Staffordshire University Academies Trust

Online Safety Policy

Last reviewed	**September 2026**
Reviewed by	**Estates and Compliance Manager**
Approved by	**Trust Board**
Date of approval	**September 2027**
Policy owner	**Estates and Compliance Manager**
Location	**Trust Website**

Online Safety Policy

Purpose

The purpose of this policy is to:

- Ensure the safety and wellbeing of children and staff when using digital technologies.
- Ensure that digital technologies are used appropriately by all who access them.
- Provide staff and volunteers with information to guide and support their approach to online safety.
- Meet statutory obligations and ensure that users of digital technology are protected from harm both on and off site.
- Ensure that, as an organisation, we operate in line with our values, and within the law, in terms of how we use online devices and services.
- Provide clarity about the use of electronic communications equipment, to ensure that they are accessed and used in a manner that is safe and deters users from accessing inappropriate materials.
- Promote awareness and to provide guidance to assist staff in providing safeguards to the children in our Trust.
- Safeguard pupils and staff in using digital technology and in accordance with Keeping Children Safe in Education statutory guidance.
- Ensure that online safety is embedded in our practices.
- Protect our online systems and technology from harm.
- Embed online safety in our cultures and raise awareness of online safety practices, within and for our communities.

The DfE Keeping Children Safe in Education statutory guidance requires Local Authorities, Multi Academy Trusts, and schools in England to ensure pupils are safe from harm:

*"It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to **online safety** empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate."*

*"Governing bodies and proprietors should ensure **online safety** is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how **online safety** is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement."*

The DfE Keeping Children Safe in Education guidance also recommends:

***Reviewing online safety**…Technology, and risks and harms related to it, evolve, and change rapidly. Schools and colleges should consider carrying out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face.*

The DfE Keeping Children Safe in Education guidance advises that:

The breadth of online-safety issues is considerable and continually evolving. The Trust addresses content risks, including illegal and harmful material, extreme sexual or physical violence, misinformation, disinformation and conspiracy theories; contact risks, including harmful interaction

with other users or generative AI applications; conduct risks, including bullying and the making, sending or receiving of explicit images, including AI-generated images; and commerce risks, including gambling, inappropriate advertising, phishing and financial scams.

This Online Safety Policy:

- Sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication.
- Allocates responsibilities for the delivery of the policy.
- Is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours.
- Establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves, the academies and the Trust, and how they should use this understanding to help safeguard pupils in the digital world.
- Describes how academies will help to prepare pupils to be safe and responsible users of online technologies.
- Establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms.
- Is supplemented by a series of related acceptable use agreements contained within the Acceptable Use Policy.
- Is made available to staff at induction, and to parents and carers during admission, and through normal communication channels in each Academy.
- Is published as the Trust's core Online Safety Policy and must not be amended locally. Each Academy will maintain a standard local Online Safety Appendix containing the Academy-specific operational information required by this policy. The Trust core policy and relevant Academy appendix will be made available through the Academy website.

Scope of the Policy

Safeguarding children from online harm forms part of the Trust's wider statutory safeguarding responsibilities. This policy should be read alongside Keeping Children Safe in Education 2026, Working Together to Safeguard Children, the Trust Safeguarding Policy, the Prevent duty guidance, the Department for Education's digital and technology standards and other relevant statutory and non-statutory guidance.

The Trust and its Academies will take a whole-school approach to online safety which reflects children's experiences both online and offline and recognises that technology and associated risks evolve rapidly. Online safety will be considered as an integral part of safeguarding and child protection and will be reflected, as appropriate, in relevant policies, curriculum provision, staff training, filtering and monitoring arrangements and risk management.

The Trust recognises that children's use of the internet, social media, online games, applications, artificial intelligence and other digital technologies provides significant opportunities for learning, communication and development, but may also expose children to safeguarding risks. These include risks arising from content, contact, conduct and commerce, as well as risks associated with harmful or inappropriate content, online sexual harassment and abuse, bullying, exploitation, radicalisation, misinformation and disinformation, and the misuse or manipulation of digital images and other content.

Online-safety education, reporting routes, investigations, sanctions and support will be accessible and responsive to individual need. Academies will consider age, developmental stage, SEND, communication needs, EAL, medical needs, care experience and other factors that may increase vulnerability or create barriers to recognition, disclosure or support. Reasonable adjustments will be made where required.

The Trust also recognises that online safety incidents may occur outside the Academy but have an impact on pupils, staff or the Academy community. Academies will respond to such incidents in accordance with their safeguarding and behaviour responsibilities and relevant legislation and statutory guidance. Where appropriate, this may include action in relation to pupil behaviour outside the Academy and the lawful searching of pupils and confiscation of prohibited or inappropriate items, including electronic devices, in accordance with the Academy Behaviour Policy and current Department for Education guidance.

This policy applies to all members of SUAT's community (including staff, pupils, volunteers, parents / carers, members of the Trust Board, members of the Local Academy Councils, visitors, community users, suppliers) who have access to and are users of SUAT and Academy ICT systems, both in and out of the educational / work setting. It also applies to the use of personal digital technology on Academy sites (where allowed).

SUAT and the Academies will manage online safety incidents and associated behaviour in a manner which is proportionate to the incident, to ensure that pupils and students learn in a supportive, caring and safe environment without fear of bullying and online safety threats, and to defend the right of every child and adult to be happy and secure inside and outside of the educational environment. Academies will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

This Online Safety Policy outlines the commitment of SUAT and our academies to safeguard members of our Trust community, online, in accordance with statutory guidance and best practice. There is an expectation that the required professional standards will be applied to online safety as in other aspects of school life i.e., policies and protocols are in place for the use of online communication technology between the staff and other members of the Trust and wider community, using officially sanctioned mechanisms.

Schedule for Development, Monitoring and Review

The implementation of this Online Safety Policy will be monitored by	Designated safeguarding leads Online safety leads Senior leadership teams
Monitoring will take place at regular intervals	At least annually. Academies will monitor the impact of the policy using: • Logs of reported incidents • Filtering and monitoring logs • Internal monitoring data for network activity • Staff meetings and parental feedback forums • Online safety training • Periodic reviews of pupil images and videos published on Academy websites, official social media accounts and other public-facing online platforms, to identify content that is no longer required, is no longer current or no longer

	meets the requirements of this policy. • Surveys / questionnaires of pupils, parents / carers, staff
Each LAC 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:	At least once per year.
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The identification of a credible new risk involving the copying, harvesting, alteration, AI-enabled manipulation or criminal misuse of pupil images will trigger an earlier review of the Digital and Video Images, Social Media and Online Publishing sections of this policy and the related Academy procedures. The next anticipated review date will be:	September 2027.
Serious online safety incidents will be escalated in accordance with the Trust Safeguarding Policy, Cyber Response Plan and relevant incident-response procedures.	The Designated Safeguarding Lead and/or Headteacher will determine whether referral to the Trust, local authority, police, children's social care or another relevant agency is required, according to the nature of the incident.

