Thoughtfulness, Respect and Hard Work

Sandford Hill Primary School

e-Safety Policy

School website: www.sandfordhill.org.uk

Email: office@sandfordhill.org.uk

Thoughtfulness, Respect and Hard Work

Sandford Hill Primary School e-Safety Policy 2022

The e-safety policy supports the National Curriculum for Computing objectives to use technology safely and respectfully.

This policy was last reviewed in the Autumn Term of 2022

This policy has been based upon the approved core e-Safety Policy developed by Stoke on Trent Children and Young People's Service and the SWGFL guidance for Online Safety in schools.

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 the school.

The Education and Inspections Act 2006 empowers Head teachers 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. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The e-Safety Policy will operate in conjunction with other policies including those for pupil Behaviour, Bullying, Curriculum, Data Protection, Security, Mobile Phones, Social Networks, The iPad Home-School Agreement, Remote Learning and also Acceptable Usage Policies for Staff and Pupils.

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 will be appointed to the role of Online Safety Governor. The role of the Online Safety Governor will include:

- meetings with persons with responsibility for online safety
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors / Board / Committee / meeting

Head teacher / Principal and Senior Leaders:

- The Head teacher 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 Leader.
- The Head teacher and the Senior Leadership Team will be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Head teacher / Senior Leaders are responsible for ensuring that the e-Safety Leader 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 Head teacher/ Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the e-Safety Leader.

e-Safety Leader

- works closely alongside the Computing Leader, the Digital Technologies Leader and the Business Operations Leader
- 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

Business Operations Leader / Technical staff

The Business Operations leader and the school's technical staff will ensure:

- 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 and other relevant body Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- 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 school network is regularly monitored in order that any misuse / attempted misuse can be reported to the Head teacher or e-Safety Leader 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 the **Staff Acceptable Use Policy** / Agreement (AUP)
- they report any suspected misuse or problem to the Head teacher/e-Safety Leader for investigation / action / sanction
- 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 (through Apple Classroom where appropriate), mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices **(see Digital Images Policy).**
- 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 materialthat is found in internet searches

Designated Safeguarding Lead

Will 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

Pupils:

- are responsible for using the school digital technology systems in accordance with the **Pupil Acceptable Use Agreement.**
- need to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- will be expected to know and adhere to The Smart Rules
- 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 actionsout 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 and information about national/local online safety campaigns and 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
- their children's personal devices in the school (where this is allowed)

Writing and reviewing of the-Safety policy:

The school will appoint an e-Safety Leader. **This is Mr. I. Walford** who will work alongside the school's designated Child Protection Officer (Mr. D. Wardle) as the roles overlap.

This policy has been written by the school, building on the Stoke-on-Trent e-Safety Policy, guidance from SWGFL and the 360 Safe website (www.360safe.org.uk) and latest government guidance.

The e-Safety Policy and its implementation will be reviewed annually in the Autumn Term.

Useful information:

e-Safety Leader	Mr. I. Walford
Computing Leader	Miss S. Jones
Digital Technologies Leader	Mr. D. Jones
Business Operations Leader	Miss R. Morton
Child Protection Officer	Mr. D. Wardle
Online Safety Governor	Mrs. A. Jackson
School Website	www.sandfordhill.org.uk
Technical Support	Evolve IT Support
Network Monitoring	Securus
WAN issues	TRUSTNet - 01689 814777 Or school controlled
Inappropriate e-mails	TRUSTNet - Or school controlled

1. Teaching and Learning:

The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

All users will be made aware at the beginning of the academic year, and at regular periods throughout the year that use of the school's computers and its network is monitored and recorded using Securus Software.

Discretion and professional conduct is essential at all times.

Members of the Senior Leadership Team will monitor Securus captures and weekly report logs will be stored. Members of the Senior Leadership Team will attend Securus workshops as appropriate.

iPads

The school has moved to 1:1 iPad implementation across Key Stage 2. A risk assessment has been completed and an iPad Acceptable Use Agreement between Home and School is implemented.

The iPad is a tool for teaching and learning to be used under the direction of staff. Through the use of the school's mobile device management systems (Meraki and Apple Classroom) the staff can monitor the individual use of each iPad. Through this system, identified staff can also safely navigate and lock children in and out of a variety of apps and websites. Staff are also aware that if needed, they can lock iPads in order to check history and usage of each individual pupil. The use of Meraki and Apple Classroom, will further enhance our monitoring and e-safety procedures.

