Marsh Hill Primary School

Online Safety Policy

Date policy reviewed: 1st March 2023

Date Adopted by Governing Board

Signed by:

____________________ Head teacher Date: ____________________

____________________ Chair of governors Date: ____________________

PAUL BASIL VICE CHAIR

21/3/2023

J. Cusack

21/03/23

Guidance
Once this policy has been ratified by the School's Governors it should be issued to all personnel, including Governors and pupils involved in the working of the school.

The Acceptable Use of ICT Agreement should be issued to the appropriate user for signature and collated by a designated member of staff.

Our Vision
Marsh Hill Primary School embraces the positive impact and educational benefits that can be achieved through appropriate use of the internet and associated communications technologies. We are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. To that end, Marsh Hill Primary School aims to provide a safe and secure environment which not only protects all people on the premises but also educates them on how to stay safe in the wider world.

1. Introduction

1.1 The governing board of Marsh Hill Primary School has adopted this policy to help the school meet its responsibilities for safeguarding and educating children, for regulating the conduct of employees and for complying with legislation covering the use of information and communication technologies and digital and mobile devices.

1.2 This policy was adopted by the governing board on 9th December 2015 and will be **reviewed annually** in the light of guidance from the local authority or earlier if the local authority issues further guidance in the light of particular circumstances or developments in information and communication technology.

2. Basic principles

2.1 In adopting this policy the governing board has taken into account the expectation by Ofsted that rigorous Online Safety policies and procedures are in place in the school, written in plain English, with contributions from the whole school, updated regularly and ratified by governors.

2.2 The policy applies to all members of the school community, including staff, pupils, volunteers, parents and carers, governors, visitors and community users who have access to, and are users of, the school's information and communication technology systems or who use their personal devices in relation to their work at the school.

2.3 The governing board expects the head teacher to ensure that this policy is implemented, that training in Online Safety is given high priority across the school, that consultations on the details of the arrangements for Online Safety continue with all employees on a regular basis, and that any necessary amendments to this policy are submitted to **the governing board or designated committee for approval**.

2.4 The principal context for this policy is the need to safeguard children. It will be applied in conjunction with the procedure for safeguarding children approved by the Birmingham

Safeguarding Children Board. It will also be applied in conjunction with the school's behaviour and anti-bullying policies for pupils and with the rules and procedures governing the conduct of employees.

2.5 The governing board expects the head teacher to arrange for this policy to be published to all employees and volunteers in the school and for necessary instructions and guidance, particularly on acceptable use, to be given to pupils in a manner suited to their ages and abilities.

3. Roles and responsibilities

Governing board

3.1 The governing board will consider and ratify this Online Safety policy, and review it annually in the light of guidance from the local authority, or sooner if the local authority issues new guidance in the light of particular circumstances or developments in information and communication technology. Governors are expected to follow the policy in the same way as volunteers are expected to follow it, including participating in annual Online Safety training if they use information and communication technology in their role as school governors.

3.2 Governors are responsible for ensuring that proper procurement procedures are used if they decide to purchase information technology services from an external contractor and that City Council or other reputable specialist advice is taken on the specification for those services to ensure proper security and safeguarding of children.

Head teacher

3.3 The head teacher is responsible for ensuring that

- the governing board is offered appropriate support to enable this policy and its application to be reviewed regularly, and to ensure that other school policies, including that on pupils' behaviour, Internet access Policy statement and Data Protection, take account of this Online Safety policy;
- the governing board is given necessary advice on securing appropriate information and communication technology systems;
- the school obtains and follows City Council or other reputable guidance on information and communication technology to support this policy;
- the school has an Online Safety Co-ordinator – **Cathy Lomas**. They are the central point of contact for all Online Safety issues and will be responsible for the day to day management. The school has established an Online Safety committee that are responsible for policy review, risk assessments and Online Safety in the curriculum. The current members are: **Cathy Lomas**,(Designated Safeguarding Lead), **Neil Ward** (Academe IT – responsible for IT support) **Rachel Cureton (**ICT Curriculum Lead) and **Nicola Clover** - Assistant Head Teacher
- there is effective consultation with all employees, and other users of the school's information and communication technology systems, to take account of the particular features of those systems and educational, technical and administrative needs;
- the school provides all employees with annual Online Safety training and additional update training, if required, relevant to their roles and responsibilities and that training is also provided to volunteers and school governors who use information

and communication technology in their capacity as volunteers or governors, as the case may be;