1. Roles and Responsibilities

To ensure the online safeguarding of members of our Trust community, it is important that all members of our community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the MAT. It will be important for each individual Academy to ensure that there is a 'separation of responsibility' for roles within their setting.

The Trust Board and Local Academy Councils

The Trust Board are responsible for the approval of the Online Safety Policy.

The Trust Board, as proprietor, retains strategic oversight of online safety across all academies. It will receive at least annual Trust-wide assurance covering completion of academy online-safety risk assessments; filtering and monitoring reviews and checks; significant and recurring incidents; staff training; curriculum assurance; compliance exceptions; and overdue actions. The Trust will undertake proportionate sampling and escalate material weaknesses through its safeguarding and risk-governance arrangements.

Reviewing the effectiveness of the policy will be the responsibility of individual academies and their safeguarding leads, supported by Local Academy Council members, who will receive regular information about online safety incidents and monitoring reports. LAC members can review the effectiveness of the policy and arrangement by asking questions which are posed in the UKCIS

document “Online Safety in Schools and Colleges – questions from the Governing Body,” for example.

This review will be carried out by the relevant link LAC member, Senior Leaders and the Safeguarding / Online Safety Lead, who will receive regular information about online safety incidents and monitoring reports. A member of the LAC will take on the role of Online Safety LAC member, to include:

- Regular meetings with the Designated Safeguarding Lead / Online Safety Lead in their Academy.
- Regularly receiving (collated and anonymised) reports of online safety incidents.
- Checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended).
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible LAC member in-line with the DfE Filtering and Monitoring Standards.
- Reporting back to the full LAC.
- Receiving (at least) basic cyber-security training to enable LAC members to ensure that academies meet the DfE Cyber-Security Standards.
- Membership of the Academy Online Safety Group.

The LAC will also support their Academy in encouraging parents/carers and the wider community to become engaged in online safety activities.

Reports from the LAC will be referred to the Trust Board via Governor Hub.

Principal / Head Teacher and Senior Leaders

- The Principal / Head Teacher has a duty of care for ensuring the safety (including online safety) of members of their Academy community and fostering a culture of safeguarding. Though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The Principal / Head Teacher and 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.
- The Principal / Head Teacher and Senior Leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff, carry out their responsibilities effectively. All staff must receive suitable training to enable them to carry out their roles and the DSL / OSL should be able to train other colleagues, as relevant.
- The Principal / Head Teacher and 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.
- The Principal / Head Teacher and Senior Leadership Team will either receive regular monitoring reports directly from the system, or from the Designated Safeguarding Lead / Online Safety Lead and be made immediately aware of a safeguarding issue.
- The Principal / Head Teacher and Senior Leaders will work with the responsible LAC member, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.
- The Principal / Head Teacher and Senior Leaders will be responsible for ensuring that staff are appropriately trained in online safety and understand the procedures they must follow to a) help mitigate incidents and b) promptly report and manage incidents should they arise.
- The Principal / Head Teacher and Senior Leaders will ensure that responsibility is allocated for reviewing pupil images and videos published on Academy websites, official social media

accounts and other public-facing platforms, and that the outcomes of these reviews and any resulting actions are recorded.

Designated Safeguarding Lead (DSL)

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

- Sharing personal data.
- Access to illegal / inappropriate materials.
- Inappropriate online contact with adults / strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.
- The unauthorised copying, manipulation or AI-enabled misuse of pupil images, including associated coercion, extortion or threats of distribution.

The DSL will:

- Hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online.
- Meet regularly with the online safety LAC member to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out.
- Attend relevant LAC meetings/groups.
- Report regularly to Headteacher / Senior Leadership Team.
- Be responsible for receiving reports of online safety incidents and handling them and deciding whether to make a referral (in conjunction with the Head Teacher / SLT) by liaising with relevant agencies, ensuring that all incidents are recorded.
- Ensure that concerns involving the unauthorised copying, alteration, AI-enabled manipulation or misuse of a pupil's image, including associated coercion, extortion or threats of distribution, are treated as potential safeguarding incidents. Such concerns will be recorded and managed in accordance with the Academy's safeguarding procedures, with referrals made to relevant agencies where appropriate.
- Liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety).

Online Safety Lead (OSL)

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

- Sharing personal data.
- Access to illegal / inappropriate materials.
- Inappropriate online contact with adults / strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.

The Online Safety Lead will:

- Lead the Online Safety Group for their setting.

- Work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL).
- Receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged, to inform future online safety developments.
- Have a leading role in establishing and reviewing Academy online safety policies/documents.
- Promote an awareness of and commitment to online safety education / awareness raising across their Academy and beyond.
- Liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents.
- Provide (or identify sources of) training and advice for staff/LAC members/parents/carers/pupils.
- Liaise with technical staff, pastoral staff and support staff (as relevant).
- Receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by pupils) with regard to the areas defined in Keeping Children Safe in Education:
    - Content
    - Contact
    - Conduct
    - Commerce.

Curriculum Leads
Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme e.g. ProjectEVOLVE .

Each Academy will provide an age- and developmentally appropriate, sequenced online-safety curriculum through Relationships Education, Relationships and Sex Education and Health Education, PSHE, computing and relevant wider curriculum opportunities. Provision will be adapted for pupils with SEND and other vulnerabilities, will address current and emerging risks including generative AI, and will be evaluated using pupil voice, incident intelligence and curriculum assurance.

This will be provided according to each individual Academy's arrangements, and for example, through:

- A discrete programme.
- PSHE, Relationships Education, Relationships and Sex Education and Health Education, as applicable to phase.
- A mapped cross-curricular programme.
- Assemblies and pastoral programmes.
- Through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Teaching and Support Staff
All Academy staff are responsible for ensuring that:

- They have an awareness of current online safety matters/trends and of the current Online Safety Policy and Academy practices.
- They understand that online safety is a core part of safeguarding.
- They have read, understood, and signed the staff acceptable use agreement (AUA).
- They immediately report any suspected misuse or problem to the designated person for investigation/action, in line with the Academy's safeguarding procedures.
- All digital communications with pupils and parents/carers are on a professional level and only carried out using official Academy and Trust 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 agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices.
- Before submitting, selecting or publishing images or videos of Pupils, staff will follow the Digital and Video Images and Online Publishing sections of this policy. This includes checking current permissions and any safeguarding restrictions, considering whether Pupils are clearly identifiable, ensuring that names or other identifying information are not linked to images, and ensuring that images are appropriately prepared before publication. Any uncertainty about whether an image is suitable for publication must be referred to the Designated Safeguarding Lead and, where appropriate, the Data Protection Officer.
- In lessons where internet use is pre-planned pupils are 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 lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies.
- There is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc.
- They model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.
- They follow all relevant guidance and legislation including, for example, Keeping Children Safe in Education 20026 and UK GDPR regulations
- All digital communications with pupils, parents and carers and others should be on a professional level and only carried out using official school systems and devices (where staff use AI, they should only use Trust and Academy-approved AI services for work purposes which have been evaluated to comply with organisational security and oversight requirements.
- They adhere to the data protection and information security policies, with regard to the use of devices, systems and passwords and have an understanding of basic cybersecurity
- They have a general understanding of how the pupils in their care use digital technologies out of school, in order to be aware of online safety issues that may develop from the use of those technologies
- They are aware of the benefits and risks of the use of Artificial Intelligence (AI) services in school, being transparent in how they use these services, prioritising human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated.

ICT Manager / ICT Support Team
If an Academy has an IT / technology service provided by an outside contractor, it is the responsibility of the Academy to ensure that the provider carries out all the online safety measures that the Academy's obligations and responsibilities require. It is also important that the provider follows and implements the Online Safety Policy and procedures.

The IT Provider / Academy IT Team is responsible for ensuring that:

- They are aware of and follow the school Online Safety Policy and Information Security Policy, to carry out their work effectively in line with these policies.
- The Academy technical infrastructure is secure and is not open to misuse or malicious attack as per the requirements of the Information Security Policy.
- Academies meet the relevant requirements set out in the Department for Education's Meeting digital and technology standards in schools and colleges, including the filtering and

monitoring and cyber security standards, together with Trust requirements and other relevant statutory and non-statutory guidance.

- There is clear, safe, and managed control of user access to networks and devices.
- 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.
- The use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the relevant person in the Academy for investigation and action.
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- Monitoring systems are implemented and regularly updated as agreed in Academy procedures and policies.
- Users must access Trust and Academy systems through individually assigned accounts protected in accordance with the Trust Information Security Policy. Passwords or passphrases must be strong and unique, must not be shared, and must be changed immediately where compromise is known or suspected. Multi-factor authentication must be used where required by Trust standards. Access rights must be reviewed and removed promptly when no longer required.
- Requests to amend filtering policy, such as unblocking uncategorised websites, are carefully reviewed before approving (approval for unblocking sites to be provided by the Principal / Head Teacher).
- The firewall is functional and incorporates appropriate security rules to prevent a compromise to the network.
- That the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the relevant leader for investigation / action / sanction.
- That monitoring software / systems are implemented and updated as per this policy.
- Academy owned devices are appropriately restricted to ensure there is no misuse of cameras or online platforms such as unauthorised websites, social media, personal emails etc.
- Servers, wireless systems and cabling must be securely located and physical access restricted.

Pupils

- Are responsible for using Academy digital technology systems in accordance with the relevant pupil Acceptable Use Agreement and Online Safety Policy. This will include personal devices, if they are allowed.
- Should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should know what to do if they or someone they know feels vulnerable when using online technology.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the Online Safety Policy covers their actions out of school, if related to their membership of the Academy.
- Should avoid plagiarism and uphold copyright regulations, taking care when using Artificial Intelligence (AI) services to protect the intellectual property of themselves and others and checking the accuracy of content accessed through AI services.

Parents / Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

Academies will take every opportunity to help parents and carers understand these issues through:

- Publishing the Online Safety Policy on the website.

- Providing them with a copy of the pupils' Acceptable Use Agreement (including the AUA for parents).
- Publish information about appropriate use of social media relating to posts concerning the Academy.
- Seeking their permissions concerning digital images, cloud services etc. as relevant.
- Parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the academies in:

- Reinforcing the online safety messages provided to pupils in school.
- The safe and responsible use of their children's personal devices in the Academy (where this is allowed.

Community Users

Community users who access SUAT and Academy systems / website / learning platforms as part of the wider Academy provision will be expected to sign the relevant Acceptable Use Agreement before being provided with access to Academy/SUAT systems**.** Academies will ensure that appropriate security measures are implemented before any members of the community and visitors are permitted access to online environments using SUAT / Academy ICT systems (inclusive of Wi-Fi).

The Trust encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other education providers and the community.

Online Safety Group

The Online Safety Group is a consultative team that has wide representation from an Academy's community, with responsibility for issues regarding online safety and monitoring the Online Safety Policy including the impact of initiatives. The implementation of an Online Safety Group will depend on the size or structure of each Academy. Terms of Reference for the OSG are provided within the appendices to this policy. Members could include:

- Designated Safeguarding Lead
- Online Safety Lead
- Senior leaders
- Online safety LAC member
- Technical staff
- Teacher and support staff members
- pupils Parents/carers
- Community representatives

Members of the Online Safety Group may support the following tasks in accordance with their role and responsibilities:

- The production/review/monitoring of the Online Safety Policy/documents.
- The production/review/monitoring of the filtering policy and requests for filtering changes.
- Mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage.
- Reviewing network/filtering/monitoring/incident logs, where this does not conflict with data protection policies (Senior Leaders / DSL / Head Teacher only).
- Encouraging the contribution of pupils to staff awareness, emerging trends and the online safety provision.
- Consulting stakeholders – including staff/parents/carers about the online safety provision.

- Monitoring improvement actions identified through use of the 360-degree safe self-review tool.

Professional Standards

There is an expectation that professional standards will be applied to online safety as in other aspects of school life i.e.:

- There is a consistent emphasis on the central importance of literacy, numeracy, digital competence and digital resilience. pupils will be supported in gaining skills across all areas of the curriculum and every opportunity will be taken to extend pupils' skills and competence.
- There is a willingness to develop and apply new techniques to suit the purposes of intended learning in a structured and considered approach and to learn from the experience, while taking care to avoid risks that may be attached to the adoption of developing technologies e.g. Artificial Intelligence (AI) tools.
- Staff can reflect on their practice, individually and collectively, against agreed standards of effective practice and affirm and celebrate their successes.
- Policies and protocols are in place for the use of online communication technology between the staff and other members of the academy and wider community, using officially sanctioned mechanisms.
- Where Generative AI is used to monitor staff communications, it will be balanced with respect for privacy and transparency about what is being monitored and why.

2. Acceptable Use

The Online Safety Policy and Acceptable Use Agreements define acceptable use within the academies and the Trust. The acceptable use agreements will be communicated/re-enforced through:

- Pupil inductions / admissions.
- Staff induction and handbook.
- Signage.
- Posters/notices around where technology is used.
- Communication with parents/carers.
- Built into education sessions.
- Websites.
- Peer support.
- INSET days.