Keeping children safe using iPads

Staff are aware that the iPad is a tool to enhance teaching and learning through feedback and creativity. Staff understand that too much screen time is not good for the children. The e-Safety Leader and The Digital Technologies Leader, alongside the teachers will manage the iPads using Meraki/ Apple Classroom. Internet safety filters will be applied to all of the children's iPads. Access to the internet is restricted through LGFL Home Protect, an internet filtered browser. Relevant members of staff will be trained on the use of Apple Classroom which displays a live feed of children's screens to ensure their safe use. Identified members of staff will be able to 'Navigate' and 'Lock' child iPads when appropriate. If children misuse the iPad they may be prohibited from further use. Passcode and fingerprint recognition will be enabled where possible.

1.1 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 provision is mapped coherently within The e Safety Overview and Progression document and will be a focus in all areas of the curriculum. Staff will reinforce online safety messages across the curriculum. The online safety curriculum has been designed to be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum will be provided as part of Computing/PSHE lessons and will be regularly revisited. The school curriculum is aligned to the guidance set out within Education For A Connected World. The school also subscribes to National Online Safety to support staff with resourcing e-Safety lessons All classes will receive at least one e-Safety focused lesson per half term.
- Key online safety messages will be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.
- Pupils will 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 will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students / pupils will be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils will be helped to understand the need for the pupil **Acceptable Use Policies** and encouraged to adopt safe and responsible use both within and outside school.
- Staff will 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 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.
- Where students / 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 (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) 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.

1.2 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, the school website, blog and social media feeds
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. Digital Parenting Magazine, swgfl.org.uk; www.saferinternet.org.uk/

Advice on filtering systems and educational and leisure activities that include responsible use of the internet will be made available to parents.

2. Managing Internet Access

2.1 Information system security

Virus protection (Symantec) will be updated regularly on all networked computers.

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 children are provided with a unique username and secure password. Users areresponsible for the security of their username and password
- The "master / administrator" passwords for the school ICT system,) will be available to the Head teacher / or other nominated senior leader and kept in a secure place
- The Business Operations Leader is responsible for ensuring that software license logs are accurate and up to date and that regular checks are made to reconcile the number of licenses 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 or filtering provider. Internet use is logged and regularly monitored.
- **Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.**
- School technical staff regularly monitor and records the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.

Staff should use remote access to the school's servers via VPN when off site. This provides the most secure access and greatly reduces the potential for data loss or theft when compared to USB memory sticks/pen drives. All staff can gain access to the secure school server when off-site via VPN (Cisco Secure Mobility Client is installed on staff laptops). Where USB memorysticks are required, these should be encrypted to prevent data loss.

2.2 e-Mail

Pupils may only use approved e-mail accounts on the school system. Pupils must immediately tell a teacher if they receive offensive e-mails. Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

Staff must use their email account responsibly and professionally at all times. The official school e-mail service may be regarded as safe and secure and is monitored. Users should be aware that e-mail communications are monitored. Staff and pupils should therefore use only the school e-mail service to communicate with others when in school, or on school systems (e.g. by remote access).

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 students / pupils or parents / carers (email, social media, chat, and blogs) must be professional in tone and content.

2.3 Website and web published content

The school's website shall contain the school address, telephone number and a contact e-mail address. No personal information for staff or pupils will be listed on the school website.

Editorial responsibility of the website is restricted to the Head Teacher, the e-safety Leader and the school's Business Operations Leader. Staff and class teachers will be responsible for blogging as a method of home-school communication.

2.4 Publishing of images

In accordance with the school's **Digital Images Policy**, any images that are published to the internet (either for use on the school's website or in any blogs) will be selected carefully and will not enable individual pupils to be clearly identified. **Written permission from parents or carers** will be obtained before images of pupils are electronically published to the web. The e Safety leader will ensure a list of children who do not have permission to publish digital images is maintained and will ensure that staff are familiar with this list.

2.5 Social networking

Staff and governors are strongly advised to refer to the school's **Social Networking Policy** for further guidance on the use of social networks.

The school will block/filter access to social networking sites, except those specifically purposed to support educationally approved practice. Newsgroups will be blocked unless a specific use is approved.

School staff and governors should ensure that:

- First name only reference should be made in social media to pupils, parents / carers or given names (example Mr. Walford) for school staff
- No personal information should be disclosed on social networks or in any online space.
- 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

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 Head Teacher, Assistant Head Teacher, Business Operations Leader and Digital Technologies Leader will take editorial responsibility for the school Twitter (@sandford_hill) and Facebook (@sandfordhillprimary) accounts. The accounts are to be used to broadcast school related news and publicise events, celebrate successesand promote awareness of other pertinent issues that parents or carers may need to be aware of. Only the persons mentioned above will have access to the account to make tweets and edit the account toensure that content is accurate and appropriate. In order to protect itself from inappropriate content being distributed into its news feed, the Twitter account will not actively seek to follow other Twitter users. Exceptions may be made where following other users has obvious benefits to the school. This will be decided on a case-by-case basis, at the discretion of the SLT and Online Safety Coordinator.

