks and all occasions when I am in school uniform or when otherwise representing the school
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring the school community into disrepute, including through uploads of images, video, sounds or texts
- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community
- I will respect the privacy and ownership of others' work on-line at all times

- I will not attempt to bypass the internet filtering system
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted
- I will not bring a Smart Watch to school because I am not permitted to wear one during the school day
- I will not sign up to online services until I am old enough to do

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

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

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Head 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 pupils and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to pupils
- I will only use the approved, secure email system(s) for any school business
- I will ensure that personal data (such as data held on MIS software) 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. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop or memory stick
- I will not install any hardware or software without permission of XXX
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes 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 Headteacher
- I will support the school approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community'
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies
- I will not use personal electronic devices (including smart watches) in public areas of the school between the hours of 8.30am and 3.30pm, except in the staff room and where there are signs to indicate this.
- I understand this forms part of the terms and conditions set out in my contract of employment

User Signature

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

Signature …… Date ……

Full Name …….... (printed)

Job title ……

Safety Lead

All Saints Catholic College has an e-safety lead person (Head of ICT) and a Deputy Safeguarding Lead (Deputy Head)who have both produced this policy.

- Ensuring that the organisation's policies and procedures include aspects of e-safety. For example: the anti-bullying procedures include cyber bullying and the child protection policy includes internet grooming
- Monitoring the effectiveness of the filter system provider to it is set at the correct level for staff, children and young people
- Report issues to the head of the organisation
- Ensure that staff participate in e-safety training
- Ensure that e-safety is included in staff induction

Concerns, issues or any matters arising MUST be reported to the Designated Safeguarding Lead (DSL) who is the Deputy Head, who will advise the safety lead where appropriate.

Incident Reporting, eSafety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person or eSafety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your Information Asset Owner.

Misuse and Infringements

Complaints

Complaints and/ or issues relating to eSafety should be made to the eSafety co-ordinator or Headteacher or Designated Safeguarding lead as appropriate should be followed.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation by the Headteacher Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)
- Users are made aware of sanctions relating to the misuse or

Managing Incidents

Any incident where it is considered a child or young person is at risk will be responded to in line with Tameside Safeguarding Children Boards Safeguarding procedures and referred to the Tameside Hub.

The Deputy Headteacher in the first instance followed by the Assistant Head of Pastoral / e-Safety lead will ensure that these procedures are followed in the event of any misuse of the internet.

The Risks

The table below identifies the key risks that students may encounter using the internet and/or ICT equipment

	Commercial	Aggressive	Sexual	Values
Content (child as recipient)	Adverts Spam Sponsorship Personal info	Violent/hateful content	Pornographic or unwelcome sexual content	Bias Racist Misleading info or advice
Contact (child as participant)	Tracking Harvesting personal info	Being bullied, harassed or stalked	Meeting strangers Being groomed	Self-harm Unwelcome persuasions
Conduct (child as actor)	Illegal downloading Hacking Gambling Financial scams Terrorism	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading info/ advice

This table includes reference to items that may come under the Prevent agenda.

Inappropriate Contact

1. Report to the DSL/ Deputy Headteacher in the first instance or to Assistant Head for Pastoral/ e-Safety lead using the YELLOW/GOLD Safeguarding Children Record Form. This form must be handed to them directly.
2. The Assistant Head Pastoral/E Safety Lead MUST discuss the matter with the DSL who will then implement the relevant actions
3. Advise the child or young person on how to terminate the communication and save all evidence
4. Contact the child or young person's parent(s) / carer(s)
5. Log the incident
6. Identify support for the child or young person
7. Contact the police

Bullying

1. Report to the Assistant Head of Pastoral Care / Head of Year who will discuss the matter with the DSL (Deputy Head). It may be necessary to complete a the YELLOW/GOLD Safeguarding Children Record Form. They will implement the next stages for action.
2. In the immediate stage advise the child or young person not to respond to the message
3. Refer to relevant policies including anti-bullying, e-safety and apply appropriate sanctions
4. Secure and preserve any evidence
5. Contact the child or young person's parent(s) / carer(s) – in discussion with Assistant Head of Pastoral/ HOY/ DSL (Deputy Head)
6. If appropriate, a discussion about informing the police will be had. This will depend on the severity or repetitious nature of the offence . An identified staff member will be appointed to make this call.
7. Log the incident
8. Identify support for the child or young person