Activities which are considered acceptable and unacceptable can vary with the size/structure of the Academy and the ages of the pupils. Each Academy must review, discuss and agree on these activities and to complete the following tables as guidance for members of the school community:

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming					**X**

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	• Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering N.B. Refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) A decision will be made as to whether these will be dealt with internally or by the police. Serious or repeat offences should be reported to the police. The National Crime Agency has a remit to prevent pupils becoming involved in cyber-crime and harness their activity in positive ways– further information here					**X**
Users shall not undertake activities that are classed as unacceptable in Academy and MAT policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)				X	X
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the Academy				X	
	Infringing copyright and intellectual property (including through the use of AI services)				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the Academy/Trust or brings the school into disrepute				X	

This section is to be populated by each Academy individually:

Consideration should be given for the following activities when undertaken for non-educational purposes: Academies may wish to add further activities to this list.	**Staff and other adults**				**Pupils**			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/ awareness
Online gaming								
Online shopping/commerce								
File sharing								
Social media (Academy / Trust)								
Social media (personal)								
Messaging/chat								

Entertainment streaming e.g. Netflix, Disney+								
Use of video broadcasting, e.g. YouTube, Twitch, TikTok								
Mobile phones may be brought to school								
Use of pupil mobile phones during the school day – not permitted except where an individually agreed exception or reasonable adjustment applies								
Use of pupil mobile phones during breaktimes/lunchtimes – not permitted except where an individually agreed exception or reasonable adjustment applies								
Taking photos on mobile phones/cameras								
Use of other personal devices, e.g. tablets, gaming devices								
Use of personal e-mail in school, or on school network/wi-fi								
Use of AI services that have not been approved by the academy / Trust								
Use of Academy e-mail for personal e-mails								

When using communication technologies, Academies consider the following as good practice:

- When communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the Academy and only use Academy accounts.
- Any digital communication between staff and pupils or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- Staff are expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community.
- Users should immediately report to the nominated person regarding 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.
- Relevant policies and permissions should be followed when posting information online e.g., Academy website and social media. Only Academy email addresses should be used to identify members of staff and pupils within their communications.

3. Reporting and Responding

Each Academy will take all reasonable precautions to ensure online safety for all users but recognises that incidents may occur inside and outside of school (with impact on the Academy) which will need intervention (please also see section 13). Each Academy will ensure:

- There are clear reporting routes which are understood and followed by all members of the Academy community, which are consistent with Academy safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies. Reporting systems, which can be used by all members of the Academy community, may be used, for example, SWGfL Whisper.
- All members of the Academy community will be made aware of the need to report online safety issues/incidents.
- Reports will be dealt with as soon as is practically possible once they are received and will be prioritised according to their severity.
- The Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks, and keep up to date with the latest safeguarding and online safety practices through ongoing CPD.
- If there is any suspicion that the incident involves any illegal activity or the potential for serious harm, the incident must be escalated through the agreed Academy safeguarding procedures. Harms and illegal activity can include:
    - Non-consensual images
    - Images of pupils that have been copied, digitally altered, manipulated or generated using artificial intelligence or other digital technologies
    - Threats to publish or distribute altered, fabricated or abusive images of pupils
    - Coercion or extortion connected with genuine, altered or fabricated images of pupils
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/abuse
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation
    - Grooming
    - Extreme Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking offences under the Computer Misuse Act 1990
    - Copyright theft or piracy

Responding to image misuse

Where an Academy becomes aware that an image of a pupil published by the Academy or Trust may have been copied, altered, manipulated or used to create harmful or potentially illegal content, the matter must be reported immediately to the Designated Safeguarding Lead. Staff must not conduct their own online investigation, download or copy suspected illegal content, or share or circulate the material. The Designated Safeguarding Lead will follow the Academy's safeguarding procedures, ensure that available evidence is preserved appropriately and seek advice from the police, local safeguarding partners, the Internet Watch Foundation or another appropriate specialist service where required.

- Any concern about staff misuse will be reported to the Headteacher / Principal, unless the concern involves the Headteacher / Principal, in which case the concern or complaint

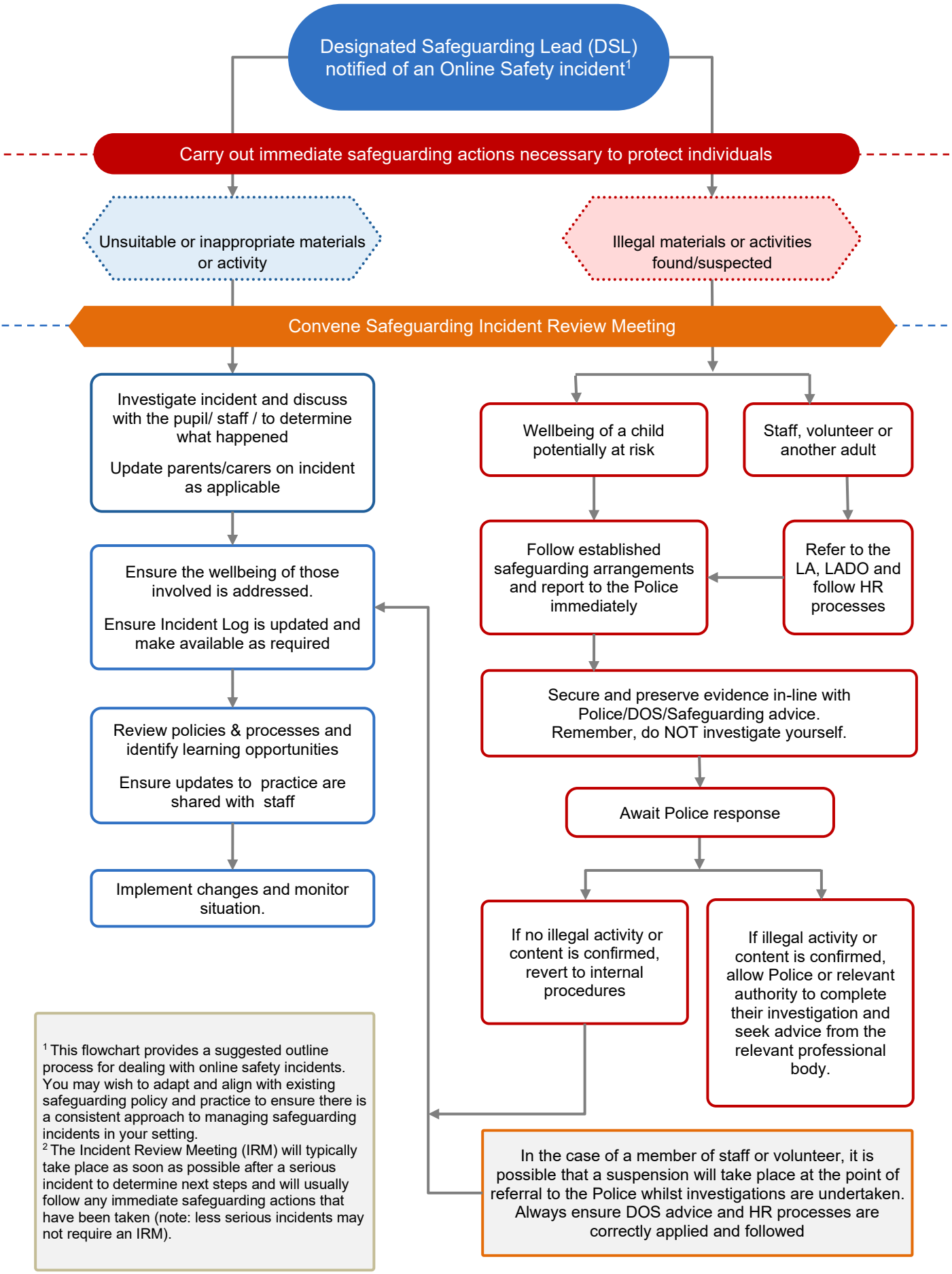
is referred to the Chair of the LAC and the CEO of the Trust, and Local Authority as relevant to the case.