2.6 Misuse of internet access

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 (e.g. 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		

2.7 Managing filtering

The school will work with Technical Support staff from Evolve and Network Support Staff from the broadband provider, LGFL, to ensure that systems are in place to protect pupils, and that these systems are regularly reviewed and improved. As a school, we are aware that e-Safety does not stand still, and that new threats online can present themselves rapidly. As a result, all staff need to monitor local and national government guidance regularly to ensure that any new issues are made aware to staff and pupils as appropriate.

If staff or pupils discover an unsuitable site, the URL (website address) must be reported to the school filtering manager (Mrs J. Wildgoose) or the e-Safety leader or internet provider helpdesk (via Mrs J. Wildgoose).

2.8 Managing remote teaching/videoconferencing

Full IP video conferencing will use the national educational or the school's broadband network to ensure quality of service and security. All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.

Pupils must always ask permission from the supervising teacher before making or answering a video conference call.

Video conferences will be supervised appropriately for the age of the pupils. Video conferencing, will be delivered through Office 365 and when delivered, only during school hours. Default Department for Education Security settings are applied- the children's access to initiate video conferencing is denied. When members of staff need, to video conference groups of children, this will be done via prior agreement with the Headteacher.

2.9 Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out and protocols established before use in school is allowed.

Pupils are not allowed to use mobile phones in school. Those children needing to bring a mobile phone into school will be required to complete a **parental permission form**. Pupil phones will be kept safe in the school office during the school day and then collected from the office at the end of the school day.

Staff are strongly advised to refer to the **School Mobile Phone policy** for further guidance.

Staff can ask to be issued with the school phone (stored in the downstairs office) where text or mobile contact with pupils is required.

3. Policy decisions

3.1 Authorising Internet Access

The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications, which includes internet access. The record will be kept up to date, for instance a member of staff may leave, or a pupil's access may be withdrawn. The Business Operations Leader will be responsible for this record keeping.

All staff must read and sign the **'Staff information systems code of conduct'** before using any school ICT resource.

At EYFS/Key Stage 1, access to the internet will be by adult demonstration or by directly supervised access to specific, approved online materials.

Parents will be asked to sign and return Acceptable Usage Policies and consent forms to authorise internet access for pupils. This information is contained within the Pupil Information Booklets sent out to all parents at the start of the children's time at Sandford Hill Primary School.

Sanctions for inappropriate use will be enforced. These may include notifying parents and/or prohibiting a user from accessing the internet. Additional guidance is provided in Appendix 1.

3.2 Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of online content, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor local authority can accept liability for material accessed online, or for any consequences of internet access.

The school will annually audit ICT provision to establish if the e-Safety Policy is adequate and that the implementation of the e-Safety Policy is appropriate.

3.3 Handling e-Safety complaints

A senior member of staff will deal with complaints of internet misuse.

Any complaint about staff misuse must be referred to the Head teacher.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. More information can be found in the school's **Safeguarding Policy**.

3.4 Cyber bullying

The school will take all reasonable precautions to prevent cyber bullying whilst pupils are in its care. However, due to the global and connected nature of new technologies, it is not possible to guarantee that inappropriate use via a school device (computer or tablet device) will not occur. Neither the school nor the local authority can accept liability for inappropriate use, or any consequences resulting outside of school.

The school will proactively engage with Key Stage 2 pupils in preventing cyber bullying by:

- Understanding and talking about cyber bullying – the inappropriate use of e-mails, text messages or social networking apps.
- Keeping existing policies and practices up to date with new technologies.
- Ensuring easy and comfortable procedures for reporting (including CEOP and Whisper methods of reporting incidents)
- Promoting the positive use of technology
- Evaluating the impact of prevention activities.

Records of e-Safety incidents such as cyber bullying will be kept by the e-Safety Leader and will be used to help to monitor the effectiveness of the school's prevention activities.

3.5 Handling cyber bullying incidents

Any complaints of cyber bullying will be dealt with by a senior member of staff.

Evidence of offending messages, pictures or online conversations will be kept, in order to demonstrate to others what is happening. It can be used by the school, internet service provider, mobile phone company or the police to investigate cyber bullying.

