

ALUMNIS

Inspiring Changemakers

Online Safety Policy

Date approved:	29/09/2026
Approved by:	Executives
Version:	5.1
Date for Review	September 2027

Version History

Version	Date Issued	Brief Summary of Change	Owners Name
0.1	04.02.2020	New Policy	Wendy Ainscough
1.1	01.09.2020	Annual Review	Wendy Ainscough
2.1	07.02.2021	Annual Review	Wendy Ainscough
3.1	06.09.2022	Annual Review	Wendy Ainscough
4.1	05.09.2023	Annual Review	D Railston
5.1	2026	Targeted 2026 review; updated KCSIE, filtering and monitoring, generative AI, mobile device, data protection, incident and transfer arrangements	Alumnis

Development / Monitoring / Review of this Policy

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

This policy should be read with the Trust's Safeguarding and Child Protection Policy, Acceptable Use arrangements, Behaviour Policy, Cyber Security Policy, Data Protection Policy and school mobile phone arrangements. It must also reflect current Keeping Children Safe in Education (KCSIE) and Department for Education filtering and monitoring standards.

- The Trust Leadership Group
- Online Safety Coordinators
- Staff – including Teachers, Support Staff, Technical staff
- Board of Directors
- Local School Committee

Schedule for Monitoring and Review

The implementation of this Online Safety policy will be monitored by the:	The Local Schools Committee / Designated Safeguarding Lead
Monitoring will take place at regular intervals:	Termly, with a recorded review of filtering and monitoring at least annually and after significant change or incident
The Board of Directors 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:	Annually
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	September 2027
Should serious online safety incidents take place, the following external persons / agencies should be informed:	LA Safeguarding Officer, LADO, Police, Trust Central Team

The school will monitor the impact of the policy using:

Monitoring should include documented checks that filtering and monitoring systems are working effectively on relevant internet-connected devices and services, that alerts and

reports reach the appropriate staff, and that identified actions are followed through. The frequency of technical checks should reflect the school's risk profile.

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

Scope of the Policy

This policy applies to all members of the Trust community (including staff, pupils, volunteers, parents/carers, visitors and community users) who access or use Trust digital technology systems, whether on school premises, remotely or through school-provided services. It applies to online activity where there is a relevant connection with the school and its safeguarding, behaviour or employment responsibilities.

Schools may take proportionate action in response to online behaviour outside school where there is a sufficient connection to school life and where the relevant behaviour and safeguarding powers apply. Action will be taken in accordance with current law, the Behaviour Policy and safeguarding procedures.

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:

Board of Directors

The Board/Trustees are responsible for approval and oversight of the Online Safety Policy. Oversight may be delegated to the appropriate committee, but the Trust should receive assurance that online safety, filtering and monitoring are effective and that identified risks are being addressed.

In each school a member of the Local Schools Committee has taken on the role of Online Safety Lead Committee Member, this forms part of the responsibilities of the Child Protection / Safeguarding Lead.

The role of the Online Safety Lead Committee Member will include:

The safeguarding/governance oversight role should include assurance that filtering and monitoring arrangements have been reviewed, that concerns identified through monitoring are acted upon, and that online safety training and curriculum provision remain current.

- regular meetings with the Online Safety Co-ordinator / Headteacher
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Local Schools Committee / meeting

Headteacher and Senior Leaders

- The Headteacher has overall responsibility for ensuring the safety of members of the school community, including online safety, while day-to-day responsibilities may be delegated. The Headteacher and at least one other senior leader should understand the procedures for serious online safety and safeguarding incidents involving pupils, staff or other members of the community.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority / MAT / other relevant body disciplinary procedures).
- The Headteacher is responsible for ensuring that the Online Safety Lead, DSL and other relevant staff receive suitable online safety and safeguarding training, including the expectations for filtering and monitoring and emerging risks such as generative AI, harmful content, online sexual abuse, cyberbullying and misinformation.
- 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 Online Safety Lead.

Online Safety Lead:

- leads the Online Safety Group;
- takes day-to-day responsibility for online safety issues and leads the review of online safety policies, filtering/monitoring arrangements and related safeguarding processes;

- 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 Trust Central Team;
- liaises with Trust technical staff;
- receives reports and relevant monitoring alerts relating to online safety and maintains an appropriate incident/action log so that trends, recurring concerns and required improvements can be identified;
- meets regularly with Online Safety Local Schools Committee Member to discuss current issues, review incident logs and filtering / change control logs;
- attends relevant Local Schools Committee Meetings;
- reports regularly to the Senior Leadership Team.

