Blagdon Primary School

Online Safety

Policy

Reviewed by	Computing Lead	June 2019
Approved by	TLA	3rd July 2019
Endorsed by	Full Governors	17th July 2019
Next Reviewed:	Jul 2021	

Rationale

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors and community users) who have access to and are users of school ICT systems.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behavior of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents such as cyber-bullying, which may take place out of school, but are linked to membership of the school.

The school will manage Online Safety as described within this policy and associated behaviour and anti-bullying policies, and will inform parents and carers of know incidents of inappropriate Online Safety behaviour that take place in and out of school.

Development/Monitoring/Review of this Policy

This online safety policy has been developed through contributions from:

- ICT Coordinator
- Head teacher
- Teachers
- Governors
- ICT Technical staff

Consultation with the whole school community has taken place through the following:

- Staff meetings
- Parent and Pupil Questionnaires
- Governors meetings
- Parents evening

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Governing Body on:	
The implementation of this Online Safety policy will be monitored by the:	*ICT co-ordinator* *Head teacher*
Monitoring will take place at regular intervals:	*Termly (Autumn, Winter and Spring terms)*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	*March 2020*

Should serious online safety incidents take place, the following external persons / agencies should be informed:	*Head teacher- Mrs Claire Golding* *ICT Co-ordinator/Online-Safety Co-ordinator- Mrs A Fennell* *ICT Governor-Mr Iain Martin* *ICT Technician- Richard Sheppard* *(Further action will be taken through LA or other agencies when necessary)*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Internal monitoring data for network activity
- Review of school's online-safety scheme of work – future developments
- Comments from children, school staff, parents and carers
- Questionnaires of pupils, parents / carers and school staff

Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- meetings with the ICT co-ordinator
- monitoring of e-safety incident logs
- reporting to relevant Governors committee meetings

Head teacher and Senior Leaders:

- The Head teacher is responsible for ensuring the safety (including Online safety) of members of the school community, though the day to day responsibility for Online safety will be delegated to the ICT co-ordinator.
- The Head teacher / Senior Leaders are responsible for ensuring that the ICT co-ordinator and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Head teacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Head teacher and another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

ICT Co-ordinator/ E-Safety Co-ordinator:

- Take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school online safety policies / documents.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provide training and advice for staff.

- Liaise with the Local Authority.
- Liaise with school ICT technical staff.
- Receive reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Meet regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs.
- Attend relevant meetings.
- Report regularly to Senior Leadership Team and Headteacher.

Network Manager / Technical staff:

The school's ICT Technician is responsible for ensuring:

- That the school's ICT infrastructure is as secure as possible
- Maintaining and informing the online safety leader of issues relating to filtering
- Keep up to date with online safety technical information and update others as relevant
- use of the network is regularly monitored in order that any misuse can be reported to the e-safety leader for investigation
- Ensure monitoring systems are implemented and updated
- All security updates are applied (including anti-virus and Windows)

Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school online safety policy and practices.
- They have read, understood and signed the school Staff Acceptable Use Agreement.
- They report any suspected misuse or problem to the Headteacher, ICT Co-ordinator or ICT Governor for investigation.
- Digital communications with pupils should be on a professional level, i.e. setting and/or reviewing homework tasks, communicating through a Learning Platform.
- Online safety issues are embedded in all aspects of the curriculum and other school activities.
- Pupils understand and follow the school online safety and acceptable use policies.
- They monitor ICT activity in lessons, extra curricular and extended school activities.
- They are aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated person for child protection:

The designated person for child protection should be trained in online safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data.
- Access to illegal / inappropriate materials.
- Inappropriate on-line contact with adults / strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.

Students / pupils:

- Are responsible for using the school ICT systems in accordance with the School Acceptable Use Agreement- this will be signed after completing the Online Safety scheme of work (appropriate to the age group) at the start of each new academic year.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good online-safety practice when using digital technologies out of school.

Parents / Carers :

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, notices on the school website, online activities and websites to support learning and information about online-safety campaigns.

School visitors/ Volunteers:

School visitors and volunteers who regularly access the school ICT systems will be expected to read and sign the School Acceptable Use Agreement before being provided with access to school systems.

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online-safety provision. Children and young people need the help and support of the school to recognise and avoid online-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned online-safety programme should be provided as part of ICT and across the curriculum and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Key online-safety messages should be reinforced as part of a planned programme of assemblies and PSHE activities.
- Pupils should be taught throughout the curriculum to be critically aware of the materials / content they access online and be guided to validate the accuracy of information
- Pupils should be helped to understand the need for School Acceptable Use Policy and be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Rules for use of ICT systems and the internet will be posted in all classrooms and workspaces.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

Education – Parents / Carers

Many parents and carers have only a limited understanding of online-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. “There is a generational digital divide”. (Byron Report).
The school will therefore seek to provide information and awareness to parents and carers through:

- Notices on the school website.
- Letters and newsletters.
- Parents’ evenings.
- Homework activities.
- Referrals to relevant websites.

