

Warden Hill Infant School



Online Safety Policy

Content

Schedule for development, monitoring and review

Scope of the Policy

Roles and Responsibilities

- Governors
- Headteacher and Senior Leaders
- Online Safety Co-ordinator
- Network Manager / Technical Staff
- Teaching and Support Staff
- Designated Person for Child Protection
- Students / Pupils
- Parents and Carers

Policy Statements

- Education – Students / Pupils
- Education – Parents / Carers
- Education – Extended Schools
- Education and training – Staff
- Training – Governors
- Technical – infrastructure / equipment, filtering and monitoring
- Curriculum
- Use of digital and video images
- Data protection
- Communications
- Unsuitable / inappropriate activities
- Responding to incidents of misuse

Acknowledgements

Appendices:

- Pupil Acceptable Use Policy
- Staff Acceptable Use Policy
- Parents and Carers Acceptable Use Policy Agreement
- Consent form taking images
- Acceptable use policy for digital images
- School Filtering Policy
- School Personal Data Policy
- Mobile Technologies Policy
- Legislation
- Links to other organisations and documents
- Glossary of Terms

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:	Online Safety Group
Monitoring will take place at regular intervals:	Annually
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 online safety or incidents that have taken place. The next anticipated review date will be:	Summer 2017
Should serious online safety incidents take place, the following external persons / agencies should be informed:	LADO, Safeguarding in Education Manager, Senior ICT Teaching and Learning Consultant, Police Commissioner's Office

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Surveys / questionnaires of
 - pupils
 - parents / carers
 - staff

Scope of the Policy

This policy applies to all members of the school community (including staff, students / 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 Headteachers 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 online bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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 Online Safety behaviour that take place out of school.

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.

Headteacher and Senior Leaders:

- The Headteacher 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 *Online Safety Co-ordinator*.
- *The Headteacher / Senior Leaders are responsible for ensuring that the Online Safety Coordinator 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 Senior Leadership Team / Senior Management Team will receive regular monitoring reports from the Online Safety Co-ordinator.*
- The Headteacher 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. (see Responding to Incidents of misuse)

Online Safety Coordinator:

- takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT technical staff
- receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments,
- reports regularly to Senior Leadership Team

ICT Technical staff:

The school has a managed ICT service provided by an outside contractor.

The ICT Technician is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the Online Safety technical requirements outlined in the Acceptable Usage Policy and any relevant Local Authority Online Safety Policy.
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly change
- that he / she keeps up to date with Online Safety technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant
- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Co-ordinator, Headteacher, Senior Leader, Class teacher for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

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 Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Online Safety Co-ordinator and Headteacher for investigation / action / sanction
- digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level *and only carried out using official school systems*
- Online Safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school Online Safety Policy and acceptable use policy
- they monitor ICT activity in lessons, extra-curricular and extended school activities
- they monitor the use of digital technologies, mobile devices, cameras, tablets etc in lessons and other school activities (where allowed) and implement current 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

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

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
- 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, tablets and hand held devices. They should also know and understand school policies on the taking / use of images and online-bullying.
- should understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will therefore take every opportunity to help parents understand these issues through website and information about national and local Online Safety campaigns or literature. *Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:*

- endorsing (by signature) the Pupil Acceptable User Policy Agreement
- *digital and video images taken at school events*
- accessing the school website or on-line pupil records in accordance with the relevant school Acceptable User Policy Agreement.
- *their children's personal devices in the school (where this is allowed)*

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.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned Online Safety programme should be provided as part of *Computing* / PHSE / other lessons 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 *whole school, Year group and class* activities
- 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
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Staff should act as good role models in their use of ICT, the internet and mobile devices

In order to prevent radicalisation and related extremist content children are regularly taught about how to stay safe when using the internet and are encouraged to recognise that people are not always who they say they are online. They are taught to seek adult help if they are upset or concerned about anything they read or see on the internet.

Education – parents and 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 may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters and website,
- Reference to the relevant web sites / publications

Education - Extended Schools

Everyone has a role to play in empowering children to stay safe while they enjoy current and new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world. The school will provide opportunities for families to gain from the school's online safety knowledge and experience by running courses in ICT, media literacy and online safety so that parents and children can together gain a better understanding of these issues. These courses will be extended to grandparents and other relatives

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. This will be regularly updated and reinforced.*
- All new staff should receive a copy of the *Online Safety Policy and Acceptable User Policies* as part of their induction programme, *and training* to ensure that they fully understand the school Online Safety Policy.
- *The Online Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.*
- This Online Safety policy and its updates will be presented to and discussed by staff in staff meetings or INSET days.