Technical staff

The IT technical lead is responsible for ensuring:

- that the schools technical infrastructure is secure and is not open to misuse or malicious attack;
- that the school meets required online safety technical requirements and any Trust Online Safety Policy / Guidance that may apply;
- that users access networks and devices through appropriately secure authentication arrangements, including multi-factor authentication where supported and appropriate, and that compromised credentials are dealt with promptly;
- the filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- 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 network, internet, remote access, email and relevant application activity is monitored where appropriate and lawful, with reports and alerts provided to the relevant DSL/Online Safety Lead and Trust technical staff for investigation or action;
- that filtering and monitoring systems are implemented, maintained, checked and reviewed in accordance with current DfE standards, the school's risk assessment and Trust procedures;

Teaching and Support Staff

Are responsible for ensuring that:

- they maintain current awareness of online safety and the school's current policy and practices, including emerging risks and reporting routes;

- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP);
- they report suspected misuse, safeguarding concerns, phishing/cyber incidents or problems with filtering/monitoring promptly to the appropriate safeguarding/technical contact;
- all digital communications with 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 (where allowed) and implement current policies with regard to these devices;
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Lead

Should be appropriately trained in online safety and understand the potential for 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;
- online-bullying.

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the Trust community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. The Group will consist of the Online Safety Leads from each school within the Trust. The group will also be responsible for regular reporting to the Board of Directors.

Members of the Online Safety Group will assist with:

- the production / review / monitoring of the Trust Online Safety Policy / documents;
- the production / review / monitoring of the Trust filtering policy (and requests for filtering changes;

- mapping and reviewing the online safety / digital literacy curricular provision – ensuring relevance, breadth and progression;
- monitoring network / internet / incident logs;
- consulting stakeholders – including parents / carers and the pupils about the online safety provision;
- monitoring improvement actions identified through use of the 360 degree safe self-review tool.

Pupils:

- are responsible for using the school digital technology systems in accordance with the Student / 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, bullying, exploitation, inappropriate contact, harmful content or misuse and know how to do so safely and confidentially;
- 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 online-bullying.
- should understand the importance of safe and responsible online behaviour both inside and outside school, including the risks associated with social media, gaming, messaging, live streaming, sharing images, scams, misinformation and generative AI;

Parents / Carers

Parents/carers play a crucial role in helping children understand safe and responsible internet and mobile-device use. Schools will provide accessible information and signposting about current online risks and encourage parents/carers to raise concerns with the school promptly.

- digital and video images taken at school events;
- access to parents' sections of the website / Learning Platform and on-line student / pupil records.

Community Users

Community Users who access school systems / website / Learning Platform as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school.

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are important, educating pupils to recognise, assess and manage online risks is an essential part of safeguarding. Online safety education should be developmentally appropriate, inclusive and regularly updated to reflect emerging technologies and risks.

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

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited ;
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities;
- Pupils should be taught to evaluate online content critically, understand how algorithms, advertising and AI-generated content can influence what they see, and check information using reliable sources.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Pupils should be supported to recognise and respond safely to harmful extremist or terrorist content, radicalisation risks and manipulative online activity, in accordance with the school's Prevent and safeguarding arrangements.
- 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 search the internet, staff should remain vigilant and the school's filtering and monitoring systems should operate as intended. Filtering should not be bypassed by pupils or staff and should not unreasonably restrict legitimate teaching and learning.
- Where legitimate teaching requires access to material that may normally be blocked, any temporary filtering exception must be authorised through the school's documented process, be proportionate and time-limited, be recorded, and be reviewed to ensure that appropriate safeguarding controls remain in place.

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 online 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, 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
www.saferinternet.org.uk/ <http://www.childnet.com/parents-and-carers>

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in the use of new digital technologies, digital literacy and online safety;
- Online safety messages targeted towards grandparents and other relatives as well as parents;
- The school website will provide online safety information for the wider community;
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their Online Safety provision

Education & Training – Staff / Volunteers

All staff must receive online safety training as part of safeguarding training and induction, with updates at least annually and additional updates where risk or significant change indicates a need. Training should cover the staff member's role in online safety, filtering and monitoring, reporting concerns, cyber security and emerging risks including AI.

