

Thirsk Community Primary School



Online Safety Policy

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by a working group made up of:

- Headteacher
- Online Safety Officer Coordinator
- Governors
- Parent/Pupils

Consultation with the whole school community has taken place through a range of formal and informal meetings. It has been based on the South-West Grid for Learning and Guidance for Schools and Settings in North Yorkshire September 2017.

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Governing Body	<i>December 2017</i>
The implementation of this Online Safety policy will be monitored by the:	<i>E-Safety Coordinator Senior Leadership Team School Governors</i>
Monitoring will take place at regular intervals:	<i>Once a year</i>
The Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	<i>Once a year</i>
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:	<i>Sept 2020</i>
Should serious online safety incidents take place, the following external persons / agencies should be informed:	<i>Richard Chandler Headteacher Dave Duffey Chair of Governors LADO/ Children's Services</i>

The school will monitor the impact of the policy using:

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

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers and visitors) who have access to and are users of school ICT systems, both in and out of the 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 cyber-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 (see appendix for template policy). 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 online safety roles and responsibilities of individuals and groups within the school:

Governors:

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

- regular meetings with the E-Safety coordinator
- regular monitoring of E-safety incident logs
- reporting to relevant Governors

Headteacher and Senior Leaders:

- The Headteacher has a duty of care 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 E-Safety Coordinator.
- The Headteacher and Deputy Head will be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.

E-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 technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting of Governors
- reports regularly to Senior Leadership Team

Technical staff (Schools ICT):

The Computing Co-ordinator for Computing 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 required online safety technical requirements and any Local Authority E-Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that they keep 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 / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation

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 E-safety Policy and practices

- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Headteacher or E- Safety Coordinator for investigation.
- all digital communications with students / pupils / parents / carers 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 activities
- pupils understand and follow the Online Safety Policy and Acceptable Use Policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students / 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 Safeguarding Lead

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Students / Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and 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 policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-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 / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, Learning Platform and information about national / local online safety campaigns / 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:

- digital and video images taken at school events
- access to parents' sections of the website / Learning Platform and on-line student / pupil records
- their children's personal devices in the school

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 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 E-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited.
- Key E-safety messages should be reinforced as part of a planned programme of assemblies and pastoral 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 taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students / pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. 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, newsletters, web site, e-schools -Learning Platform
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. [swgfl.org.uk](http://www.swgfl.org.uk) www.saferinternet.org.uk/
<http://www.childnet.com/parents-and-carers>

Education & Training – Staff / Volunteers

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. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school's E- Safety Policy and Acceptable Use Agreements.
- The E-Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This E-Safety Policy and its updates will be presented to and discussed by staff in staff meetings.
- The E-Safety Coordinator will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any group involved in safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation

- 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 recommended technical requirements.
- 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.
- All users will be provided with a class username and secure password by the class teacher *who will keep an up to date record of users and their usernames*. Users are responsible for the security of their username and password.
- The “master / administrator” passwords for the school ICT system, used by the Network Manager are held by North Yorkshire School’s ICT.
- The School Business Manager 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 North Yorkshire School’s ICT. Content lists are regularly updated and internet use is logged and regularly monitored. Requests for filtering changes should be made through the Computing Coordinator or Headteacher
- Any actual or potential incident should be immediately reported to the Headteacher.
- 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.
- Visitors such as trainee teachers and supply teachers are given guest user logon details for school systems, including SIMS. They do not have access to server or personal data.
- The school acceptable use policy (AUP) applies to school devices that may be used out of school.
Staff must not download executable files and installing programmes on school devices without prior agreement of the Headteacher or Computing Coordinator.
- Memory sticks must not be used by users on school devices. CDs and DVDs may be used, unless they contain executable files and installing programmes. Data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website / social media / local press.
- 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 / academy 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.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that includes 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.
- Pupil's work can only be published with the permission of the student / pupil and parents or carers.

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. The mobile technologies policy should be consistent with and inter-related to other relevant school policies including but not limited to the safeguarding policy, behaviour policy, bullying policy, acceptable use policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

In preparing a mobile technologies policy the school should consider possible issues and risks. These may include: security risks in allowing connections to your school network, filtering of personal devices, breakages and insurance, access to devices for all students, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership. A range of mobile technology implementations is possible

For further reading, please refer to "[NEN Technical Strategy Guidance Note 5 – Bring your own device](#)"

A more detailed Mobile Technologies Template Policy can be found in the appendix. The school may however choose to include these aspects of their policy in a comprehensive acceptable use agreement, rather than in a separate Mobile Technologies Policy. It is suggested that the school should in this overall policy document outline the main points from their agreed policy. A checklist of points to be considered is included below.