- Where AI is used to support monitoring and incident reporting, human oversight is maintained to interpret nuances and context that AI might miss.
- Where there is no suspected illegal activity, devices may be checked using the following procedures:
    - At least two senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - Conduct the procedure using a designated device that will not be used by pupils and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
    - Ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
    - Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form.
    - 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 / MAT (as relevant)
        - Police involvement and/or action

- It is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively.
- There are support strategies in place e.g. peer support for those reporting or affected by an online safety incident.
- Incidents should be logged and logs should contain sufficient detail regarding the incident.
- Relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant and appropriate).
- Learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    - The Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
    - Staff, through regular briefings
    - Pupils, through assemblies/lessons
    - Parents/carers, through newsletters, school social media, website
    - LAC members and Trustees, through regular safeguarding updates
    - The Trust
    - Local authority/external agencies, as relevant

The below flowchart is available to staff to support the decision-making process for dealing with online safety incidents:

Please turn over.



[1] This flowchart provides a suggested outline process for dealing with online safety incidents. You may wish to adapt and align with existing safeguarding policy and practice to ensure there is a consistent approach to managing safeguarding incidents in your setting.
[2] The Incident Review Meeting (IRM) will typically take place as soon as possible after a serious incident to determine next steps and will usually follow any immediate safeguarding actions that have been taken (note: less serious incidents may not require an IRM).

4. Academy Actions

It is more likely that academies 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 and in a proportionate manner, and that members of the Academy 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, which will be updated and adjusted in accordance with behaviour and HR policies and procedures.

Responding to pupil Actions

Incidents	Refer to class teacher/tutor	Refer to Head of Department / Principal Teacher / Deputy Head	Refer to Headteacher	Refer to Police/Social Work	Refer to local authority technical support for advice/action	Inform parents/carers	Remove device/ network/internet access rights	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).									

Attempting to access or accessing the school network, using another user's account (staff or pupil) or allowing others to access school network by sharing username and passwords									
Corrupting or destroying the data of other users.									
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature									
Unauthorised downloading or uploading of files or use of file sharing.									
Using proxy sites or other means to subvert the school's filtering system.									
Accidentally accessing offensive or pornographic material and failing to report the incident.									
Deliberately accessing or trying to access offensive or pornographic material.									
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.									
Unauthorised use of digital devices (including taking images)									
Unauthorised use of online services									
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.									
Continued infringements of the above, following previous warnings or sanctions.									

Responding to Staff Actions

Incidents	Refer to line manager	Refer to Headteacher/ Principal	Refer to local authority/MAT/HR	Refer to Police	Refer to Technical Staff for action e.g. filtering, improve security.	Issue a 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		In accordance with HR policies and procedures.		
Deliberate actions to breach data protection or network / cyber security rules.		X	X		X			
Deliberately accessing or trying to access offensive or pornographic material		X	X		X			
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X		X			
Using proxy sites or other means to subvert the school's filtering system.	X	X			X			
Unauthorised downloading or uploading of files or file sharing	X	X			X			
Breaching copyright or licensing regulations (including the use of AI systems)	X	X						
Allowing others to access the academy network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	X	X						
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X	X						
Using personal e-mail/social networking/messaging to carry out digital communications with pupils and parents/carers	X	X						
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail	X	X						
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner	X	X	X					
Actions which could compromise the staff member's professional standing	X	X						

Actions which could bring the school into disrepute or breach the integrity or the ethos of the Academy	X	X						
Failing to report incidents whether caused by deliberate or accidental actions	X	X						
Continued infringements of the above, following previous warnings or sanctions.	X	X	X	X				

5. Online Safety Education and Training

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 each Academy's Online Safety and Safeguarding provision. Pupils need the help and support of each Academy to recognise and avoid Online Safety risks and build their resilience.

Online safety should be a focus 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 by:

- A planned online safety curriculum for all year groups matched against a nationally agreed framework e.g. Education for a Connected Work Framework by UKCIS/DCMS and the SWGfL, Project Evolve, which is regularly taught in a variety of contexts.
- Lessons are matched to need, are age-related and build on prior learning.
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes.
- Pupil needs and progress are addressed through effective planning and assessment.
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g., PSHE; phase-appropriate Relationships Education/RSE terminology; Literacy etc.
- It incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.
- The programme will be accessible to pupils at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- Pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information (including where the information is gained from Artificial Intelligence services).
- Pupils should be taught to acknowledge the source of information used and to respect copyright / intellectual property when using material accessed on the internet and particularly through the use of Artificial Intelligence services.
- Vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- 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. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990. Lessons and further resources are available on the CyberChoices site.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices.

- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in supervising the pupils and monitoring the content of the websites the young people visit.
- If pupils are allowed to freely search the internet, staff should be vigilant in supervising the pupils and monitoring the content of the websites / tools (including AI systems) that the pupils visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of 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.
- The online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

Academies acknowledge, learn from, and use the skills and knowledge of pupils in the use of digital technologies. Academies recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- Mechanisms to canvass pupil feedback and opinion.
- Appointment of digital leaders/anti-bullying ambassadors/peer mentors (or similar groups).
- The online safety group has pupil representation.
- Pupils contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger pupils, online safety campaigns.
- Pupils designing/updating acceptable use agreements.
- Contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.