- 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.
- The Online Safety Lead (or other nominated person) will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Lead will provide advice / guidance / training to individuals as required.

Training – Directors / Local Schools Committee Members

Directors / Local Schools Committee Members should take part in online safety training / awareness sessions, with particular importance for those who are Lead Members for health and safety / safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / Trust / National Governors Association / or other relevant organisation (e.g. SWGfL).
- Participation in school training / information sessions for staff or parents.

Technical – infrastructure / equipment, filtering and monitoring

The Trust will ensure that infrastructure and network arrangements support safe and secure use of technology and that filtering and monitoring are implemented in accordance with current DfE standards, KCSIE and the school's risk profile. The governing body/proprietor, DSL/safeguarding lead and IT support should work together on oversight and review.

- 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 Trust 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;
- Users are responsible for protecting their credentials. Passwords must be strong and unique, must not be shared, and must be changed promptly where compromised.

Multi-factor authentication should be used where supported and appropriate. Routine password changes should follow the Trust's current cyber security standard rather than an automatic 30-day cycle.

- The “master / administrator” passwords for the Trust ICT systems, used by the Network Manager (or other person) must also be available to the Trust Business Manager and kept in a secure place.
- The Trust 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 should be appropriately filtered and monitored for users, with particular attention to safeguarding children. Filtering should address illegal, inappropriate and potentially harmful content, including relevant AI-generated content, and should be configured so that users cannot simply bypass required safeguards.
- Internet filtering and monitoring must take account of terrorist and extremist material and other safeguarding risks identified through the school's risk assessment. The effectiveness of these controls must be reviewed and recorded at least annually and after significant change or incident.
- The Trust will use differentiated filtering and monitoring appropriate to user age, role and risk wherever the technical solution supports this.
- Trust technical staff will maintain and review monitoring arrangements, and reports/alerts will be available to the DSL or Online Safety Lead for safeguarding action. Monitoring must be lawful, proportionate and transparent and should align with the Trust's data protection and privacy arrangements.
- An appropriate system must be in place for users to report any actual or potential technical incident, cyber security concern, harmful online content or safeguarding concern, with clear escalation routes to both IT and the DSL where relevant.
- 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.
- An agreed procedure is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technologies (including BYOD/BYOT)

The school's mobile phone arrangements must also reflect the Department for Education statutory guidance on mobile phones in schools. From 1 September 2026, schools should follow the statutory guidance requiring schools to prohibit the use of mobile phones throughout the school day, subject to the limited exceptions and context described in the guidance. Any local exceptions must be clearly set out in the school's mobile phone policy and supported by safeguarding considerations.

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 use of mobile/personal devices in school is subject to the school's mobile phone, BYOD, acceptable use, safeguarding and data protection arrangements. Personal devices must not be used to capture, store or transmit pupil or staff personal data or images for school purposes unless specifically authorised and appropriately secured.

- The school Acceptable Use Agreements for staff, students and parents / carers will give consideration to the use of mobile technologies

The school allows:

	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	No	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only	Yes	Yes	Yes	No	No	Yes
No network access	No	No	No	No	No	No

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

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.

Personal devices:

- Which users are allowed to use personal mobile devices in school (staff / pupils / 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.

Generative AI and manipulated content

The school recognises that generative AI can create or alter text, images, audio and video and may be used to produce misinformation, impersonation, bullying or harmful sexual imagery. Online safety education, filtering and monitoring, image-use arrangements and incident response should take account of these risks. Pupils and staff should be taught not to create, share or request harmful or non-consensual intimate imagery and to report concerns promptly.

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.
- The school will use an appropriate lawful basis and its published image/photography arrangements when taking or publishing photographs of pupils. Consent will be obtained where consent is the appropriate lawful basis, and permissions will be recorded and managed consistently.
- Parents/carers may be permitted to take images for personal use at school events where the school allows this, but they should be reminded to respect the privacy and safeguarding of other children and to follow the school's event and image guidance. Images should not be shared publicly where this would identify or affect other children without an appropriate basis.
- Staff and volunteers may only take images for legitimate educational or safeguarding purposes using school-approved equipment or systems and in accordance with the Trust's image, data protection and acceptable use arrangements. Personal devices should not be used for school photography unless specifically authorised under the Trust's procedures.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available in accordance with current UK data protection law, the Trust's Data Protection Policy and applicable privacy notices.