- The school acceptable use agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies
- The school allows: (the school should complete the table below to indicate which devices are allowed and define their access to school systems)

	School Devices			Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device ¹	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes/No ²	Yes/No ²	Yes/No ²
Full network access	Yes	Yes	Yes			
Internet only						
No network access						

¹ Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

² The school should add below any specific requirements about the use of mobile/personal devices in school

Aspects that the school may wish to consider and be included in their online safety policy, mobile technologies policy or acceptable use agreements:

School owned/provided devices:

- Who they will be allocated to
- Where, when and how their use is allowed – times/places/in school/out of school
- If personal use is allowed
- Levels of access to networks/internet (as above)
- Management of devices/installation of apps/changing of settings/monitoring
- Network/broadband capacity
- Technical support
- Filtering of devices
- Access to cloud services
- Data Protection
- Taking/storage/use of images
- Exit processes – what happens to devices/software/apps/stored data if user leaves the school
- Liability for damage
- Staff training

Personal devices:

- Which users are allowed to use personal mobile devices in school (staff/pupils/students/visitors)
- Restrictions on where, when and how they may be used in school
- Storage
- Whether staff will be allowed to use personal devices for school business
- Levels of access to networks/internet (as above)
- Network/broadband capacity
- Technical support (this may be a clear statement that no technical support is available)
- Filtering of the internet connection to these devices
- Data Protection
- The right to take, examine and search users devices in the case of misuse (England only) – N.B. this must also be included in the Behaviour Policy.
- Taking/storage/use of images
- Liability for loss/damage or malfunction following access to the network (likely to be a disclaimer about school responsibility).
- Identification/labelling of personal devices
- How visitors will be informed about school requirements
- How education about the safe and responsible use of mobile devices is included in the school online safety education programmes.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school must ensure that:

- has a Data Protection Policy.
- implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- pays the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- has appointed an appropriate Data Protection Officer (DPO) Veritau, who has a high level of understanding of data protection law and is free from any conflict of interest.
- has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
- the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
- will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. The school should develop and implement a 'retention policy' to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- provides staff, parents, volunteers, teenagers and older children with information about how the school/academy looks after their data and what their rights are in a clear Privacy Notice
- procedures are in place to deal with the individual rights of the data subject.
- Data Protection Impact Assessments (DPIA) are carried out where necessary.
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- understands how to share data lawfully and safely with other relevant data controllers.
- [reports any relevant breaches to the Information Commissioner](#) within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- Has Freedom of Information Policy which sets out how it will deal with FOI requests.
- all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media the:

- data is encrypted and password protected.
- device is password protected. (be sure to select devices that can be protected in this way)
- device is protected by up to date virus and malware checking software
- data is securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

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
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- will not transfer any school data to personal devices except as in line with school policy
- access personal data sources and records 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

The Personal Data Advice and Guidance in the appendix provides more detailed information on the school's/academy's responsibilities and on good practice

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.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held 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”.
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified – Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner’s Office.

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, memory stick or any other removable media:

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

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				
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Communication Technologies								
Mobile phones may be brought to the school/academy	✓							✓
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time	✓							✓
Taking photos on mobile phones/cameras				✓				✓
Use of other PERSONAL mobile devices e.g. tablets, gaming devices				✓				✓
Use of personal email addresses in school/academy, or on school/academy network	✓							✓
Use of school/academy email for personal emails				✓				✓
Use of messaging apps	✓							✓
Use of social media			✓					✓
Use of blogs				✓				✓

~~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 and other adults					Pupils			
	Permitted	Permitted at certain times	Permitted for named staff	Not Permitted		Permitted	Permitted at certain times	Allowed with staff permission	Not Permitted
Communication Technologies									
Mobile phones may be brought to school	✓								✓

Mobile phones used in lessons				✓				✓
Use of mobile phones in social time	✓							✓
Staff should only contact a pupil on a school issued mobile phone	✓							✓
Taking photographs/film on personal mobile devices / digital camera				✓				✓
Taking photographs/film on school mobile devices / digital camera for school purposes only	✓						✓	
Parent / carer taking photos of a school event on their own device and uploading online with public access				✓				✓
Use of personal tablets/ laptops ipads etc in school				✓				✓
Use of school owned tablets/ laptops/ ipads in school but not for personal use	✓				✓			

Use of school owned tablets/ laptops/ ipads out of school but not for personal use	✓ (within the AUP)				✓ (within the AUP)			
Only using school provided encrypted storage devices	✓				✓			
Use of school email for personal emails				✓				✓
Social use of chat rooms/ facilities	✓							✓
Use of social network sites in school			✓				✓	
Use of educational 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 should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, social media, chat, blogs, VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use.
- 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.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools 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 liable to the injured party. Reasonable steps to prevent predictable harm must be in place. Refer to school Social Media Policy.