Staff / Volunteers

All 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 and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- The training will be an integral part of each Academy's annual safeguarding, data protection and cyber-security training for all staff.
- Data protection, cyber security and online safety training will be undertaken at the point of induction and carried out annually thereafter.
- A data protection and safeguarding induction.
- The training will be an integral part of each Academy's annual safeguarding programme.
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the Online Safety Policy and Acceptable Use Agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.
- The online safety lead and designated safeguarding lead (or other nominated person) will receive regular updates through attendance at external training events, (e.g. UKSIC / SWGfL / MAT / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- Staff involved in taking, selecting, preparing, approving or publishing images and videos of pupils will receive appropriate guidance on the safeguarding risks associated with making images publicly available online. This will include checking current permissions and safeguarding restrictions, reducing unnecessary pupil identification, avoiding names or other

identifying information in captions, removing unnecessary metadata, using an appropriately reduced image resolution where practicable, and recognising and reporting suspected AI-enabled image misuse.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/inset days.
- The designated safeguarding lead/online safety lead (or other nominated person) will provide advice/guidance/training to individuals as required.

LAC Members

LAC members should take part in online safety training/awareness sessions, which will be particularly important for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:
- Attendance at training provided by the local authority/MAT or other relevant organisation (e.g., SWGfL).
- Participation in Academy training / information sessions for staff or parents (this may include attendance at assemblies/lessons).
- Attending cyber security training, which is an annual requirement under the Risk Protection Arrangement's cyber cover.

A higher level of training will be made available to (at least) the Online Safety LAC Member. This will include:
- Cyber-security training (at least at a basic level).
- Training to allow the LAC member to understand the Academy's filtering and monitoring provision, in order that they can participate in the required checks and reviews.

Families
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.

Academies will seek to provide information and awareness to parents and carers through:
- Regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes.
- Regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc.
- The pupils – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by pupils leading sessions at parent/carer evenings.
- Letters, newsletters, websites, learning platform.
- High profile events / campaigns e.g. Safer internet day.
- Reference to the relevant web sites/publications, e.g. SWGfLI; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers (see appendix for further links/resources).
- Sharing good practice with other academies locally, within the Trust and across the Local Authority.

Adults and Agencies
Academies may wish to provide opportunities for local community groups and members of the wider community to gain from their online safety knowledge and experience. This may be offered through the following:
- Online safety messages targeted towards families and relatives.
- Providing family learning courses in use of digital technologies and online safety.
- Providing online safety information via the website and social media for the wider community.

- Supporting community groups, e.g. early years settings, childminders, youth/sports/voluntary groups to enhance their online safety provision (consider supporting these groups with an online safety review using 360 Groups or 360 Early Years).

6. Technology and AI

Each Academy is responsible for ensuring that their infrastructure/network is as safe and secure as is reasonably possible (see Information Security Policy), and that procedures approved within this policy are implemented. All staff need to be made aware of policies and procedures in place on a regular basis and academies should explain that everyone is responsible for online safety and data protection.

Academies who have an external technology provider must ensure that the provider carries out all online safety, cyber security, filtering and monitoring measures that would otherwise be the responsibility of the Academy, in accordance with the Department for Education's Meeting digital and technology standards in schools and colleges, including the filtering and monitoring and cyber security standards, and this Online Safety Policy. Policies which support information security and data protection matters include the Data Protection Policy, Information Security Policy and Acceptable Use Policy.

As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in, its role in education is also evolving. There are currently 3 key dimensions of AI use in schools: pupil support, teacher support and school operations; ensuring all use is safe, ethical and responsible is essential.

We realise that there are risks involved in the use of Gen AI services, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address the risks. We will educate staff and pupils about safe and ethical use of AI, preparing them for a future in which these technologies are likely to play an increasing role. The safeguarding of staff and pupils will, as always, be at the forefront of our policy and practice.

Academies recognise that generative AI and other digital technologies may be used by third parties to copy, alter, manipulate or repurpose genuine images of children without permission. This includes the risk that publicly available images may be used to create fabricated, abusive or otherwise harmful content, or in connection with coercion, extortion or other criminal activity. This risk will be considered when images of pupils are selected and prepared for online publication, in accordance with the Digital and Video Images and Online Publishing sections of this policy.

Academies acknowledge the potential benefits of the use of AI in an educational context - including enhancing learning and teaching, improving outcomes, improving administrative processes, reducing workload and preparing staff and pupils for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work. Academies will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe in Education and UK GDPR

Academies will provide relevant training for staff and governors in the advantages, use of and potential risks of AI, and will support staff in identifying training and development needs to enable relevant opportunities.

Academies will seek to embed learning about AI as appropriate in their curriculum offer, including supporting pupils to understand how gen AI works, its potential benefits, risks, and ethical and social impacts. Academies recognise the importance of equipping pupils with the knowledge, skills and strategies to engage responsibly with AI tools.

Staff will be supported to use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information, and avoid inputting personal information into AI tools to minimise the risks.

Staff will always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.

Only those AI technologies approved by the academy in conjunction with the DPO, may be used. Staff should always use academy-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.

When considering the procurement, approval or deployment of generative artificial intelligence products or services, the Trust and its Academies will have regard to the Department for Education's Generative AI: product safety standards. Appropriate due diligence will be undertaken before a product is approved for use and will consider, as relevant, safeguarding and content moderation; age and SEND appropriateness; filtering and monitoring; security; privacy and data protection; intellectual property; transparency; human oversight; equality and accessibility; governance and accountability; and the provider's arrangements for testing, reporting concerns and managing emerging risks.

Generative AI products must not be introduced or used with pupils solely because they are freely or commercially available. Products used within the Trust must be appropriately assessed and approved in accordance with Trust procedures, taking account of the intended users, purpose of use and associated safeguarding, data protection, cyber security and educational risks.

Staff will protect sensitive information and must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognise and safeguard sensitive, personal data and business critical data.

Academies will ensure that when AI is used, they will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the pupils, being used to train generative AI models without appropriate consent.

AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately in accordance with the Data Breach Management Plan. Quick reporting helps mitigate risks and facilitates a prompt response.

Academies will audit all AI systems in use and assess their potential impact on staff, pupils and the school's systems and procedures, creating an AI inventory listing all tools in use, their purpose and potential risks.

Academies are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, they will follow due care and diligence to prioritise fairness and safety.

Academies will support parents and carers in their understanding of the use of AI in the school. AI tools may be used to assist teachers in the assessment of pupils' work, identification of areas for improvement and the provision of feedback. Teachers may also support pupils to gain feedback on their own work using AI.

Staff should ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance. Clearly marking AI-generated content helps build trust and ensures that others are informed when AI has been used in communications or documents, maintaining transparency.