The school must ensure that:

- It has a Data Protection Policy.
- It will meet any current statutory data protection registration/fee requirements that apply to the Trust, and will maintain the appropriate ICO registration and documentation.
- It has appointed a Data Protection Officer (DPO). The school may also wish to appoint a Data Manager and systems controllers to support the DPO.

- 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.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIAs) will be carried out where required, including for high-risk monitoring, filtering or new technology processing.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

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							
	Allowed	ertain times	ected staff	Not allowed	Allowed	ertain times	d with staff permission	ot allowed
Communic ation Technologi es								
Mobile phones may be brought to the school								
Use of mobile phones in lessons								
Use of mobile phones in social time								
Taking photos on personal mobile phones / cameras								
Taking Photos on School owned devices								
Use of other personal mobile devices								

e.g. tablets, gaming devices								
Use of school owned other mobile devices e.g. tablets, gaming devices								
Use of personal email addresses in school , or on school network								
Use of school email for personal emails								
Use of messaging apps								
Use of social media								
Use of blogs								

When using communication technologies the Trust considers the following as good practice:

- The official Trust email and approved communication services must be used for school business. Where communications or activity are monitored for safeguarding, security or compliance, staff and pupils must be informed through the Trust's acceptable use, privacy and monitoring arrangements.
- Users must promptly report communications or online activity that is uncomfortable, offensive, discriminatory, threatening, bullying, exploitative or otherwise concerning to the appropriate safeguarding or management route, and should not engage with or escalate the communication unnecessarily. <https://boost.swgfl.org.uk/>
- 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, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or Trust liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues. Online Safety BOOST includes unlimited webinar training on this subject: <https://boost.swgfl.org.uk/>
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- Staff must not identify or discuss individual pupils, parents/carers or colleagues on personal social media in a way that could breach confidentiality, safeguarding, professional boundaries or data protection requirements.
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school /academy or local authority / MAT
- Staff should maintain appropriate privacy and security settings on personal social media accounts and should consider the professional and safeguarding implications of publicly visible content.

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

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

Personal Use:

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

Monitoring of Public Social Media

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

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies. Online Safety BOOST includes Reputation Alerts that highlight any reference to the school in online media (newspaper or social media for example) <https://boost.swgfl.org.uk/>

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:

The list should not be treated as exhaustive. New forms of online harm, including AI-generated or manipulated sexual imagery, sextortion, cyberflashing, scams, harmful challenges and misuse of generative AI, may also constitute safeguarding concerns or breaches of school policy.