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:

- No reference should be made in social media to pupils, parents / carers or school
- 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 or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

The school's use of social media for professional purposes will be checked regularly by the Headteacher to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Dealing With Unsuitable / inappropriate activities

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.

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 or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
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 –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	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				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			X			
On-line gaming (non-educational)			X			
On-line gambling					X	

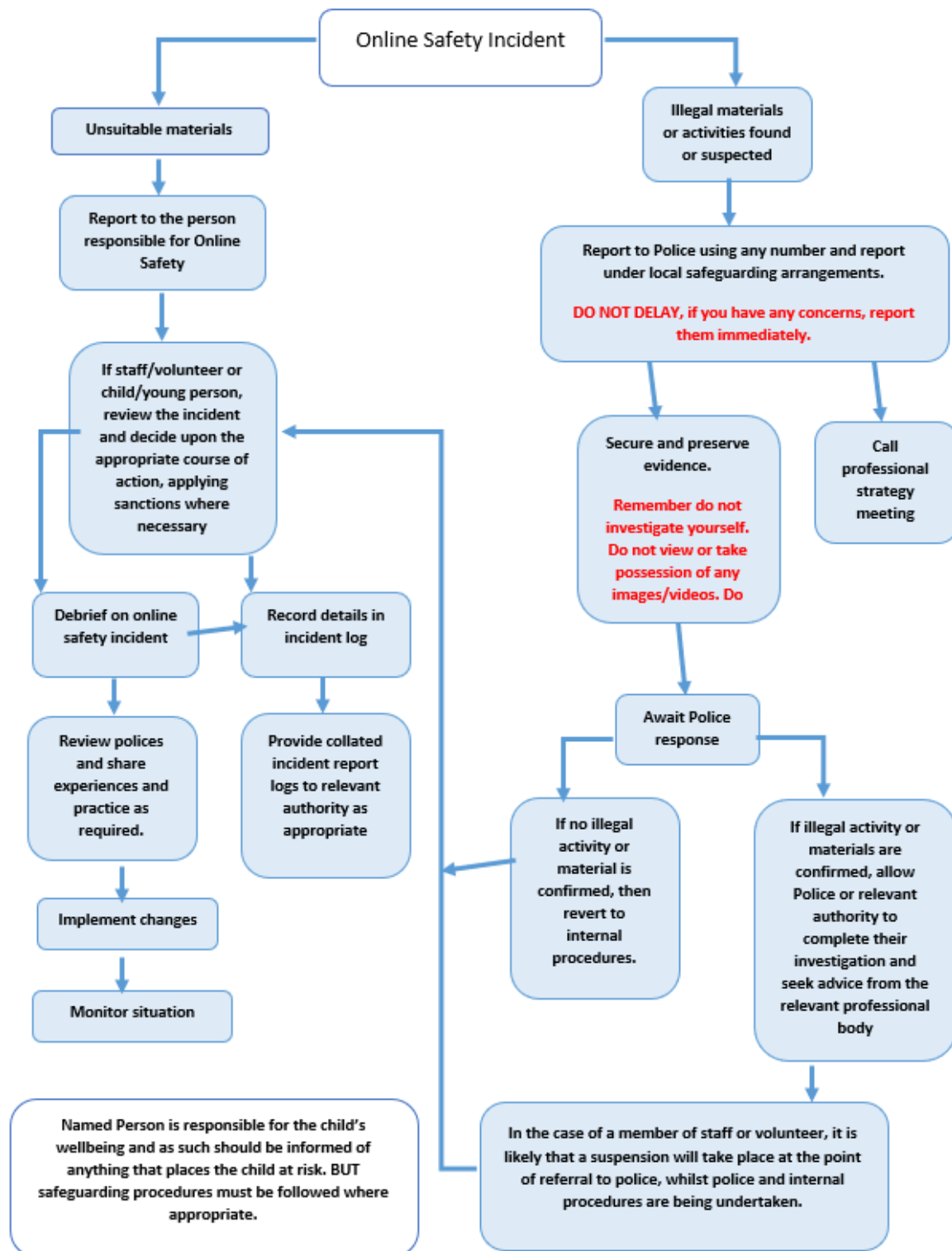
On-line shopping / commerce			X		
File sharing			X		
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting e.g. Youtube			X		

Responding to incidents of 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.