- pupils are taught Online Safety as an essential part of the curriculum;
- the senior leadership team is aware of the procedures to be followed in the event of a serious Online Safety incident, including an allegation made against an employee, and that all employees know to whom they should report suspected misuse or a problem.
- The school uses Smoothwall which is monitored regularly by a senior member of staff.
- Records are kept of all Online Safety incidents and that these are reported to the senior leadership team. This is in line with the Child Protection, code of Conduct and On-line Safety Agreements.
- necessary steps have been taken to protect the technical infrastructure and meet technical requirements of the school's information and communication technology systems;
- there is appropriate supervision of, and support for, technical staff;
- any outside contractor which manages information technology for the school undertakes all the safety measures which would otherwise be the responsibility of the school to the standard required by the school and is fully aware of this policy and that any deficiencies are reported to the board which commissioned the contract.

Other employees

3.4 Other employees are responsible for

- undertaking such responsibilities as have been delegated by the head teacher commensurate with their salary grade and job descriptions;
- participating in training in Online Safety provided by the school and in consultations about this policy and about its application, including Online Safety within the curriculum;
- using information and communication technology in accordance with this policy and the training provided;
- reporting any suspected misuse or problem to the person designated by the school for this purpose.

Pupils

3.5 Pupils are expected to use information and communication technology systems and devices as they have been taught and in accordance with the school's behaviour policy and the instructions given to them by staff.

Other users

3.6 Volunteers, including governors, work experience students and teacher students, who help in the school and who use information and communication technology systems and devices in helping the school are expected to

- participate in training in Online Safety provided by the school and in consultations about this policy and about its application, including Online Safety within the curriculum;
- use information and communication technology in accordance with this policy and the training provided;

- report any suspected misuse or problem to the person designated by the school for this purpose.

Parents

3.7 Parents who help in the school as volunteers are covered by 3.6 above. Parents who are not voluntary helpers in the school are nonetheless subject to the law in the event of misuse of information and communication technology.

4. Acceptable use

4.1 The use of information and communication technology should follow the following general principles:

- This policy should apply whether systems are being used on or off the school premises.
- The school's information and communication technology systems are intended primarily for educational use and the management and administration of the school. During work breaks/non-teaching hours, appropriate reasonable personal use is permitted.
- Data Protection legislation must be followed.
- Users must not try to use systems for any illegal purposes or materials.
- Users should communicate with others in a professional manner.
- Users must not disclose their password and they should not write it down or store it where it is possible that another person might steal it. Users must not attempt to use another person's user-name or password.
- Users must report as soon as possible any apparently illegal, inappropriate or harmful material or event to the person designated by the school.
- Staff are required to lock their computer devices - including: desktop computers, laptop computers and interactive displays (when used in PC mode), when unattended.
-

4.2 Employees, volunteers and governors should:

- not open, copy, remove or alter any other user's files without that person's express permission;
- only take and/or publish images of other people with their permission, or, in the case of pupils, the permission of their parents or guardians;
- when recording or publishing such images for educational purposes should not attach to those images any names or other personal information enabling identification;
- as far as possible communicate with pupils and parents only through the school's official communication systems and not publish personal contact details through those systems;
- if they occupy a senior post in which they need to keep e-mail and other messages confidential, ask the school for a separate e-mail address for this purpose;
- if they use personal devices during their work (subject to the agreement of the school in the case of employees), ensure that the systems which they use are secure, protected with passwords and encrypted;
- not use personal social networking sites through the school's information and communication technology systems;

- not open any hyperlinks in, or attachments to, e-mails, unless the source is known and trusted;
- ensure that their data is backed-up regularly in accordance with the rules of the school's systems;
- only download or upload large quantities of information if they have permission to do so, in order to avoid overloading the school's systems;
- not try to install any programmes or alter any computer settings unless this is allowed under the rules for the school's information and communication technology systems;
- not deliberately disable or damage any information and communication technology equipment;
- report any damage or faults to the appropriate member of staff.

5. Education and training

5.1 Education and training in Online Safety will be given high priority across the school.

5.2 The education of pupils in Online Safety is an essential part of the school's Online Safety provision. A planned online safety education programme takes place through both discreet lessons and wider curriculum opportunities. The school currently uses **Active Learn and Purple Mash.**

5.3 The school will offer education and information to parents, carers and community users of the school about Online Safety via leaflets, newsletters, workshops and signposting on the school website.

5.4 Suitable training will be provided through the school for all employees, as part of induction and subsequently during their employment in the school. There will be a regular review of the training needs of all staff and the content of training should be kept up to date. The training will be linked to training about child protection and data protection. It will cover related matters such as the law on copyright of electronic materials.

