NELSON MANDELA SCHOOL

E-Safety Policy

"An inclusive school putting your child at the heart of learning"

- Nelson Mandela School is committed to working in partnership with the community to ensure the best outcomes for all.
- We strive to remove the barriers which may hinder learning
- We will provide challenge and high expectations and help our children to reach their goals
- We strive to open minds and open doors to support everyone on their lifelong journey of learning.

How We Will Achieve This.

We will:

- ✓ Have Your child at the heart of their learning;
- ✓ Value and support our children, staff and community.
- ✓ Provide a school which is stimulating, safe and secure;
- ✓ Provide consistently high quality teaching and outcomes;
- ✓ Provide resources which are used to provide the best opportunities to succeed;
- ✓ Be forward thinking and acting;
- ✓ Prepare for an ever changing world;
- ✓ Work together to become responsible global citizens;
- ✓ Have everyone achieving their best and giving their best.

The Headteacher is responsible for the E-Safety Policy. It is also managed at school by:

- Nicola Mills – E-Safety Governor and SLT Lead
- Ranjeet Bhachu
- Sarah Naylor – The E Safety Coordinator/ Computing Coordinator
- Mrs Razia Ali (safeguarding)
- Mrs Sabah Ouasker (Computing governor)

This E-Safety Policy was created by the ICT and Computing Team in consultation with the LA and children.

The policy was completed on: **December 15**

The policy was approved by The Full Governing Body on:
Signed: Chair of Governors
Review: Next Review:

The policy is due for review: **Ongoing in response to incidents and current issues**

Responsibilities of the E-Safety Coordinator

- Promote an awareness and commitment to E-Safety throughout the school
- Be the first point of contact in school on all E-Safety matters
- Lead the school E-Safety team
- Create and maintain E-Safety policies and procedures
- Develop an understanding of current E-Safety issues, guidance and appropriate legislation
- Ensure delivery of an appropriate level of training in E-Safety issues
- Ensure that E-Safety education is embedded across the curriculum
- Ensure that E-Safety is promoted to parents and carers
- Ensure that any person who is not a member of school staff , who makes use of the school IT equipment in any context, is made aware of the Acceptable Use Policy
- Liaise with the Local Authority, the Local Safeguarding Children's Board and other relevant agencies as appropriate
- Monitor and report on E-Safety issues to the E-Safety group, the Leadership team and Governors as appropriate
- Ensure that staff and pupils know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable
- Ensure an E-Safety incident log is kept up-to-date (Policy central monitored by SMT and Link2Ict, my concern is monitored SLT)
- Ensure that Good Practice Guides for E-Safety are displayed in classrooms and around the school

Responsibilities of all Staff

- Read, understand and help promote the school's E-Safety policies and guidance

- Read, understand and adhere to the staff Acceptable Use Policy (AUP)
- Take responsibility for ensuring the safety of sensitive school data and information
- Develop and maintain an awareness of current E-Safety issues and legislation and guidance relevant to their work
- Maintain a professional level of conduct in their personal use of technology at all times
- Embed E-Safety messages in learning activities where appropriate
- Supervise pupils carefully when engaged in learning activities involving technology
- Ensure that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable
- Report all E-Safety incidents which occur in the appropriate log and/or to their line manager
- Respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home

Additional Responsibilities of IT Technical team (Ranj and Paddy Bhachu)

- Support the school in providing a safe technical infrastructure to support learning and teaching
- Ensure appropriate technical steps are in place to safeguard the security of the school ICT and Computing system, sensitive data and information. Review these regularly to ensure they are up to date
- At the request of the Leadership team conduct occasional checks on files, folders, email and other digital content to ensure that the Acceptable Use Policy is being followed
- Report any E-Safety-related issues that come to their attention to the E-Safety coordinator and/or leadership team
- Ensure that procedures are in place for new starters and leavers to be correctly added to and removed from all relevant electronic systems

- Ensure that suitable access arrangements are in place for any external users of the schools IT equipment
- Liaise with the Local Authority and others on e-safety issues

Responsibilities of Pupils

- Read, understand and adhere to the pupil Acceptable Use Policy (AUP)and follow all safe practice guidance
- Take responsibility for their own and each others' safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school
- Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home
- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening
- Report all E-Safety incidents to appropriate members of staff
- Discuss E-Safety issues with family and friends in an open and honest way

Responsibilities of Parents and Carers

- Help and support the school in promoting E-Safety
- Read, understand and promote the pupil AUP with their children
- Discuss E-Safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology
- Consult with the school if they have any concerns about their child's use of technology

Responsibilities of Governing Body

- Read, understand, contribute to and help promote the school's E-Safety policies and guidance as part of the schools overarching safeguarding procedures

- Support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in E-Safety awareness
- Ensure appropriate funding and resources are available for the school to implement their E-Safety strategy

Responsibility of any external users of the school systems e.g. adult or community education groups; breakfast or afterschool club

- Take responsibility for liaising with the school on appropriate use of the school's ICT and Computing equipment and internet
- Ensure that participants follow agreed Acceptable Use Procedures

Learning and Teaching

We believe that the key to developing safe and responsible behaviors online for everyone within our school community lies in effective education. We know that the Internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to benefit safely from the opportunities that these present.