Stakeholders will be made aware that they are able to report issues via the 'Whisper' button, which is embedded on the home page of the school website. (www.sandfordhill.org.uk) Half termly reminders will be given regarding this method of disclosure.

4. Communications Policy

4.1 Introducing thee-Safety Policy to pupils

The SMART and e-Safety rules will be posted in all networked rooms and discussed with pupils regularly throughout the year. Pupils will also be shown how to report concerns using the Whisper button, and will be reminded of the button regularly throughout the year.

Pupils in all classes will be informed that network and internet use is monitored. The relevant **pupils e-Safety Rules** will be explained to the pupils at the start of the year and should be regularly reinforced.

An e-Safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.

Instruction in responsible and safe internet use should precede any internet access. e-Safety will be delivered throughout the year. A minimum of 1 computing or other lesson per half term should be dedicated to promoting e-Safety and digital citizenship.

4.2 Staff and the e-Safety Policy

It is essential that all staff read and understand the e-Safety Policy. The policy will be circulated to all staff, and ready access will be available via the school's secure servers. The application and importance of the policy will be explained.

Staff will 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 Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The e-Safety Leader/ Business Operations Manager will provide advice / guidance / training to individuals as required.

Staff may be issued with a laptop to support their professional duties. The Business Operations Leader will keep a signed record of those issued with a laptop. Staff laptops will be monitored using Forensic Software and staff will be made aware of this.

In addition, staff may also be issued with an iPad to support their professional duties. Before an iPad is issued to a member of staff, a training session will be held and the member of staff will be made aware of the **iPad User Policy.** The Business Operations Leader will keep a signed record those issued with an iPad.

Although the school makes every effort to ensure the integrity and backup of data held by the organisation, users are advised and required to ensure that they have a backup copy of all of their academic data and teaching resources. Any USB devices used for this purpose should be encrypted to ensure that any sensitive data located on the device is secure.

4.3 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 technology / online safety / health and safety /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.

4.4 Passwords

All users (staff or pupils) should have an alphanumeric password, which contains letters, numbers and punctuation. All users should not disclose their password to anyone else other than an ICT manager when requested.

Staff should always lock their computer when not in use.

4.5 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.

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:

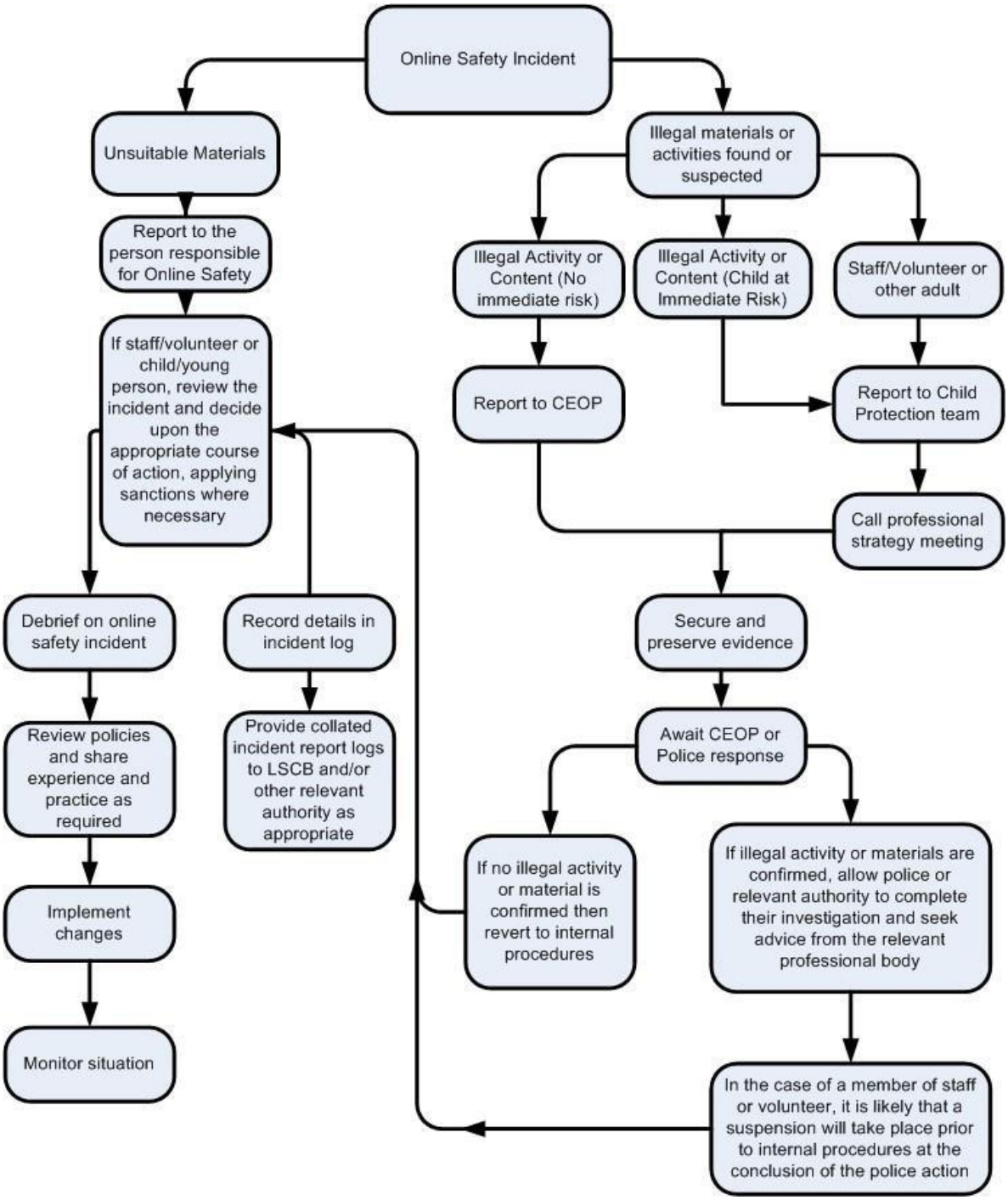
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.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