5.5 Volunteers and governors who use information and communication technology during their work will be offered the same training as employees.

6. Data Protection

6.1 The school will ensure that its information and communication technology systems are used in compliance with current data protection legislation and that all users are annually updated on the school's data protection policy, including the requirement for secure storage of information. (For more details see the Data Protection Policy and **Online Safety Policy**).

7. Technical aspects of Online Safety

7.1 The school will seek to ensure that the information and communication technology systems which it uses are as safe and secure as is reasonably possible by taking reputable advice and guidance on the technical requirements for those systems.

7.2 The school will undertake regular reviews of the safety and security of its information and communication technology systems.

7.3 Particular attention will be paid to secure password protection and encryption for devices located in the school and mobile devices.

7.4 The school's systems will also provide for filtering internet access for all users, preventing access to illegal content, and with additional filtering for different groups of users for inappropriate content.

7.5 The school will ensure that its information and communication technology systems include standard, automated monitoring for illegal materials, profanity, and unsolicited materials (generally known as 'spam'). It should safeguard children and adults against inappropriate use. It should provide the head teacher and senior leadership team with regular reports to indicate whether or not there have been any incidents.

7.6 Additional monitoring may take place as part of an investigation following evidence of apparent misuse.

Dealing with incidents

8.1 Any suspicions of misuse or inappropriate activity related to child protection should be reported as prescribed in the Safeguarding Board's child protection procedures.

8.2 Any suspicions of other illegal activity should be reported to the head teacher, who should take advice from appropriate persons (according to the nature of the suspected activity and the individuals apparently involved) and, depending on the advice and the outcome of preliminary investigations, should report alleged criminal activity to the police and may also instigate disciplinary procedures.

8.3 Suspicions of inappropriate, as distinct from illegal, use of information and communication technology should be reported to the head teacher or other designated member of the senior leadership team for investigation and appropriate action. This may lead to informal management discussions, improved training or, depending on the nature of the alleged misuse, investigation under the disciplinary procedure for employees, or the school's behaviour policy for pupils.

8.4 Any incidents involving pupils misuse of technology either inside or out of school will be recorded and dealt with in accordance with the Behaviour Policy and Safeguarding Policy, see Acceptable Use rules and Internet Access statements.

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: Safeguarding, Health and Safety, Home School Agreement, Positive Behaviour Policy, Anti-Bullying Policy and RSE.

Primary Pupil Acceptable Use

Agreement / Online Safety Rules

- I will only use Technology in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my login passwords.
- I will only open/alter/save/retrieve delete my own files.
- I will make sure that all online contact with other children and adults is done is a safe, responsible and respectful manner in and out of school.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using Technology because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I know that my use of Technology can be checked and that my parent/ carer contacted if a member of school staff is concerned about my online behaviour

Dear Parent/ Carer

Digital Literacy including the internet, e-mail and mobile technologies, has become an important part of learning in our school. We expect all children to be safe and responsible when using any Technology.
Please read and discuss these Online Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation, please contact **Miss Cathy Lomas.**

Parent/ carer signature
We have discussed this and ....(child name) agrees to follow the Online Safety rules and to support the safe use of Technology at Marsh Hill Primary School.

Parent/ Carer Signature ....

Class .... Date ....

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

Technology (including data) 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 Technology. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with **Cathy Lomas** (Online Safety coordinator and Senior Information Risk Owner).

- I will only use the school's email / Internet and any related technologies for professional purposes or for uses deemed "reasonable" by the Head or Governing Board.
- Staff are required to lock their computer when it is unattended.
- I will comply with the technical security measures in place 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 and only via my school based emails.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- 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 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 Board. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware of software without permission of **John Cusack (Head Teacher).**
- 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 on school own devices, stored and used for professional purposes in line with the Online Safety 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 Head teacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school 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 Head teacher.
- 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 Online Safety and Data Protection policies and help pupils and staff to be safe, responsible and respectful in their use of technology.
- I understand this forms part of the terms and conditions set out in my contract of employment.
- If accessing the school WiFi on a personal device during non-teaching hours I

agree to use it in a safe, responsible and respectful manner. I understand that misuse of the school WiFi goes against my professional conduct and will result in disciplinary action.

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 . . . .

Physical Environment / Security

The school endeavors to provide a safe environment for the whole community and we review the network security regularly and monitor who has access to the system consulting with the LA where appropriate.