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 community will be responsible users of digital technologies, who understand and follow school 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
 - 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 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 Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X	X	X	
Unauthorised use of non-educational sites during lessons	x						
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X			X		X	
Unauthorised / inappropriate use of social media / messaging apps / personal email	X			X		X	
Unauthorised downloading or uploading of files	X					X	
Allowing others to access school by sharing username and passwords	X					X	
Attempting to access or accessing the school network, using another pupil's account	X						
Attempting to access or accessing the school network, using the account of a member of staff	X			X	X	X	

Corrupting or destroying the data of other users	X					X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X			X	X	X	
Continued infringements of the above, following previous warnings or sanctions	X	X		X	X	X	X
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school	X			X			
Using proxy sites or other means to subvert the school's / academy's filtering system	X			X	X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident	X		X			X	
Deliberately accessing or trying to access offensive or pornographic material	X		X	X	X	X	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act						X	

Staff Incidents

	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X				
Inappropriate personal use of the internet / social media / personal email	X				X		
Unauthorised downloading or uploading of files	X				X		
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	X				X		

Careless use of personal data e.g. holding or transferring data in an insecure manner	X				X		
Deliberate actions to breach data protection or network security rules	X	X		X			X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X	X			X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X			X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X			X		X
Actions which could compromise the staff member's professional standing	X				X		X
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy	X				X		X
Using proxy sites or other means to subvert the school's / academy's filtering system	X	X		X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X		X	X		
Deliberately accessing or trying to access offensive or pornographic material	X	X		X	X		X
Breaching copyright or licensing regulations	X				X		
Continued infringements of the above, following previous warnings or sanctions	X	X			X		X

Acknowledgements

With thanks to Rob Simmonds of Well Chuffed Comms (wellchuffedcomms.com) and Chelmsford College for allowing the use of their policies in the creation of this policy.

Appendix

School Policy Template – Online Safety Group Terms of Reference

1. Purpose

To provide a consultative group that has wide representation from the [school/academy] community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives. Depending on the size or structure of the school/academy this group may be part of the safeguarding group. The group will also be responsible for regular reporting to the Full Governing Body.

2. Membership

2.1. The online safety group will seek to include representation from all stakeholders.

The composition of the group should include (N.B. in small schools/academies one member of staff may hold more than one of these posts):

[add/delete where appropriate]

- SLT member/s
- Child Protection/Safeguarding officer
- Teaching staff member
- Support staff member
- Online safety coordinator (not ICT coordinator by default)
- Governor
- Parent/Carer
- ICT Technical Support staff (where possible)
- Community users (where appropriate)
- *Student/pupil representation – for advice and feedback. Student/pupil voice is essential in the make-up of the online safety group, but students/pupils would only be expected to take part in committee meetings where deemed relevant.*

2.2. Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

2.3. Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

2.4. Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature

2.5. When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

3. Chairperson

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying committee members;
- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;

- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

4. Duration of Meetings

Meetings shall be held [insert frequency] for a period of [insert number] hour(s). A special or extraordinary meeting may be called when and if deemed necessary.

5. Functions

These are to assist the Online Safety Lead (or other relevant person) with the following [add/delete where relevant]:

- To keep up to date with new developments in the area of online safety
- To (at least) annually review and develop the online safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the online safety policy
- To monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching/learning/training.
- To co-ordinate consultation with the whole school/academy community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. This could be carried out through [add/delete as relevant]:
 - Staff meetings
 - Student/pupil forums (for advice and feedback)
 - Governors meetings
 - Surveys/questionnaires for students/pupils, parents/carers and staff
 - Parents evenings
 - Website/VLE/Newsletters
 - Online safety events
 - Internet Safety Day (annually held on the second Tuesday in February)
 - Other methods
- To ensure that monitoring is carried out of Internet sites used across the school/academy
- To monitor filtering/change control logs (e.g. requests for blocking/unblocking sites).
- To monitor the safe use of data across the school/academy
- To monitor incidents involving cyberbullying for staff and pupils

6. Amendments

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority

The above Terms of Reference for [insert name of organisation] have been agreed

Signed by (SLT):

Date:

Date for review:

Acknowledgement

This template terms of reference document is based on one provided to schools/academies by Somerset County Council

Legislation

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

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

Computer Misuse Act 1990

This Act makes it an offence to:

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

School/academies may wish to view the National Crime Agency website which includes information about ["Cyber crime – preventing young people from getting involved"](#). Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works with schools to encourage young people to make positive use of their cyber skills. There is a useful [summary of the Act on the NCA site](#).

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.

