Springwell Leeds Academy

E-Safety Policy

The internet and e-mail are powerful tools to open up new opportunities for people of all ages. The Government wants everyone to have access to the wealth of cultural, scientific and intellectual material to be found on the internet. However, we are equally determined to ensure that our pupils are protected from unsuitable material and that they can access appropriate material safely.

Revised March 2017

Contents

Scope of the Policy

New technologies have revolutionised the movement, access and storage of information with important implications for all schools. Use of ever more powerful computers, iPads, broadcast media, the Internet, digital recorders of sound and images together with increased opportunities to collaborate and communicate are changing established ideas of when and where learning takes place. At Springwell, we recognise that learning is a lifelong process and that e learning is an integral part of it. Ensuring that we provide pupils with the skills to make the most of information and communication technologies is an essential part of our curriculum. The school is committed to the continuing development of our ICT infrastructure and embracing new technologies to maximise the opportunities for all pupils, staff, parents and the wider community to engage in productive, cooperative and efficient communication and information sharing.

However, as in any other area of life, children are vulnerable and may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies. Additionally, some young people may find themselves involved in activities that are inappropriate, or possibly illegal. E-safety seeks to address the issues around using these technologies safely and promote an awareness of the benefits and the risks.

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

The Education and Inspections Act 2006 empowers Principals, to such extent as is reasonable, to regulate the behaviour 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 of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but which are linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities Governors

The Governors of the school are responsible for the approval of this E-Safety Policy and for reviewing the effectiveness of the policy. This is carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor under their safeguarding responsibility. The named Governor is Raminda Aujla. The role of the E-Safety Governor includes:

• regular meetings with the E-Safety Co-ordinator

• regular monitoring of e-safety incident logs

• regular monitoring of filtering / change control logs

• reporting to the Governing body

Principal and Senior Leaders

The Executive Principal is responsible for ensuring the safety (including e-safety) of members of the school community, though day to day responsibility for e-safety has been delegated to the Designated Lead for Safeguarding and E-Safety.

The Executive Principal and Senior Leadership Team are responsible for ensuring that the Designated Lead for Safeguarding and E-Safety and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues as deemed appropriate.

The Executive Principal and Senior Leadership Team will ensure that there is a system in place to allow for monitoring and support of the Designated Lead for Safeguarding and E-Safety. This is to provide a safety net and support for those colleagues who take on important monitoring roles. The Senior Leadership Team will receive regular monitoring reports from the Designated Lead for Safeguarding and E-Safety.

The Executive Principal and Executive Vice Principal are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

Technical Support

The ICT Service Provider is currently Primary ICT. They are responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the academy meets the e-safety technical requirements outlined in the Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- That it keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices

- they have read, understood and signed the school Staff Acceptable Use Policy (AUP)

- they report any suspected misuse or problem to the Designated Lead for Safeguarding and E-Safety for investigation, action or sanction

- digital communications with pupils should be on a professional level and only carried out using official school systems

- e-safety issues are embedded in all aspects of the curriculum and other school activities

- pupils understand and follow the school e-safety and acceptable use policy

- pupils have a good understanding of research skills and uphold copyright regulations

- they monitor ICT activity in lessons, extra curricular and extended school activities

- they are aware of e-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

- that the use of the network, Virtual Learning Environment (VLE), remote access and email are regularly monitored in order that any misuse or attempted misuse can be reported to the Designated Lead for Safeguarding and E-Safety for investigation ,action, or sanction

- that monitoring software and systems are implemented and updated as agreed in school policies

Designated Lead for Safeguarding and E-Safety

The Designated Lead for Safeguarding and E-Safety is trained in e-safety issues and is aware of the potential for serious child protection issues to arise from:

- sharing of personal data

- access to illegal or inappropriate materials

- inappropriate on-line contact with adults and strangers

- potential or actual incidents of grooming

- cyber-bullying

The Designated Lead for Safeguarding and E-Safety is Steve Tighe.

Pupils

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems. (It is expected that parents of pupils in key stage one will sign on their behalf).

- have a good understanding of research skills and the need to uphold copyright regulations

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and

understand school policies on the taking and use of images and on cyberbullying.

- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet and 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, letters and information about national and local e-safety campaigns and literature. Parents and carers will be responsible for endorsing (by signature) the Pupil Acceptable Use Policy.

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 e-safety is therefore an essential part of the school's e-safety provision.

Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. E-Safety education will be provided in the following ways:

- A planned e-safety programme will be provided as part of ICT, PHSE and other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and tutorial and pastoral activities
- Pupils will be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information
- Pupils will be helped to understand the need for the pupil Acceptable Use Policy and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet will be posted in all rooms.
- Staff will 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 e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and 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:

• Letters and newsletters

• Parents evenings

Education & Training – Staff

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

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- The Designated Lead for Safeguarding and E-Safety will receive regular updates from the Local Authority, other information training sessions and by reviewing guidance documents released by BECTA, the Local Authority and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff team meetings and INSET days.
- The Designated Lead for Safeguarding and E-Safety will provide advice and guidance and training as required to individuals as required

Training – Governors

E-Safety awareness sessions will be delivered to members of the governing body in particular those who are members of any sub committees with responsibility for e-safety, health and safety and safeguarding.

Technical – infrastructure, equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure and 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 e-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the Acceptable Usage Policy and any relevant Local Authority E-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 groups of users will be recorded by the Service Provider (or other person) and will be reviewed, at least annually.