- Anti-virus software is installed on all computers and updated regularly Central
- filtering is provided and managed by Link2ICT. All staff and students understand that if an inappropriate site is discovered it must be reported to the Online Safety lead leader who will report it to the Link2ICT Service Desk to be blocked. All incidents will be recorded in the Online Safety log for audit purposes.

  Requests for changes to the filtering will be directed to the Online Safety leader in the first instance who will forward these on to Link2ICT or liaise with the Head as appropriate. Change requests will be recorded in the Online Safety log for audit purposes.

  The school uses Smoothwall on all school owned PC, laptops, and iPads to ensure compliance with the Acceptable Use Policies and rules. Pupils use is monitored by John Cusack, Rebecca Leavey and Cathy Lomas; Staff use is monitored by John Cusack.

  All staff are issued with their own username and password for network access. Visitors / Supply staff are issued with temporary ID's and the details recorded in the school office.

  All pupils are issued with their own username and password and understand that this must not be shared.
- School iPads are monitored by Smoothwall. The iPads access the school WiFi system and are therefore subject to the same filtering protection as the school computers.

Mobile / emerging technologies

Teaching staff at the school are provided with a laptop for educational use and their own professional development. All staff understand that the Acceptable Use Policies apply to this equipment at all times.

To ensure the security of the school systems, personal equipment is currently not permitted to be connected to the school network without the permission of the Head Teacher.

Staff understand that they should use their own mobile phones sensibly and in line with school policy.

If pupils bring a mobile phone into school, they understand it must be turned off and handed in to Reception and can be collected at the end of the day.

The Educations and Inspections Act 2006 grants the Head the legal power to confiscate mobile devices where there is reasonable suspicion of misuse and the Head will exercise this right at their discretion

Pictures / videos of staff and pupils should not be taken on personal devices.

New technologies are evaluated and risk assessed for their educational benefits before they are introduced to the school community

E-mail

- The school e-mail system is provided, filtered and monitored for content, language and malware scanning by Link2ICT using intel security and is governed by Birmingham City Council E-mail Use Policy
- All staff are given a school e-mail address and understand that this must be used for all professional communication
- Everyone in the school community understands that the e-mail system is monitored and should not be considered private communication
- Guidance is given to the school community around how e-mail should be structured when using school e-mail addresses
- Staff are allowed to access personal e-mail accounts on the school laptops or PCs outside directed time understand that any messages sent using the school equipment should be in line with the e-mail policy. In addition, they also understand that these messages will be scanned by the monitoring software
- Pupils may be given the opportunity to check their own e-mail on school laptops or PCs outside directed time and understand that any messages sent using the school equipment should be in line with the e-mail policy. In addition, they also understand that these messages will be scanned by the monitoring software. Everyone in the school community understands that any inappropriate e-mails must be reported to the class teacher / Online Safety Lead as soon as possible.

Published content

The Head Teacher takes responsibility for content published to the school web site but delegates general editorial responsibility to **Nicola Clover, Assistant Head**. (Internet Access Statement) Class teachers and Phase Leaders are responsible for the editorial control of work published by their Students.

The school will hold the copyright for any material published on the school web site or will obtain permission from the copyright holder prior to publishing with appropriate attribution.

The school encourages the use of e-mail to contact the school via the school office / generic e-mail addresses / staff e-mail addresses

The school does not publish any contact details for the pupils

The school encourages appropriate, educational use of other Web 2.0 technologies and where possible embeds these in the school web site or creates a school account on the site

Digital Media

We respect the privacy of the school community and will obtain written permission from staff, parents, carers or pupils before any images or video are published or distributed outside the school.

- Photographs will be published in line with the local authority guidance and not identify any individual pupil.
- Only school based equipment will be used for taking images and storing digital images
- Students' full names will not be published outside the school environment Written permission will be obtained from parents or carers prior to pupils taking

part in external video conferencing.

- Students understand that they must have their teacher's permission to make or answer a video conference call.
- Supervision of video conferencing will be appropriate to the age of the pupils. Outside agencies are required to seek permission from the school before publishing images of staff, parents/carers or pupils on their website, such as workshop providers.

Social Networking and online communication

The school constantly reviews the use of social networking sites and online communication and currently allows access to Twitter and YouTube for teaching and communication purposes via the school network or school based devices on educational visits. If staff want to access social media sites during non-contact time they must do so via their own personal devices and not using the school WiFi systems.