Training – Governors

Governors should take part in Online Safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in ICT / Online Safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority
- Participation in school training / 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 technical systems will be managed in ways that ensure that the school meets the online safety technical requirements outlined in relevant Local Authority and other relevant body policy and guidance
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- The “administrator” passwords for the school ICT system, used by the ICT Technician (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place
- All users will be provided with a username and secure password by the ICT Technician and Mrs Bright who will keep an up to date record of users and their usernames. Users will be made responsible for the security of their username and password, 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. Staff be required to change their password every 2 years.

- The ICT Technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband provider (RM Education) and their filtering system (RM SafetyNet) by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and Internet use is logged and regularly monitored. Requests from staff for sites to be removed from the filtered list will be considered by the ICT Technician / Headteacher and Online Safety Co-ordinator. If the request is agreed, this action will be recorded and logged.
- In the event of the ICT Technician needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head teacher.
- The school has provided enhanced user-based filtering allowing different filtering levels for different groups of users – staff / pupils etc.
- Systems are in place to regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement. Reports are regularly reviewed by the ICT Technician and Online Safety Group
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person via ICT Support online call logging system.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- The Acceptable user policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students / pupils need to be aware of the risks associated with sharing images and with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. 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 eg 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.
- 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
- Pupil's work can only be published with the permission of the student / pupil and parents or carers.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

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.**

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools 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 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:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues. Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

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

When official school social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school / academy disciplinary procedures

Personal Use: (also see separate Social Network Policy)

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies.

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

Actions

Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
------------	-----------------------------	--------------------------------	--------------	--------------------------

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 other mobile devices e.g. tablets, gaming devices		✓				✓		
Use of personal email addresses in school, or on school network		✓						✓
Use of school email for personal emails				✓				✓
Use of chat rooms / facilities				✓				✓
<i>Use of messaging apps</i>		✓						✓
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 must not respond to any such email.
- Any digital communication between staff and pupils or parents and carers (email, chat, blogs, Learning Platform etc.) must be professional in tone and content
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

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				✓		
On-line shopping / commerce	✓					
File sharing	✓					
Use of social networking sites	✓					
Use of video broadcasting e.g. YouTube	✓					

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:

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-

bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

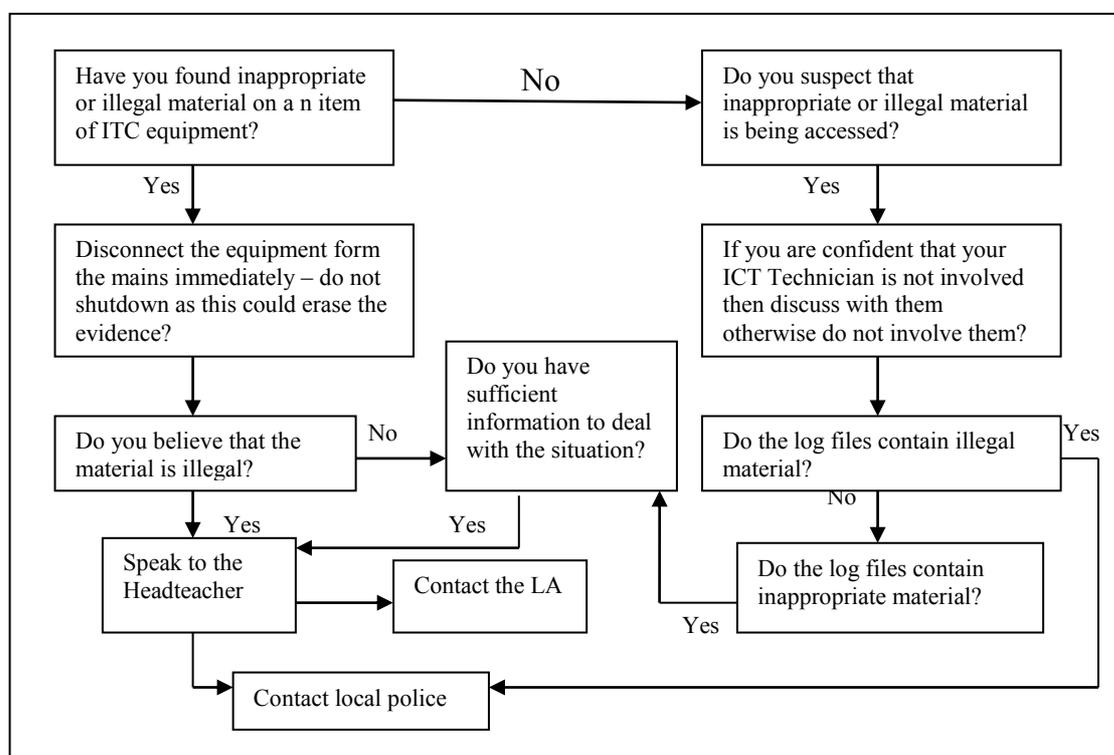
Responding to incidents of misuse

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. This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