Malicious/Threatening Comments Towards a Child, Young Person or Organisation Staff

1. Report to the Assistant Head of Pastoral Care / Head of Year who will discuss the matter with the DSL (Deputy Head). It may be necessary to complete a the YELLOW/GOLD Safeguarding Children Record Form. They will implement the next stages for action.
2. Secure and preserve any evidence
3. In the case of offending web-based e-mails being received, capture / copy "the header" info, if possible.
4. Inform and request that the comments are removed from the site / block the sender
5. If appropriate, an identified member of staff will report the matter to the police
6. Log the incident
7. Identify support for the child or young person

Safeguarding Issues

DEALING WITH A CONCERN YOU HAVE REGARDING A CHILD– ADVICE FOR ALL MEMBERS OF STAFF

If you witness behaviour that causes you concern, or note that a child has accessed inappropriate material (ie. Pornography, extreme radicalised material), have concerns about the actions of a child or the comments they are making or have been told that this is potentially the case with a child the member of staff or volunteer should follow this guidance.

- Report to the Assistant Head of Pastoral Care / Head of Year who will discuss the matter with the DSL (Deputy Head). It may be necessary to complete a the YELLOW/GOLD Safeguarding Children Record Form. They will implement the next stages for action.
- If illegal the matter will be reported to the police by an identified member of staff (likely DSL/ Assistant Head of Pastoral)

- If illegal images have been viewed (child pornography/ extreme pornography) a member of staff or the police should seize the computer to ensure that evidence can be preserved so that it can be presented in a court of law at a future date if necessary. Even as part of an investigation staff *should not* view images of child pornography or extreme pornography as it is illegal
- Inform the parents
- Contact the filtering software provider / IT section to notify them of the websites viewed
- Decide on an appropriate sanction
- Log the incident in full
- Identify support for the child or young person

DEALING WITH A CONCERN YOU HAVE REGARDING ANOTHER ADULT – ADVICE FOR ALL MEMBERS OF STAFF

If you witness behaviour that causes you concern, or note that an adult in the community has accessed inappropriate material (ie. Pornography, extreme radicalised material), have concerns about the actions of an adult in the community or the comments they are making or have been told that this is potentially the case with an adult in the community, the member of staff or volunteer should follow this guidance.

Viewing of Inappropriate / Illegal Websites

- Report to the matter to the DSL (Deputy Head) or Headteacher ONLY.
- The Headteacher and DSL will discuss the matter with the Finance Manager
- If illegal images have been viewed (child pornography/ extreme pornography) a member of staff or the police should seize the computer to ensure that evidence can be preserved so that it can be presented in a court of law at a future date if necessary. Even as part of an investigation staff *should not* view images of child pornography or extreme pornography as it is illegal
- Contact the filtering software provider / IT section to notify them of the websites viewed
- Decide on an appropriate action and follow relevant procedures
- Log the incident in full

If a staff member inadvertently or accidently accesses inappropriate materials then they should inform the DSL or Headteacher immediately.

Computer Viruses

- All files downloaded from the Internet, received via email or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.

- Never interfere with any anti-virus software installed on school ICT equipment.

- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team.

- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

email

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

Staff and governors should use a school email account for all official communication to ensure that children are protected through the traceability of all emails through the school email system. In addition, it is important that governors are protected against possible allegations of inappropriate contact with children. This is to help mitigate the chance of issues occurring and is an essential element of the safeguarding agenda.

Managing email

- The school gives all staff & governors their own email account to use for all school business as a work based tool This is to protect staff, minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed

- Staff & governors should use their school email for all professional communication.

- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. The school email account should be the account that is used for all school business

- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses

- All emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper

- Staff sending emails to external organisations, parents or pupils are advised to cc line manager or designated line manager and, if relevant, the Heaadteacher

- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes

- Emails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your email account as follows:

    - Delete all emails of short-term value

- Organise email into folders and carry out frequent house-keeping on all folders and archives

- The following pupils have their own individual school issued accounts ***(list groups of children or individuals)***, all other children use a class/ group email address

- The forwarding of chain emails is not permitted in school.