We will deliver a planned and progressive scheme of work to teach E-Safety knowledge and understanding and to ensure that pupils have a growing understanding of how to manage the risks involved in online activity. Each class will teach a lesson per half term on e-safety (SWGFL curriculum to support) and the cross curriculum throughout the year.

We believe that learning about E-Safety should be embedded across the curriculum and also taught in specific lessons in ICT and Computing and PSHE.

We will discuss, remind or raise relevant E-Safety messages with pupils routinely wherever suitable opportunities arise.

We will remind pupils about their responsibilities to which they have agreed through the AUP.

Staff and pupils will be reminded that third party content should always be appropriately attributed so as not to breach copyright laws.

How parents and carers will be involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe.

To achieve this we will offer opportunities for finding out more information through school newsletters, website and parent workshops.

We will ask all parents to discuss the pupil's AUP with their child at home.

We request our parents to support the school in applying the E-Safety policy.

We will have advice regarding E-Safety on our Website.

Managing and safeguarding IT Systems

The school will ensure that access to the school IT system is as safe and secure as reasonably possible.

Servers and other key hardware or infrastructure are located securely with only appropriate staff permitted access. Servers, workstations and other hardware and software are kept updated as appropriate. A firewall is maintained and virus and malware protection is installed on all appropriate hardware and is kept active and up-to-date. All computers, laptops owned by the school have virus protection installed.

Any administrator or master passwords for school IT systems are kept secure in the School Safe.

The wireless network is protected by a secure log on which prevents unauthorized access.

We do not allow anyone except technical staff to download and install software onto the network.

We have four different desktops in place, Nursery, Key stage 1, Key stage 2 and Staff all colour coded and with different curriculum software suited to the staff and children's needs.

Filtering Internet access

Web filtering of internet content is provided by LINK2ICT. This ensures that all reasonable precautions are taken to prevent access to inappropriate material. However it is not possible to guarantee that access to unsuitable material will never occur. Teachers are encouraged to check out websites they wish to use. All users are informed about the action they should take if inappropriate material is accessed or discovered on a computer.

FACEBOOK is NOT ALLOWED on any school machines. Staff have access to YOUTUBE, children do not have access to YouTube unless it has been requested for a lesson for a limited period only.

Access

All users have Internet access. The latest Policy Central is installed on all school machines, monitoring safe usage by everyone using the school network. This is monitored on a daily basis by the Head Teacher and the ICT and Computing Operations Manager.

There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to the school who may be granted a temporary log in.

All teachers are provided with a login username and must change password on first login. Pupils are taught about safe practice in the use of their login.

Early years and Key stage 1 children only have a username as access to the network and children in Key stage 2 have a username and password to access the network.

Staff are given appropriate guidance on managing access to laptops which are used both at home and school and in creating secure passwords.

Ipads – see Ipad policy (No 07 and 08)

Access to personal, private or sensitive information and data is restricted to authorized users only, with proper procedures being followed for authorizing and protecting login and password information.

Our curriculum server is separated from our Admin server and has very limited access.

Remote access to school systems is covered by specific agreements and is never allowed to unauthorized third party users.

Using the Internet

We provide the internet to -

- Children in Key Stage 1 and 2 will search the internet through GOOGLE safe search using our school website on the pupils page.
- Support curriculum development in all subjects
- Support the professional work of staff as an essential professional tool

- Enhance the school's management information and business administration systems
- Enable electronic communication and the exchange of curriculum and administration data with the LA.

Users are made aware that they must take responsibility for their use of, and their behaviour whilst using, the school IT systems or a school provided laptop or device and that such activity can be monitored and checked.

All users of the school IT or electronic equipment will abide by the relevant Acceptable Use Policy (AUP) at all times, whether working in a supervised activity or working independently,

Pupils and staff are informed about the actions to take if inappropriate material is discovered and this is supported by notices in classrooms and around school.

Using email (see email policy No 10)

Email is regarded as an essential means of communication and the school provides all members of staff with an e-mail Office 365 email account for school based communication.

E-mail messages on school business should be regarded as having been sent on headed notepaper and reflect a suitable tone and content and should ensure that the good name of the school is maintained. All emails regarding school must be sent from the school email address. Staff are not to communicate with LA or external agencies on their personal email address.

Use of the school e-mail system is monitored and checked.