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

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

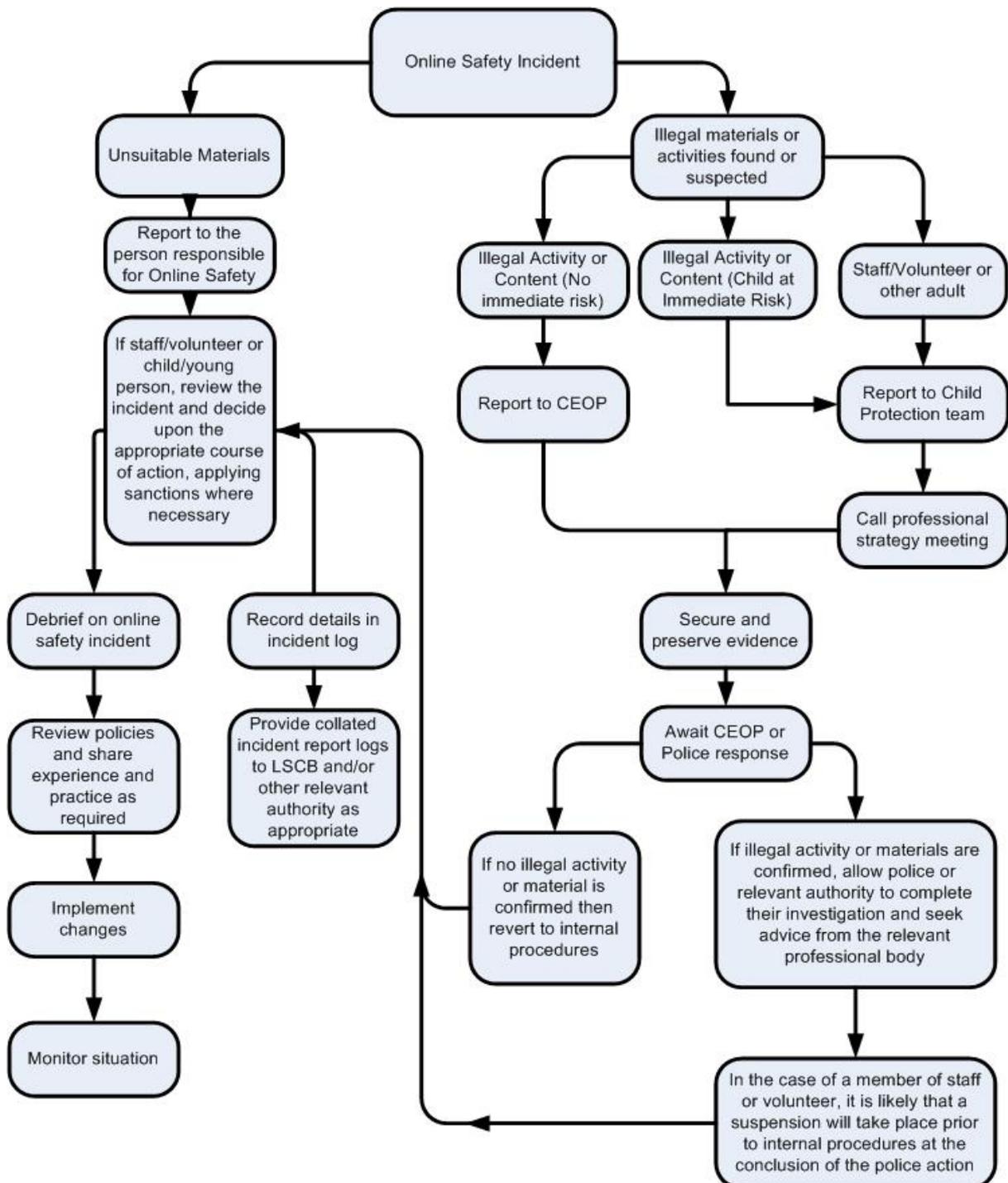
The flowchart below should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and preservation of evidence.