- All users (at KS2 and above) will be provided with a username and password

- Users will be made responsible for the security of their username and password, and 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 Executive Principal and Service Provider and if the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly. Any request for such changes must be submitted via the correct methods outlined in the service providers service level agreement.

- All staff are aware of the Local Authority policy on the use of removable media such as memory sticks, CD's and DVD's
- All staff are made aware of the prohibition of transferring data to personnel emails

Use of digital and video images - Photographic, Video

The school is responsible for the safe use of photographic and video images of all pupils. When using photographic and video images staff must:

- follow school policies concerning the sharing, distribution and publication of those images. Images should only be taken on school equipment. Personal equipment of staff should not be used for such purposes.
- ensure 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 .
- must ensure pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- ensure that written permission from parents or carers has been obtained before photographs of pupils are published.

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:
- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and checking software
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

Communications

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. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).

- 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 must not respond to any such email.

- Any digital communication between staff and pupils or parents / carers 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.

- 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, as defined below, 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

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:	child sexual abuse images
	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 or other safeguards employed by the school	
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
Use of social networking sites
Use of video broadcasting eg Youtube unless agreed by senior management

Responding to incidents of misuse

Staff

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.

• child sexual abuse images
• adult material which potentially breaches the Obscene Publications Act
• criminally racist material
• other criminal conduct, activity or materials

The staff responsible will be subject to disciplinary procedures and dealt with through the Local Area Designated Officer procedures. If any staff member suspects illegal activity, it must be reported immediately to the Designated Lead for Safeguarding and E-Safety, or direct to the Principal on site. The matter must not be discussed with any other member of staff under any circumstances.

If there is a breach of the E-Safety policy that is not considered illegal then the matter will be dealt with appropriately and proportionately. Continuous breaches of the policy will result in serious disciplinary procedures by the Executive Principal.

Pupils

All staff are responsible for ensuring that pupils respect and adhere to the E-Safety policy. If any member of staff witnesses or is informed of pupils who are deliberately trying to access material that could be considered illegal or taking part in the activities listed below, it must be reported to a member of the senior leadership team immediately.

- Unauthorised use of non-educational sites during lessons
- Unauthorised use of mobile phone, digital camera and other handheld devices
- Unauthorised use of social networking, instant messaging and personal email
- Unauthorised downloading or uploading of files
- Allowing others to access school network by sharing username and passwords
- Attempting to access or accessing the school network, using another student's / pupil's account
- Attempting to access or accessing the school network, using the account of a member of staff
- Corrupting or destroying the data of other users
- Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature
- Continued infringements of the above, following previous warnings or sanctions
- Actions which could bring the school into disrepute or breach the integrity of the ethos of the school
- Using proxy sites or other means to subvert the school's filtering system

- Deliberately accessing or trying to access offensive or pornographic material
- Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act

Appendices

Can be found on the following pages:

Pupil Acceptable Use Policy Agreement

E-Safety - Acceptable Use Agreement

These e-Safety Rules help to protect students and the Academy by describing acceptable and unacceptable computer use.

- The Academy owns the computer network and can set rules for its use
- I appreciate that ICT includes a wide range of systems, including mobile phones, tablets, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for Academy business.
- I understand that it is a criminal offence to use a computer or network for a purpose not permitted by the Academy.
- I understand that the irresponsible use of the network and internet will result in the loss of network or Internet access, plus the Academy may instigate additional sanctions. For serious breaches the Academy may involve the police.
- I agree that network access must be made via the user's authorised account and password, which must not be given to any other person.
- I understand that users may not install or run software on the network.
- I understand that all network and Internet use must be appropriate to education.
- I agree that all copyright and intellectual property rights must be respected.
- I understand that all messages shall be written carefully and politely, particularly as e-mail could be forwarded to unintended readers.
- I understand that anonymous messages and chain letters are not permitted.
- I understand that I must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- I agree to use Academy managed blogs, wikis and discussion groups appropriately and politely.
- I understand that the Academy ICT systems may not be used for private purposes, unless the Principal has given specific permission.
- I agree that any inappropriate access to materials on the network or internet will be reported to a member of staff.
- I understand that I must be socially responsible with regard to using the internet and other communication technologies, including treating others with respect, and reporting instances of online bullying.

The Academy may exercise its right to monitor the use of the Academy's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the Academy's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

E-Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Name of Pupil:

Pupil's Agreement

- I have read and I understand the Academy e-Safety Rules.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Signed:	*Date:*

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the Academy rules.

Parent's Consent for Internet Access

I have read and understood the Academy e-safety rules and give permission for my son / daughter to access the Internet. I understand that the Academy will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

In the absence of any negligence, I understand that the Academy cannot be held responsible for the content of materials accessed through the internet. I agree that the Academy is not liable for any damages arising from use of the internet facilities

Signed:	*Date:*

Please print name:

Staff (and Volunteer) Acceptable Use Policy Agreement Template School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for *students / pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Staff Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:
- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident; I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images.. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The academy and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:
- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.

- I will not disable or cause any damage to school equipment, or the equipment belonging to others.

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted.

- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work

- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

 I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name	
Signed	
Date	

Parent / Carer Acceptable Use Policy Agreement Template

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that *students / pupils* will have good access to ICT to enhance their learning and will, in return, expect the *students / pupils* to agree to be responsible users. A copy of the Student / Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name

Student / Pupil Name

As the parent / carer of the above *students / pupils*, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed

Date

Legislation

Schools should be aware of the legislative framework under which this E-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 e 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 Harrassment 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 Principals, 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.