Human oversight will remain to be a priority to ensure that AI assists, not replaces, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate any AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing; this is especially important for external communication to avoid spreading misinformation.

Recourse for improper use and disciplinary procedures. Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Disciplinary Policy.

7. Filtering and Monitoring

Each Academy's filtering and monitoring provision should be agreed by the Head Teacher / Principal and Senior Leaders, taking advice from their IT Service Provider. This must be regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours locally and nationally. The provision must have regard to the Department for Education's current Meeting digital and technology standards in schools and colleges, including the filtering and monitoring standard, and should be reviewed against those requirements whenever the DfE standards are updated.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility.

Each Academy must identify a responsible SLT member and responsible LAC member for filtering and monitoring. At least once each academic year, and following relevant change or risk, the responsible SLT member will lead a documented effectiveness review with the DSL and IT support. Checks must cover all Academy-managed internet-connected devices and services, all relevant locations, and the correct filtering profiles for pupils, staff and guests, and must consider real-time, dynamic, personalised and AI-generated content. Actions, owners and completion dates must be recorded and reported through the Trust assurance process.

Internet access should be filtered for all users. Differentiated internet access should be available for staff and customised filtering changes are managed by the Academy. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and other illegal content lists. Filter content lists must be regularly updated and internet use must be logged and frequently monitored. The monitoring process in each Academy must alert designated staff to breaches of the filtering policy, which are then acted upon in accordance with the procedures detailed within this policy. Where personal mobile devices are allowed internet access through the Academy network, filtering will be applied that is consistent with Academy practice.

Effective filtering and monitoring includes that:

- There is a filtering and monitoring system in place that safeguards staff and pupils by blocking harmful, illegal and inappropriate content.
- There is a monitoring system that enables the prompt investigation of a potential safeguarding incident and outcomes are logged.
- Roles and responsibilities for the management of filtering and monitoring systems have been defined and allocated.
- The filtering and monitoring provision is reviewed at least annually and checked regularly.

- There is a defined and agreed process for making changes to the filtering or monitoring system that involves a senior leader in the agreement of the change.
- Mobile devices that access the Academy's internet connection (whether Academy or personal devices) will be subject to the same filtering standards as other devices on the Academy systems.
- Academies can provide enhanced/differentiated user-level filtering through the use of the filtering system.

Checks on the filtering and monitoring system must carried out by the designated member of staff, in particular, when a safeguarding risk is identified, there is a change in working practice, for example, new technology is introduced. This includes:

- Discrimination: Promotes the unjust or prejudicial treatment of people on the grounds of the protected characteristics listed in the Equality Act 2010
- Drugs / Substance abuse: displays or promotes the illegal use of drugs or substances
- Extremism: promotes terrorism and terrorist ideologies, violence or intolerance
- Malware / Hacking: promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content
- Pornography: displays sexual acts or explicit images
- Piracy and copyright theft: includes illegal provision of copyrighted material
- Self Harm: promotes or displays deliberate self harm (including suicide and eating disorders)
- Violence: Displays or promotes the use of physical force intended to hurt or kill
- Gambling
- Any malicious, harmful or inappropriate content

Any member of staff employed by SUAT who comes across an online safety issue does not investigate any further but immediately reports it to the Senior Leadership Team, Designated Safeguarding Lead or Principal/Head Teacher and takes the equipment out of use.

Filtering

The DfE Technical Standards for Schools and Colleges states:

"Schools and colleges have a statutory responsibility to keep children and young people safe online as well as offline. Governing bodies and proprietors should make sure their school or college has appropriate filtering and monitoring systems in place, as detailed in the statutory guidance, Keeping children safe in education.

Filtering is preventative. It refers to solutions that protect users from accessing illegal, inappropriate and potentially harmful content online. It does this by identifying and blocking specific web links and web content in the form of text, images, audio and video.

These standards help school and college leaders, designated safeguarding leads and IT support understand how to work together to make sure they can effectively safeguard their students and staff."

A member of the SLT shall be responsible for ensuring these standards are met. Roles and responsibilities of staff and third parties, for example, in-house or third-party IT support in supporting the standards to be met should be clearly defined.

The filtering of internet content provides an important means of preventing users from accessing material that is illegal, unsafe, or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, as online content changes dynamically and new technologies are constantly being developed. It is important, therefore, to

understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that each Academy has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in each setting. Academies are recommended to use the UK Safer Internet Centre Definitions to help them determine if their filtering system is appropriate, and can test their filtering for protection against illegal materials at: SWGfL Test Filtering.

The filtering system should be operational, up to date and applied to all:

- Users, including guest accounts.
- Academy / Trust owned devices.
- Devices using the school broadband connection.

The filtering system should:

- Filter all internet feeds, including any backup connections.
- Be age and ability appropriate for the users and be suitable for educational settings.
- Handle multilingual web content, images, common misspellings and abbreviations.
- Identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them.
- Provide alerts when any web content has been blocked.

Mobile and app content is often presented in a different way to web browser content. If users access content in this way, academies should get confirmation from their provider as to whether they can provide filtering on mobile or app technologies. A technical monitoring system should be applied to devices using mobile or app content to reduce the risk of harm.

Academies should ensure that their filtering system meets the following principles:

- Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and ability to understand the complexities of internet content.
- Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, for example VPN, proxy services and DNS over HTTPS.
- Control - has the ability and ease of use that allows the Academy to control the filter themselves to permit or deny access to specific content.
- Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking. Each Academy should have access to their filtering policy.
- Group/Multi-site Management – the ability for deployment of central policy and central oversight or dashboard.
- Identification - the filtering system should have the ability to identify users.
- Mobile and App content – mobile and app content is often delivered in entirely different mechanisms from that delivered through a traditional web browser. The filter system must also block inappropriate content via mobile and app technologies (beyond typical web browser delivered content). Where mobile devices are taken off the school infrastructure or fall outside of this filtering, then other appropriate device level filtering will be in place to ensure safeguarding (such as Mobile Device Management tools).
- Multiple language support – the ability for the system to manage relevant languages.
- Reporting mechanism – the ability to report inappropriate content for access or blocking.
- Reports – the system offers clear historical information on the websites visited by Academy users.

All use of Academy internet access is logged and the logs are regularly monitored by the DSL, senior leadership team, and IT Support provider where appropriate. Whenever any inappropriate use is detected, it will be followed up by the DSL or member of the Senior Leadership Team depending on the severity of the incident.