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. Guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a “clean” designated computer.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school / academy community will be responsible users of digital technologies, who understand and follow school / academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Local Authority / Academy Group or national / local organisation (as relevant).
 - Police involvement and/or action
- **If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
 - incidents of 'grooming' behaviour
 - the sending of obscene materials to a child
 - adult material which potentially breaches the Obscene Publications Act
 - criminally racist material
 - promotion of terrorism or extremism
 - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school / academy and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Pupils

Incidents:	Refer to class teacher / tutor	Refer to Headteacher / Deputy	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓			
Unauthorised use of non-educational sites during lessons	✓			✓		
Unauthorised use of mobile phone / digital camera / tablets /other handheld device	✓	✓			✓	
Unauthorised use of social networking / messaging apps / 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		✓		✓	✓	✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓					
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						

Staff

Incidents:	Disciplinary Action	Refer to Headteacher /Deputy	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓	✓
Excessive or inappropriate personal use of the internet / social networking sites / messaging apps / personal email		✓			
Unauthorised downloading or uploading of files		✓			
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		✓			
Careless use of personal data eg holding or transferring data in an insecure manner		✓			
Deliberate actions to breach data protection or network security rules		✓			
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓			
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓			
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		✓			
Actions which could compromise the staff member's professional standing		✓			
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		✓			
Accidentally accessing offensive or pornographic material and failing to report the incident		✓			
Deliberately accessing or trying to access offensive or pornographic material		✓			
Breaching copyright or licensing regulations		✓			
Continued infringements of the above, following previous warnings or sanctions		✓			

Acknowledgements

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School Online Safety Policy Template and of the 360-degree safe Online Safety Self Review Tool:

- Members of the SWGfL Online Safety Group
- Avon and Somerset Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- NEN / Regional Broadband Grids

Copyright of these Template Policies is held by SWGfL. Schools / Academies and other educational institutions are permitted free use of the Template Policies for the purposes of policy writing, review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL (esafety@swgfl.org.uk) and acknowledge its use.

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in April 2016. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material.

© South West Grid for Learning Trust Ltd 2016

Appendices

Can be found on the following pages:

- Pupil Acceptable Usage Policy
- Staff Acceptable Usage Policy
- Parents and Carers Acceptable Usage Policy Agreement
- Consent form taking images
- Acceptable user policy for digital images
- School Filtering Policy
- School Personal Data Policy
- Mobile Technologies Policy
- Legislation
- Links to other organisations and documents
- Glossary of terms

School Filtering Policy

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

The school purchases its broadband from RM Education through School Support Services@Luton which includes RM SafetyNet as the managed filtering service.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the ICT Technician. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:

- **be logged in change control logs**
- **be reported to the Headteacher**

All users have a responsibility to report immediately to the ICT Technician or Headteacher any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Education / Training / Awareness

Pupils / students will be made aware of the importance of filtering systems through the Online Safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- *signing the AUP*
- *induction training*
- *staff meetings, briefings, Inset.*

Parents will be informed of the school's filtering policy through the Acceptable Use agreement.

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the ICT Technician who will decide whether to make school level changes (as above).

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use agreement.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- *The Headteacher*
- *Online Safety Governor*
- *Local Authority on request*

School Personal Data Handling Policy

Introduction

Schools should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature.

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data
- need to have access to that data.

Any loss of personal data can have serious effects for individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action and / or criminal prosecution. All transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data legislation and relevant regulations and guidance from the Local Authority.

The Data Protection Act (1998) lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and security and requires users of data (data processors) to be open about how it is used and to follow "good information handling principles".

Policy Statements

The school will hold the minimum personal information necessary to enable it to perform its function and information will be erased once the need to hold it has passed.

Every effort will be made to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".

Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including *pupils*, members of staff and parents and carers e.g. names, addresses, contact details, legal guardianship / contact details, health records, disciplinary records
- Curricular / academic data e.g. class lists, pupil progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members

Responsibilities

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Secure Storage of and access to data

The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them.

All users will be given secure user names and strong passwords. User names and passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media). Private equipment (i.e. owned by the users) must not be used.

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

- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

The school has procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

All paper based IL2-Protected and IL3-Restricted (or higher) material must be held in lockable storage.

The school recognises that under Section 7 of the Data Protection Act, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests ie. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of school.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information.
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority in this event.

Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of protected data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded, incinerated or otherwise disintegrated for data.