Use of social media networks or sites, whether by pupils or employees, should be subject to the same standards as the school would expect for behaviour and conduct generally, (as set out in the school's code of conduct for support staff and the Teachers' Standards for teachers). The school accepts the separation of private life and work and will not concern itself with people's private lives unless it appears that the law has been broken, or that an employee is in breach of contract, or that the school is, or will be, brought into disrepute.

Guidance is provided to the school community on how to use social media sites safely and appropriately. Helping staff to understand that they need to keep their personal and professional life separate and not bring the school into disrepute. Regular updates and staff training sessions include reminders about:

- not publishing personal information
- not publishing information relating to the school community
- how to set appropriate privacy settings
- how to report issues or inappropriate content
- unmoderated chat sites present an unacceptable level of risk and are blocked in school. Pupils are given age appropriate advice and guidance around the use of such sites

Educational Use

School staff model appropriate use of school resources including the internet.
All activities using the internet, including homework and independent research topics, will be tested first to minimise the risk of exposure to inappropriate material
Where appropriate, links to specific web sites will be provided instead of open searching for information
Students will be taught how to conduct safe searches of the internet and this information will be made available to parents and carers
Teachers will be responsible for their own classroom management when using

Technology and will remind pupils of the Acceptable Use Polices before any activity
Staff and students will be expected to reference all third party resources that are used

Online Safety training

There is a program of continuing professional development in place that includes whole school inset, in school support, consultancy and course attendance.
There is an induction process available for new members of staff.
Educational resources are reviewed by subject coordinators and disseminated through curriculum meetings / staff meetings / training sessions
Online Safety is embedded throughout the school curriculum and visited by each year group via the PSHE curriculum.
Pupils are taught how to validate the accuracy of information found on the internet
Parent workshops are available to provide appropriate advice and guidance regularly
Online Safety guidance is published on the newsletter regularly
Online Safety information is provided to Parents regularly through the Parent App Marvellous Me.

Data Security / Data Protection

Personal data will be recorded, processed, transferred and made available in line with the Data Protection Act 1998 (see Data Protection Policy).

Temporary staff

Third party users of school equipment will be advised of the policies, filtering and monitoring that is in place. They will be issued with appropriate usernames and password that will be recorded in the school office.

Equal Opportunities

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

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

Responding to incidents

Inappropriate use of the school resources will be dealt with in line with other school policies e.g. Behaviour, Anti-Bullying and Safeguarding Policy.

Any suspected illegal activity will be reported directly to the police. The Local Authority will also be informed to provide appropriate support and guidance for the school.
Third party complaints, or from parents concerning activity that occurs outside the normal school day, should be referred directly to the Head
Breaches of this policy by staff or pupils will be investigated by the head teacher or online safety leader. Action will be taken under Birmingham City Council's Disciplinary Policy where a breach of professional conduct is identified by the Head Teacher. Where this relates to a pupil the DSL will liaise with MASH for advice. Incidents will be fully investigated and appropriate records made on personal files with the ultimate sanction of summary dismissal reserved for the most serious of cases involving gross misconduct.
All monitoring of staff use will be carried out by at least 2 senior members of staff (Online coordinator and Head Teacher).
Minor student offenses, such as being off-task visiting games or email websites
will be handled by the teacher in situ by invoking the school behaviour policy.
More serious student policy breaches relating to bullying, drugs misuse, abuse and suicide must be reported to the nominated DSL and action taken in line with school anti-bullying and child protection policies. There may be occasions when the police must be involved.
Serious breaches of this policy by students will be treated as any other serious breach of conduct in line with school Behaviour Policy. Referral to Phase Leaders may be appropriate at this level. Phase leaders will also deal with email alerts generated by PCE for students. For all serious breaches, the incident will be fully investigated, and appropriate records made on personal files with the ultimate sanction of exclusion reserved for the most serious of cases.

The Educations and Inspections Act 2006 grants the Head the legal power to take action against incidents affecting the school that occur outside the normal school day and this right will be exercised where it is considered appropriate

Marsh Hill Online Incident Log

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

Review Procedure

There will be an on-going opportunity for staff to discuss with any online safety concerns with online safety leader.

There will be an on-going opportunity for staff to discuss with the SIRO any issue of data security that concerns them.

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

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

Date approved by Governing Board: **21st March 2023**

Next review date: **March 2024**

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 Online 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.

For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)

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

The Computer Misuse Act 1990 (sections 1 – 3)

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 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

http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx

Policies/ Statutory Guidance to be regarded in conjunction with Online Safety

The Safeguarding Policy
Keeping Children Safe in Education 2022
The Prevent Duty - updated 2019
Working Together to Safeguard Children – updated 2019