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	

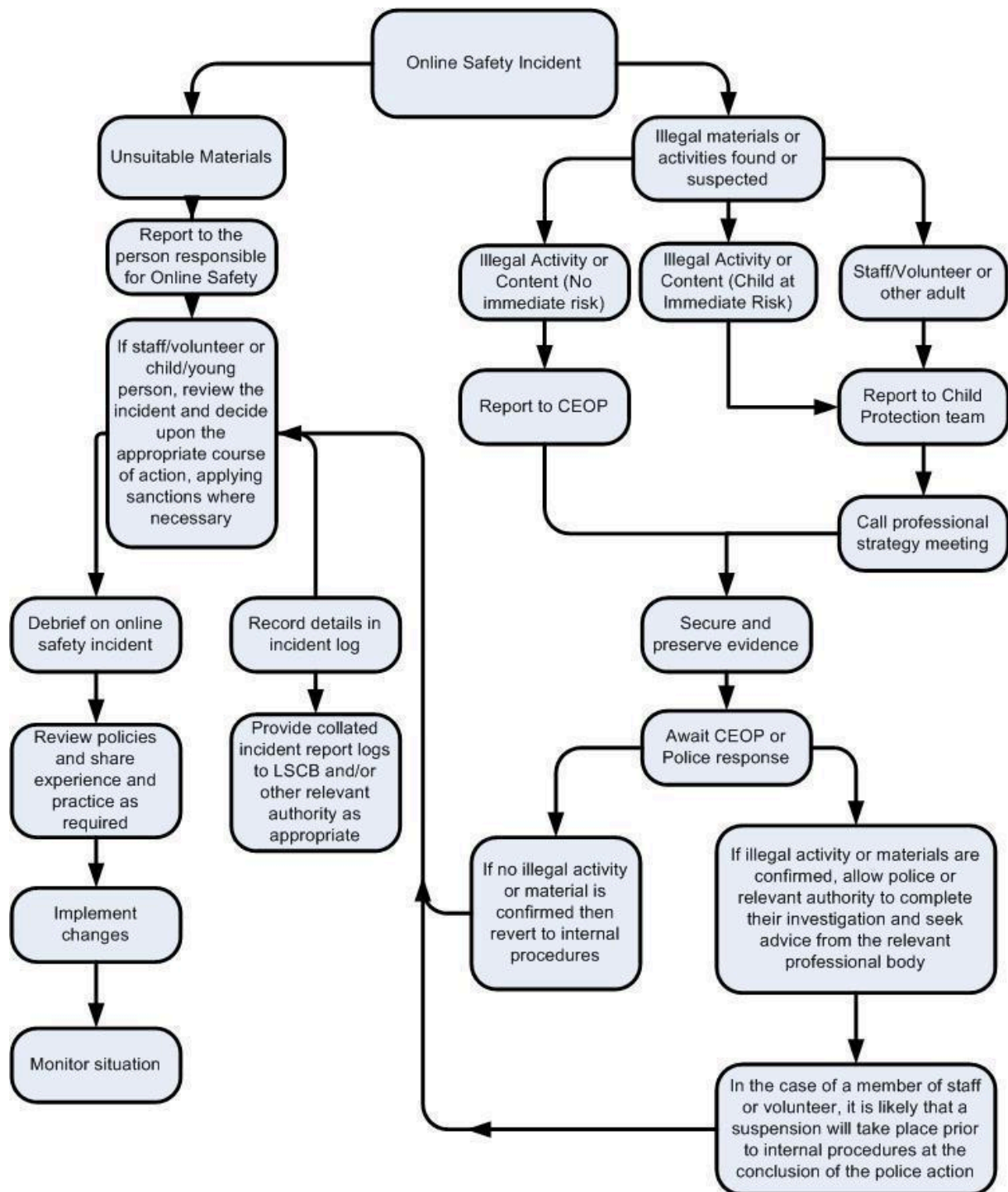
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					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 (see “User Actions” above). Online Safety BOOST includes a comprehensive and interactive ‘Incident Management Tool’ that steps staff through how to respond, forms to complete and action to take when managing reported incidents (<https://boost.swgfl.org.uk/>)

Illegal Incidents

If there is any suspicion that online material involves child sexual abuse material or other suspected criminal activity, staff should stop viewing or accessing the material, avoid copying or distributing it, preserve relevant information where safe to do so, and report immediately through the safeguarding lead and to the police/appropriate authority in accordance with current safeguarding procedures.



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:

- Where an incident requires investigation, more than one appropriately authorised senior member of staff should be involved where practicable. Staff should avoid unnecessary viewing, downloading or copying of harmful material and should follow the Trust's safeguarding, data protection and incident management procedures.
- 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 relevant URL, account, message or service details and a factual description of the concern where this can be done safely. Do not download, copy or circulate illegal sexual images or other harmful content. Preserve evidence only as directed by the safeguarding lead, IT support or police.
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Local Authority / Academy Group or national / local organisation (as relevant).
 - Police involvement and/or action
- If content being reviewed includes suspected child sexual abuse material, do not continue viewing or copying the material unnecessarily. Refer immediately through the safeguarding lead and appropriate law-enforcement/child-protection channels. Staff should not conduct their own investigation.
 - 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

Most incidents will involve inappropriate rather than criminal misuse. Incidents should be addressed promptly, proportionately and consistently through safeguarding, behaviour, staff conduct/disciplinary and technical procedures as appropriate. Any sanction should take account of the pupil's age, understanding, SEND/disability and the circumstances of the incident.

Actions / Sanctions

	Refer to class teacher / tutor	Refer to Head of Department / Year / other	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning (add to CPOMS)	Further sanction eg detention / exclusion	Refer to DPO
Pupils Incidents										
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	X				X				
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X		X			X		X		X
Unauthorised / inappropriate use of social media / messaging apps / personal email	X		X			X		X		
Unauthorised downloading or uploading of files	X		X			X		X		X
Allowing others to access school	X				X					X

network by sharing username and passwords										
Attempting to access or accessing the school network, using another student's / pupil's account	X				X					X
Attempting to access or accessing the school network, using the account of a member of staff	X		X		X			X		X
Corrupting or destroying the data of other users	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		
Continued infringements of the above, following previous warnings or sanctions	X		X	X	X			X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X		X		X					
Using proxy sites or other means to subvert the school's filtering system	X		X		X		X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident	X		X		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		X		X		X	X		X