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 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 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 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.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. ([see template policy in these appendices and for DfE guidance - http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation](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:

<https://www.gov.uk/guidance/what-maintained-schools-must-publish-online>

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy:

UK Safer Internet Centre

Safer Internet Centre – <http://saferinternet.org.uk/>

South West Grid for Learning - <http://swgfl.org.uk/>

Childnet – <http://www.childnet-int.org/>

Professionals Online Safety Helpline - <http://www.saferinternet.org.uk/about/helpline>

Internet Watch Foundation - <https://www.iwf.org.uk/>

CEOP

CEOP - <http://ceop.police.uk/>

ThinkUKnow - <https://www.thinkuknow.co.uk/>

Others

INSAFE - <http://www.saferinternet.org/ww/en/pub/insafe/index.htm>

UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis

Netsmartz - <http://www.netsmartz.org/>

Tools for Schools

Online Safety BOOST – <https://boost.swgfl.org.uk/>

360 Degree Safe – Online Safety self-review tool – <https://360safe.org.uk/>

Bullying / Cyberbullying

Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGfL & Diana Awards) - <http://enable.eun.org/>

Scottish Anti-Bullying Service, Respectme - <http://www.respectme.org.uk/>

Scottish Government - Better relationships, better learning, better behaviour - <http://www.scotland.gov.uk/Publications/2013/03/7388>

DfE - Cyberbullying guidance -

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Childnet – new Cyberbullying guidance and toolkit (Launch spring / summer 2016) -

<http://www.childnet.com/new-for-schools/cyberbullying-events/childnets-upcoming-cyberbullying-work>

Anti-Bullying Network – <http://www.antibullying.net/cyberbullying1.htm>

Social Networking

Digizen – [Social Networking](#)

UKSIC - [Safety Features on Social Networks](#)

[SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people](#)

[Connectsafely Parents Guide to Facebook](#)

[Facebook Guide for Educators](#)

Curriculum

[SWGfL Digital Literacy & Citizenship curriculum](#)

Glow - <http://www.educationscotland.gov.uk/usingglowandict/>

Teach Today – www.teachtoday.eu/

Insafe - [Education Resources](#)

Mobile Devices / BYOD

Cloudlearn Report [Effective practice for schools moving to end locking and blocking](#)
NEN - [Guidance Note - BYOD](#)

Data Protection

Information Commissioners Office:

[Your rights to your information – Resources for Schools - ICO](#)
[Guide to Data Protection Act - Information Commissioners Office](#)
[Guide to the Freedom of Information Act - Information Commissioners Office](#)
[ICO guidance on the Freedom of Information Model Publication Scheme](#)
[ICO Freedom of Information Model Publication Scheme Template for schools \(England\)](#)
[ICO - Guidance we gave to schools - September 2012 \(England\)](#)
[ICO Guidance on Bring Your Own Device](#)
[ICO Guidance on Cloud Hosted Services](#)
[Information Commissioners Office good practice note on taking photos in schools](#)
[ICO Guidance Data Protection Practical Guide to IT Security](#)
[ICO – Think Privacy Toolkit](#)
[ICO – Personal Information Online – Code of Practice](#)
[ICO Subject Access Code of Practice](#)
[ICO – Guidance on Data Security Breach Management](#)
SWGfL - [Guidance for Schools on Cloud Hosted Services](#)
LGfL - [Data Handling Compliance Check List](#)
Somerset - [Flowchart on Storage of Personal Data](#)
NEN - [Guidance Note - Protecting School Data](#)

Professional Standards / Staff Training

DfE - [Safer Working Practice for Adults who Work with Children and Young People](#)
[Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs](#)
[Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs](#)
[UK Safer Internet Centre Professionals Online Safety Helpline](#)

Infrastructure / Technical Support

Somerset - [Questions for Technical Support](#)
NEN - [Guidance Note - esecurity](#)

Working with parents and carers

[SWGfL Digital Literacy & Citizenship curriculum](#)
[Online Safety BOOST Presentations - parent's presentation](#)
[Connectsafely Parents Guide to Facebook](#)
[Vodafone Digital Parents Magazine](#)
[Childnet Webpages for Parents & Carers](#)
[Get Safe Online - resources for parents](#)
[Teach Today - resources for parents workshops / education](#)
[The Digital Universe of Your Children - animated videos for parents \(Insafe\)](#)
[Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide](#)
[Insafe - A guide for parents - education and the new media](#)
[The Cybersmile Foundation \(cyberbullying\) - advice for parents](#)

Research

[EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011](#)
[Futurelab - "Digital participation - its not chalk and talk any more!"](#)
[Ofcom – Children & Parents – media use and attitudes report - 2015](#)

Glossary of terms

AUPA	Acceptable User Policy Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ES	Education Scotland
HWB	Health and Wellbeing
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.