The Data Protection Act 2018:

Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

- Facilitate the secure transfer of information within the European Union.
- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
- Give the public confidence about how businesses can use their personal information.
- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.
- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.

All data subjects have the right to:

- Receive clear information about what you will use their data for.
- Access their own personal information.
- Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
- Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
- Prevent or query about the automated processing of their personal data.

Freedom of Information Act 2000

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

Communications Act 2003

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

Malicious Communications Act 1988

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

Regulation of Investigatory Powers Act 2000

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

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

Trade Marks Act 1994

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

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a

way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

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

Criminal Justice & Public Order Act 1994

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

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

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A 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>)

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent/carers 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)

Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

For further guidance or support please contact the [Revenge Porn Helpline](#)

Links to other organisations or documents

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

UK Safer Internet Centre

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

South West Grid for Learning – <https://swgfl.org.uk/products-services/online-safety/>

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

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

Revenge Porn Helpline – <https://revengepornhelpline.org.uk/>

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

Report Harmful Content – <https://reportharmfulcontent.com/>

CEOP

CEOP – <http://ceop.police.uk/>

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

Others

[LGfL – Online Safety Resources](#)

[Kent – Online Safety Resources page](#)

INSAFE/Better Internet for Kids – <https://www.betterinternetforkids.eu/>

UK Council for Internet Safety (UKCIS) – <https://www.gov.uk/government/organisations/uk-council-for-internet-safety>

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/>

360Data – online data protection self-review tool: www.360data.org.uk

SWGfL Test filtering – <http://testfiltering.com/>

UKCIS Digital Resilience Framework – <https://www.gov.uk/government/publications/digital-resilience-framework>

Bullying/Online-bullying/Sexting/Sexual Harassment

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

SELMA – Hacking Hate – <https://selma.swgfl.co.uk>

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 – Cyberbullying guidance and practical PSHE toolkit:

<http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit>

[Childnet – Project deSHAME – Online Sexual Harrassment](#)

[UKSIC – Sexting Resources](#)

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

[Ditch the Label – Online Bullying Charity](#)

[Diana Award – Anti-Bullying Campaign](#)

Social Networking

Digizen – [Social Networking](#)

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

[Children’s Commissioner, TES and Schillings – Young peoples’ rights on social media](#)

Curriculum

SWGfL Evolve - <https://projectevolve.co.uk>

[UKCCIS – Education for a connected world framework](#)

Teach Today – www.teachtoday.eu/

Insafe - [Education Resources](#)

Data Protection

[360data - free questionnaire and data protection self review tool](#)

[ICO Guides for Education \(wide range of sector specific guides\)](#)

[DfE advice on Cloud software services and the Data Protection Act](#)

[IRMS - Records Management Toolkit for Schools](#)

[NHS - Caldicott Principles \(information that must be released\)](#)

[ICO Guidance on taking photos in schools](#)

[Dotkumo - Best practice guide to using photos](#)

Professional Standards/Staff Training

[DfE – Keeping Children Safe in Education](#)

DfE - [Safer Working Practice for Adults who Work with Children and Young People](#)

[Childnet – School Pack for Online Safety Awareness](#)

[UK Safer Internet Centre Professionals Online Safety Helpline](#)

Infrastructure/Technical Support

[UKSIC – Appropriate Filtering and Monitoring](#)

[SWGfL Safety & Security Resources](#)

Somerset - [Questions for Technical Support](#)

NCA – [Guide to the Computer Misuse Act](#)

NEN – [Advice and Guidance Notes](#)

Working with parents and carers

[Online Safety BOOST Presentations - parent’s presentation](#)

[Vodafone Digital Parents Magazine](#)

[Childnet Webpages for Parents & Carers](#)

[Get Safe Online - resources for parents](#)

[Teach Today - resources for parents workshops/education](#)

[Internet Matters](#)

Prevent

[Prevent Duty Guidance](#)

[Prevent for schools – teaching resources](#)

[NCA – Cyber Prevent](#)

Childnet – [Trust Me](#)

Research

[Ofcom –Media Literacy Research](#)

Further links can be found at the end of the UKCIS [Education for a Connected World Framework](#)

Glossary of Terms

AUP/AUA	Acceptable Use Policy/Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of National Crime Agency, 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
ICO	Information Commissioners Office
ICT	Information and Communications Technology
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
MAT	Multi Academy Trust
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.
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.
UKCIS	UK Council for Internet Safety
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,

WAP Wireless Application Protocol

A more comprehensive glossary can be found at the end of the UKCIS [Education for a Connected World Framework](#)

Copyright of the SWGfL School Online Safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in January 2020. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal/professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.