- All pupil email users are expected to adhere to the generally accepted rules of responsible online behaviour particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission, virus checking attachments

- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting email

- Staff must inform (the eSafety coordinator or line manager) if they receive an offensive email

- Pupils are introduced to email as part of the Computing Programme of Study

- However you access your school email (whether directly, through webmail when away from the office or on non-school hardware) all the school email policies apply

Sending emails

- If sending emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section **Error! Reference source not found.**

- Use your own school email account so that you are clearly identified as the originator of a message

- Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate

- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments

- School email is not to be used for personal advertising

Receiving emails

- Check your email regularly

- Activate your ‘out-of-office’ notification when away for extended periods

- Never open attachments from an untrusted source; consult your network manager first
- Do not use the email systems to store attachments. Detach and save business related work to the appropriate shared drive/folder
- The automatic forwarding and deletion of emails is not allowed

Equal Opportunities

Pupils with Additional Needs

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

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

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

eSafety

eSafety - Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this school is **Mr Gus Diamond** 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 eSafety co-ordinator to keep abreast of current issues and .

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

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, 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 PSHCE.

eSafety in the Curriculum

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

- The school provides opportunities within a range of curriculum areas to teach about eSafety
- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the eSafety curriculum
- Pupils 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
- Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or the 'CEOP report abuse' button

e-Safety Action Plan

1. **Raise awareness and understanding of e-safety issues amongst children and young people**

Make e-safety a talking point for children and young people inside and outside the school environment Make staff aware of the latest issues relating to young people	Participate in the international Safer Internet day – second week in February Use the "Think you know" resources for starters / plenary's in ICT lessons The inclusion of e-safety questions (cyber bullying) on any wider anti-bullying surveys and questionnaires. Unit of Work to be delivered during core Computing lessons based on e-safety in Years 7,8 and 9. Staff to receive up to date training on e-safety matters.
Increase awareness of resources that support children to behave safely on-line	http://www.thinkuknow.co.uk/11_16/

2. **Raise Awareness and understanding of E-safety issues amongst parents and carers**

Improve levels of awareness amongst parents and cares of the risks posed to children and young people by their use of technology. Improve levels of awareness of parents and carers of ways of mitigating the risks posed to children and young people. Improve awareness amongst parents and carers of available resources in this area	Host a Parents / Carers Event about Internet Safety Provide a link to e-Safety resources from the College website. https://www.thinkuknow.co.uk/parents/Secondary/

Internet Access

The internet is an open worldwide communication medium, available to everyone, 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 use through XXXX is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

- The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity
- Staff will preview any recommended sites, online services, software and apps before use
- Searching for images through open search engines is discouraged when working with pupils
- 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 further research
- 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

---

Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience
- Do not reveal names of colleagues, pupils, others or any other confidential information acquired through your job on any social networking site or other online application
- On-line gambling or gaming is not allowed

It is at the Headteacher's discretion as to what internet activities are permissible for

Managing Other Online Technologies

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

- At present, the school endeavors to deny access to social networking and online games websites to pupils within school
- All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
- Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online
- Our pupils are asked to report any incidents of Cyberbullying to the school
- Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school learning platform or other systems approved by the Headteacher
- When signing up to online services that require the uploading of what could be deemed as **personal or sensitive** **data**, schools should check terms and conditions regarding the location of storage.

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting eSafety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

- Parents/carers and pupils are actively encouraged to contribute to adjustments or reviews of the school eSafety policy by contacting school if they immediately come across an issue or suspect an issue

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website)

- Parents/carers are expected to sign a Home School agreement contained within the student journal

- The school will endeavor to disseminate information to parents relating to eSafety where appropriate

Remote Access

- You are responsible for all activity via your remote access facility
- Only use equipment with an appropriate level of security for remote access
- To prevent unauthorised access to school systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone
- Select PINs to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment

Current Legislation

Acts Relating to Monitoring of Staff email

Data Protection Act 1998

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

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

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

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to eSafety

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

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 (email) 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 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.

Acts Relating to the Protection of Personal Data

Data Protection Act 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 2000

https://ico.org.uk/for-organisations/guide-to-freedom-of-information/

Counter-Terrorism and Security Act 2015 (Prevent), Anti-Radicalisation & Counter-Extremism Guidance

https://www.gov.uk/government/publications/preventing-extremism-in-schools-and-childrens-services