Education & Training – Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school’s online safety policy and Acceptable Use Agreement.
- The ICT Coordinator will receive regular updates through attending training sessions and by reviewing guidance documents released by BECTA / LA and others.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff meetings and INSET days.
- The ICT Coordinator will provide advice, guidance and training to individuals as required.

Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are involved in ICT, online safety or child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority or other relevant organisations.
- Participation in school training and information sessions for staff or parents.

Technical- Infrastructure, Equipment, Filtering and Monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the online safety technical requirements outlined in the Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance.
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to users will be explained during Online Safety training and displayed on a poster in the ICT suite. They will be reviewed, at least annually, by the Online Safety Coordinator with input from other staff members.
- All users will be provided with a username and password.
- The “master / administrator” passwords for the school ICT system must be available to the online safety coordinator or Head teacher and kept in a secure place (e.g. school safe).
- Users will be made responsible for the security of their username and password. They must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Requests from staff for sites to be removed from the filtered list will be considered by the Online Safety coordinator and Headteacher. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by staff.
- School staff and ICT technical support staff are entitled to monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Agreement.

- An appropriate system is in place for users to report any actual / potential online safety incident; any incidents should be reported to a member of staff who should record the incident in the online safety log. Any incidents recorded in the log should also be raised with the online safety coordinator, KS2 monitor or Headteacher.
- The school infrastructure and individual workstations are protected by up to date virus software.

Curriculum

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Support Provider can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites.
- Staff are allowed to take digital / video images to support educational aims but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.

- Adequate, relevant and not excessive.
- Accurate.
- Kept no longer than is necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- The device must offer approved virus and malware checking software.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school			*					*
Use of mobile phones in lessons				*				*
Use of mobile phones in social time	*							*

Taking photos on mobile phones or other camera devices		*					*	
Use of hand held devices e.g. PDAs, PSPs		*					*	
Use of personal email addresses in school, or on school network		*		*				*
Use of school email for personal emails	*							*
Use of chat rooms / facilities				*				*
Use of instant messaging				*				*
Use of social networking sites				*				*
Use of blogs		*				*		

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored.
- Users must immediately report to the nominated person, in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and they must not respond to any such email.
- Any digital communication between staff and pupils or parents / carers (email, chat, VLE, etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User Actions

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	child sexual abuse images					*

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					*
	adult material that potentially breaches the Obscene Publications Act in the UK					*
	criminally racist material in UK					*
	pornography				*	
	promotion of any kind of discrimination				*	
	promotion of racial or religious hatred				*	
	threatening behaviour, including promotion of physical violence or mental harm				*	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				*	
Using school systems to run a private business					*	
Use systems, applications, websites or other mechanisms that bypass the filtering					*	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					*	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					*	
Creating or propagating computer viruses or other harmful files					*	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					*	
On-line gaming (educational)			*			
On-line gaming (non educational)			*			
On-line gambling					*	
On-line shopping / commerce				*		
File sharing				*		
Use of social networking sites					*	
Use of video broadcasting e.g. YouTube				*		

Responding to incidents of misuse

All members of the school community will be informed about the procedure for reporting online safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
The online safety leader will record all reported incidents and actions taken in the School online safety incident log and in any other relevant areas e.g. bullying or child protection log.
The designated Child Protection officer will be informed of any online safety incidents involving child protection concerns, which will then be escalated in accordance with school procedures.

The school will manage online safety incidents in accordance with the School Behaviour Policy where appropriate.
The school will inform parents and carers of any incidents or concerns in accordance with school procedures.
After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Safeguarding for Schools Adviser, Local Authority Designated Officer or Senior ICT Adviser.

The police will be informed where users visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:-

Child sexual abuse images
Promotion or conduct of illegal acts, under the child protection, obscenity, computer misuse and fraud legislation
Adult material that potentially breaches the Obscene Publications Act in the UK
Criminally racist material

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.
Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.
The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people can not be identified by the use of their names.

Mobile Phones

The use of mobile phones is prohibited within the school grounds.
Visitors: Visitors are required to hand mobile phones and/or camera devices in to the office on arrival.
Pupils: Pupils are prohibited from mobile phones and/or camera devices in school.
Staff: Staff are required to lock mobile phones away in a lockable unit and are only permitted to use these devices within the staff room and the office.

Social Media

Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school/academy or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.
The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.

- Risk assessment.

School staff should ensure that:

- No reference should be made in social media to students/pupils, parents/ carers or school staff
- They do not engage in online discussion on personal matters relating to members relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Legislation

Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an online safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- “Eavesdrop” on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual’s data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject’s rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

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.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes 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.

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.

Protection of Children Act 1978

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

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. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

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. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.