Actions / Sanctions

		Refer to line manager	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
Staff Incidents									
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		
Inappropriate personal use of the internet / social media / personal email		X					X		
Unauthorised downloading or uploading of files	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		
Careless use of personal data e.g. holding or transferring data in an insecure manner									
Deliberate actions to breach data protection or network security rules									
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software									
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature									
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils									
Actions which could compromise the staff member's professional standing									
Actions which could bring the school into disrepute or breach the									

integrity of the ethos of the school									
Using proxy sites or other means to subvert the school's 's filtering system									
Accidentally accessing offensive or pornographic material and failing to report the incident									
Deliberately accessing or trying to access offensive or pornographic material									
Breaching copyright or licensing regulations									
Continued infringements of the above, following previous warnings or sanctions									

Legislation

Current guidance and standards: this policy should be read alongside Keeping Children Safe in Education 2026, the Department for Education Filtering and Monitoring: Core Standard, the Department for Education Mobile Phones in Schools statutory guidance, the DfE Cyber Security: Core Standard, and the Trust's safeguarding, acceptable use, data protection and cyber security policies. Current guidance takes precedence over older examples or references in this document.

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.

This section is not exhaustive. The Trust will keep its online safety arrangements aligned with current legislation and statutory guidance. Where a serious or unusual incident occurs, advice should be sought from the DSL, Trust HR/legal advisers, DPO, IT lead or relevant safeguarding agency as appropriate.

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.

UK GDPR and Data Protection Act 2018

These laws protect individuals' rights in relation to personal data and require organisations to process personal data lawfully, fairly and transparently, for specified purposes, keep it accurate and no longer than necessary, and protect it appropriately. The Trust must also meet the requirements applying to special category data and criminal offence data where relevant.

- 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.

Investigatory Powers Act 2016 and applicable communications/monitoring regulations

Monitoring of communications must be lawful, necessary and proportionate and must comply with applicable communications, data protection and privacy law. The Trust will explain monitoring arrangements through its acceptable use and privacy information and will only monitor for legitimate purposes such as safeguarding, security, service management, investigation or compliance.

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

Trade Marks Act 1994

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

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

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

Criminal Justice & Public Order Act 1994

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

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

Racial and Religious Hatred Act 2006

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

Protection from Harassment Act 1997

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

Protection of Children Act 1978

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

Sexual Offences Act 2003

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 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 / carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:

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

Serious Crime Act 2015

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

Links to other organisations or documents

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

Current official and specialist resources should be used in preference to older or broken links in this section, including DfE/KCSIE, UK Safer Internet Centre, Childnet, CEOP/Thinkuknow, Internet Watch Foundation, SWGfL and the National Cyber Security Centre.

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>

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

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 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/>

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

Bullying / Online-bullying / Sexting / Sexual Harrassment

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 – 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 Digital Literacy & Citizenship curriculum

UKCCIS – Education for a connected world framework

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

360data - free questionnaire and data protection self review tool

ICO Guide for Organisations (general information about Data Protection)

ICO Guides for Education (wide range of sector specific guides)

DfE advice on Cloud software services and the Data Protection Act

ICO Guidance on Bring Your Own Device

ICO Guidance on Cloud Computing

ICO - Guidance we gave to schools - September 2012

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](#)

Somerset - [Questions for Technical Support](#)

NEN – [Advice and Guidance Notes](#)

Working with parents and carers

[SWGfL Digital Literacy & Citizenship curriculum](#)

[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](#)

[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](#)

Research

[EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011](#)

[Futurelab - "Digital participation - its not chalk and talk any more!"](#)

[Ofcom –Media Literacy Research](#)

Glossary of Terms

AUP / AUA	Acceptable Use Policy / Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes).
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.

VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.

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.

Trust transfer / closure: Where a school transfers to another Trust or employer, online safety arrangements must remain effective until responsibility formally transfers. The handover should include current filtering and monitoring arrangements, technical contacts, safeguarding escalation routes, online safety incident logs, relevant risk assessments, acceptable use arrangements and live safeguarding concerns. The successor Trust should review and adopt its own arrangements without creating a gap in safeguarding protection.