As part of the curriculum pupils are taught about safe and appropriate use of email, children message using a username and password through our school website. Pupils are informed that misuse of email will result in a loss of privileges.

Staff are not permitted to use the internet or email for personal use during school hours. This includes PPA. In special circumstances, permission must be sought from the Headteacher. (See policy No 10)

Publishing Content Online

E.g. using the School website, Learning Platform, blogs, wikis, podcasts, social network sites

School website

The school maintains editorial responsibility for any school initiated website or learning platform content to ensure that content is accurate and the quality of presentation is maintained. The school maintains the integrity of the school website by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

The point of contact on the website is the school address, e-mail, telephone and fax number.

Identities of pupils are protected at all times. Photographs of identifiable individual pupils are not published on the web site and school obtains permission from parents for the use of pupils' photographs. Group photographs do not have a name list attached.

Children have access to useful links, Education City, Purple Mash and Matheletics . Each of these require a username and password.

Creating online content as part of the curriculum:

Pupils are taught safe and responsible behaviour in their creation and publishing of online content. They are taught to publish for a wide range of audiences which might include governors, parents or younger children. Blogging (this is currently monitored my IT team), podcasting and other publishing of online content by pupils will take place within the school learning platform or other media selected by the school. Pupils will only be allowed to post or create content on sites where members of the public have access, when this is part of a school related activity. Appropriate procedures to protect the identity of pupils will be followed.

We take all steps to ensure that any material published online is the author's own work, gives credit to any other work included and does not break copyright.

Online material published outside the school:

Staff and pupils are encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school as they are in school.

Material published by pupils, governors and staff in a social context which is considered to bring the school into disrepute or considered harmful to, or harassment of another pupil or member of the school community will be considered a breach of school discipline and treated accordingly.

Using images, video and sound

We recognise that many aspects of the curriculum can be enhanced by the use of multi-media and that there are now a wide and growing range of devices on which this can be

accomplished. Pupils are taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

Digital images, video and sound recordings are only taken with the permission of participants; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress. Full names of participants are not used either within the resource itself, within the file-name or in accompanying text online.

We ask all parents/carers to sign an agreement about taking and publishing photographs and video of their children and this list is checked whenever an activity is being photographed or filmed. (See AUP Policy No 05)

For their own protection staff or other visitors to school never use a personal device (mobile phone, digital camera or digital video recorder) to take photographs of pupils.

Using mobile phones

Where required for safety reason in off-site activities, a school mobile phone is provided for contact with pupils, parents or the school. Staff will not be expected to use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a pupil or parent.

Unauthorized or secret use of a mobile phone or other electronic device, to record voice, pictures or video is forbidden. Unauthorized publishing of such material on a website which causes distress to the person(s) concerned will be considered a breach of school discipline, whether intentional or unintentional. The person responsible for the material will be expected to remove this immediately upon request.

The sending or forwarding of text messages deliberately targeting a person with the intention of causing them distress, 'cyber bullying', will be considered a disciplinary matter.

Practitioners are permitted to have their mobile phones about their person; however there is a clear expectation that all personal use is limited to allocated lunch and/or tea breaks.

Other than in agreed exceptional circumstances, phones must be switched off and calls and texts must not be taken or made during lesson time.

Practitioners are not permitted, in any circumstance to use their phones for taking, recording or sharing images and 'mobile free' areas must be observed at all times.

Practitioners are not permitted to use their own personal phones for contacting children, young people and their families within or outside of the setting.

Parents, visitors and contractors are respectfully requested not to use their mobile phones in any of the "designated mobile free" areas. Should phone calls and/or texts need to be taken or made, use is restricted to those areas not accessed by children in order to avoid any unnecessary disturbance or disruption to others.

Under no circumstances is **any** individual permitted to take images or make recordings on a mobile phone on school premises, even of their child, without authorised permission from the Headteacher.

Any individual bringing a personal device into the setting must ensure that it contains no inappropriate or illegal content.

Staff failing to comply or endorsing the above will be dealt with using the school and LA disciplinary procedures and/ misconduct.

Using other technologies

As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an E-Safety point of view.

We will regularly review the E-Safety Policy to reflect any new technology that we use, or to reflect the use of new technology by pupils.

Staff or pupils using a technology not specifically mentioned in this policy will be expected to behave with similar standards of behaviour to those outlined in this document.

Protecting School data and Information

School recognises their obligation to safeguard staff and pupil's personal data including that which is stored and transmitted electronically. We regularly review our practices and procedures to ensure that they meet this basic obligation.

Pupils are taught about the need to protect their own personal data as part of their e-Safety awareness and the risks resulting from giving this away to third parties.