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.



Appendix 1

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:

	Actions / Sanctions								
Students / Pupils Incidents	Refer to class teacher / tutor	Refer to Online Safety Coordinator	Refer to Head teacher	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 e.g. 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			
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 / academy network by sharing username and passwords		X			X				
Attempting to access or accessing the school / academy network, using another student's / pupil's account	X	X			X				
Attempting to access or accessing the school / academy network, using the account of a member of staff		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						
Continued infringements of the above, following previous warnings or sanctions			X			X			
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school			X						
Using proxy sites or other means to subvert the school's / academy's filtering system		X	X		X				
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X							
Deliberately accessing or trying to access offensive or pornographic material	X	X	X		X				
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X	X						

Thoughtfulness, Respect and Hard Work

Actions / Sanctions

Staff Incidents	Refer to Online Safety Coordinator	Refer to Head teacher 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	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X					X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X					X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X					X		
Actions which could compromise the staff member's professional standing		X				X		
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy		X				X		
Using proxy sites or other means to subvert the school's / academy's filtering system	X						X	
Accidentally accessing offensive or pornographic material and failing to report the incident	X					X		
Deliberately accessing or trying to access offensive or pornographic material	X							X
Breaching copyright or licensing regulations	X					X		
Continued infringements of the above, following previous warnings or sanctions		X						X

Appendix 2

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 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 inprison

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

The Education and Inspections Act 2011
Extended the powers included in the 2006 Act and gave permission for Head teachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.
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)

Keeping Children Safe in Education 2016 – Annex C (page 62 and 63)

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify intervene in and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material;
- Contact: being subjected to harmful online interaction with other users; and
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

Filters and monitoring

Governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place. Whilst considering their responsibility to safeguard and promote the welfare of children, and provide them with a safe environment in which to learn, governing bodies and proprietors should consider the age range of their pupils, the number of pupils, how often they access the IT system and the proportionality of costs vs risks.

The appropriateness of any filters and monitoring systems are a matter for individual schools and colleges and will be informed in part by the risk assessment required by the Prevent Duty.

The UK Safer Internet Centre has published guidance as to what "appropriate" might look like:
Guidance on e-security is available from the National Education Network-NEN. Buying advice for schools is available here: buying for schools.

Whilst filtering and monitoring are an important part of the online safety picture for schools and colleges to consider, it is only one part. Governors and proprietors should consider a whole school approach to online safety. This will include a clear policy on the use of mobile technology in the school. Many children have unlimited and unrestricted access to the internet via 3G and 4G in particular and the school and college should carefully consider how this is managed on their premises.

Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

Staff training

Governors and proprietors should ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training (paragraph 64) and the requirement to ensure children are taught about safeguarding, including online (paragraph 68), that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

Information and support

There is a wealth of information available to support schools and colleges to keep children safe online (See Appendix 3).

Appendix 3

Useful websites

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 – e-security

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 - it's not chalk and talk anymore!"
Ofcom – Children & Parents – media use and attitudes report - 2015