Suitable procedures, and where necessary training, are in place to ensure the security of such data including the following:

- Staff are provided with encrypted USB memory sticks for carrying sensitive data. The encrypted memory sticks are 2G. If password is forgotten after 6 attempts

all data will be wiped and not retrievable. We have not gone for bigger memory sticks than 2G , so that data loss is kept to a minimum

- All computers or laptops holding sensitive information are set up with strong passwords, screens are locked when they are left unattended
- Staff are provided with appropriate levels of access to the school's management information systems holding pupil data. Admin Passwords are not shared and administrator passwords are kept securely.
- Staff have access to staff common, children's common drives and media drive on their laptops when connected to network. When taking laptop off school premises they do not have remote access to these drives
- Staff are aware of their obligation to keep sensitive data secure when working on computers outside school. The data that is taken home is from staff common – curriculum
- All data is saved on school's network or staff encrypted memory sticks and are urged not to save data on laptops. All staff have signed the school loan's agreement
- When we dispose of old computers and other equipment we wipe clean all machines off any data and format the machines, our admin machines we completely destroy the information which may be held on them and then destroy the hard drives.
- We follow strict procedures for transmitting data securely and sensitive data is not sent via emailed unless encrypted
- Remote access to computers is by authorized personnel only
- We have full back up and recovery procedures in place for school data. Our backup for curriculum is kept in a separate part of the school away from the server and data is backed up every night. The Admin backup is done remotely with LINK2ICT and Computing.

- Where sensitive staff or pupil data is shared with other people who have a right to see the information, for example Head Teacher, SEN, Admin Staff, Governors or the SIP, we label the material appropriately to remind them of their duty to keep it secure and securely destroy any spare copies (we have 3 Shredders in admin offices) Confidential documents when emailed should be password protected.

Dealing with E-Safety incidents

All e-Safety incidents are recorded in the School e-Safety Log which is regularly reviewed.

Any incidents where pupils do not follow the Acceptable Use Policy will be dealt with following the school's normal behaviour or disciplinary procedures.

In situations where a member of staff is made aware of a serious E-Safety incident, concerning pupils or staff, **they will inform the head teacher** who will then respond in the most appropriate manner.

Instances of cyber-bullying will be taken very seriously by the school and dealt with using the schools anti-bullying procedures. School recognises that staff as well as pupils may be victims and will take appropriate action in either situation.

Incidents which create a risk to the security of the school network, or create an information security risk, will be referred to the Head Teacher and technical support and appropriate advice sought and action taken to minimize the risk and prevent further instances occurring, including reviewing any policies, procedures or guidance. If the action breaches school policy then appropriate sanctions will be applied. The school will decide if parents need to be informed if there is a risk that pupil data has been lost.

School reserve the right to monitor equipment of their premises and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

Dealing with complaints and breaches of conduct by pupils:

- Any complaints or breaches of conduct will be dealt with promptly
- Responsibility for handling serious incidents will be given to a senior member of staff
- Parents and the pupil will work in partnership with staff to resolve any issues arising
- There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies

The following activities constitutes behaviour which we would always consider unacceptable (and possible illegal):

- accessing inappropriate or illegal content deliberately
- deliberately accessing downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- continuing to send or post material regarded as harassment, or of a bullying nature after being warned

- using digital communications to communicate with pupils in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or inappropriate communication via social networking sites)

The following activities are likely to result in disciplinary action:

- any online activity by a member of the school community which is likely to adversely impact on the reputation of the school
- accessing inappropriate or illegal content accidentally **and failing to report this**
- inappropriate use of personal technologies (e.g. mobile phones) at school or in lessons
- sharing files which are not legitimately obtained e.g. music files from a file sharing site
- using school or personal equipment to send a message, or create content, that is offensive or bullying in nature or could bring the school into disrepute
- attempting to circumvent school filtering, monitoring or other security systems
- circulation of commercial, advertising or 'chain' emails or messages
- revealing the personal information (including digital images, videos and text) of others by electronic means (e.g. sending of messages, creating online content) without permission

The following activities would be unacceptable;

- accessing social networking sites, chat sites, instant messaging accounts, email or using a mobile phone for personal use during lesson time
- accessing non-educational websites (e.g. gaming or shopping websites) during lesson time
- sharing a username and password with others or allowing another person to log in using your account
- accessing school ICT and Computing systems with someone else's username and password
- deliberately opening, altering, deleting or otherwise accessing files or data belonging to someone else

Legislation

Schools have to be aware of the legislative framework under which the E-Safety Policy and guidance have 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.

Below are the legislative frameworks that impact on the E-safety Policy.

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 a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

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 Head teachers, 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.

The Education and Inspections Act 2011

This extended the powers included in the 2006 Act and gave permission for Head teachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see DfE guidance - http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:

http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/b0075738/reducing-bureaucracy/requirements/changestoschoolinformationregulations