Effective filtering includes:

- Each Academy manages access to content across its systems for all users and on all devices using Academy internet provision. The filtering provided is required to meet the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate Filtering.
- Illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.
- There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective. These are acted upon in a timely manner, within clearly established procedures.
- There is a clear process in place to deal with, and log, requests/approvals for filtering changes, in each Academy.
- Filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- There are regular checks of the effectiveness of the filtering systems. Checks are undertaken across a range of devices at least termly and the results recorded and analysed to inform and improve provision. Designated staff are involved in the process and aware of the findings. (Academies may wish to use e.g. using SWGfL Testfiltering.com to carry out these checks).
- Devices that are provided by an academy have school-based filtering applied irrespective of their location.
- Each Academy has (where possible) provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/ pupils, etc.).
- Younger pupils will use child friendly/age-appropriate search engines e.g. SWGfL Swiggle
- Each Academy has a procedure for the use of mobile phones on the premises, and where personal mobile devices have internet access through the Academy network, content is managed in ways that are consistent with Online Safety practices and this policy.
- Access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with the Online Safety Policy and Academy practices.
- If necessary, academies will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

Monitoring

The DfE Technical Standards for Schools and Colleges states:
“Monitoring is reactive. It refers to solutions that monitor what users are doing on devices and, in some cases, records this activity. Monitoring can be manual, for example, teachers viewing screens as they walk around a classroom. Technical monitoring solutions rely on software applied to a device that views a user’s activity. Reports or alerts are generated based on illegal, inappropriate, or potentially harmful activities, including bullying. Monitoring solutions do not block users from seeing or doing anything.”

The UK Safer Internet Centre Appropriate Monitoring guidance can be utilised by academies.

Monitoring user activity on Academy devices is an important part of providing a safe environment for children and staff. Unlike filtering, it does not stop users from accessing material through internet searches or software. Monitoring allows settings to review user activity on Academy devices. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing settings to take prompt action and record the outcome.

Each Academy will have monitoring software in place for every device (including laptops, mobile devices and desktops) which detects potentially inappropriate content and conduct as soon as it appears on the screen, is typed in by any users or received by the user. A capture is taken of every incident detailing the time and date of capture, machine name, username and reason for capture.

Academies will recognise that some captures will be false positives however, where it has been established that the capture is a violation, this will be investigated and managed in accordance with the AUP, Behaviour Policy and other relevant SUAT / Academy policies, depending on the nature of the capture. The Senior Leadership Team and DSL will maintain the Change Control Log and record any breaches, suspected or actual, of the filtering and security systems. Potential personal data breaches will be reported to the DPO for investigation immediately.

Each Academy should follow the UK Safer Internet Centre Appropriate Monitoring guidance and protect users and Academy systems through the use of the appropriate blend of strategies informed by the their risk assessment. The monitoring strategy should be informed by the filtering and monitoring review. A variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- Physically monitoring by staff watching screens of users.
- Live supervision by staff on a console with device management software.
- Network monitoring using log files of internet traffic and web access.
- Individual device monitoring through software or third-party services.

Each Academy is required to have monitoring systems in place to protect the Academy, systems and users:

- Each Academy monitors all network use across all its devices and services.
- Monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

The monitoring provision is reviewed at least once every academic year and updated in response to changes in technology and patterns of online safety incidents and behaviours. The review should be conducted by members of the senior leadership team, the designated safeguarding lead, and technical staff and may involve the relevant link LAC member; the results of the review will be recorded and reported as relevant. Where AI –supported monitoring is used, the purpose and scope of this is clearly communicated.

Filtering and Monitoring Responsibilities

Academy-specific filtering and monitoring responsibilities are recorded in Appendix 7 – Academy Online Safety Arrangements.

Changes to Filtering and Monitoring Systems

There should be a clear process for requests to change the filtering and monitoring systems and who makes the decision to alter the filtering system in each Academy. Changes to filtering and monitoring systems are managed by (to be adapted according to the Academy's arrangements):

How, and to whom, users may request changes to the filtering and monitoring systems:	
The grounds on which changes may be permitted or denied:	
How a second responsible person / senior leader will agree to the change before it is made and how this will be recorded:	
Audit / reporting systems:	

Reviewing the filtering and monitoring provision

A review of filtering and monitoring will be carried out to identify the current provision, any gaps, and the specific needs of pupils and staff. The review will take account of:

- The risk profile of pupils, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL).
- What the filtering system currently blocks or allows and why.
- Any outside safeguarding influences, such as county lines.
- Any relevant safeguarding reports.
- The digital resilience of pupils.
- Teaching requirements, for example, the RHSE and PSHE curriculum.
- The specific use of chosen technologies, including Bring Your Own Device (BYOD).
- What related safeguarding or technology policies are in place.
- What checks are currently taking place and how resulting actions are handled.

To make the filtering and monitoring provision effective, the review will inform:

- Related safeguarding or technology policies and procedures.
- Roles and responsibilities.
- Training of staff.
- Curriculum and learning opportunities.
- Procurement decisions.
- How often and what is checked.
- Monitoring strategies.
- MAT and Academy policy reviews.

The review will be carried out as a minimum annually, or when:

- A safeguarding risk is identified.
- There is a change in working practice.
- New technology is introduced.

Checking the filtering and monitoring systems

Checks to filtering and monitoring systems are completed and recorded as part of the filtering and monitoring review process. How often the checks take place will be based on the context, the risks highlighted in the filtering and monitoring review, and any other risk assessments. Checks will be undertaken from both a safeguarding and IT perspective.

When filtering and monitoring systems are checked this should include further checks to verify that the system setup has not changed or been deactivated. Checks are performed on a range of:

- School owned devices and services, including those used off site
- Geographical areas across the site
- User groups, for example, teachers, pupils and guests

Logs of checks are kept so they can be reviewed. These record:

- When the checks took place
- Who did the check
- What was tested or checked
- Resulting actions

The SWGfL Filtering Standards checklist may be helpful.

Audit/Monitoring/Reporting/Review:

SLT/DSL/OSL will ensure that full records are kept of:

- Training provided.
- User IDs and requests for password changes.
- User logons.
- Security incidents related to this policy.
- Annual online safety reviews including filtering and monitoring.
- Reviews of pupil images and videos published on Academy websites, official social media accounts and other public-facing online platforms, including any actions identified or content removed.
- Changes to the filtering system.
- Checks on the filtering and monitoring systems.

8. Technical Security

Academy technical systems will be managed in ways that ensure that academies meet the recommended technical requirements within DfE and Trust policy documents and guidance.

In each setting the following should be in place:

- Responsibility for technical security resides with SLT who may delegate activities to identified roles.
- Access rights to academy systems and devices is reviewed annually. All users (staff and pupils) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security
- All users have clearly defined access rights to Academy technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT service provider and will be reviewed, at least annually, by the SLT/Online Safety Group.
- Password policy and procedures are implemented.

- The security of an individual's username and password and must not allow other users to access the systems using their log on details. All users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- All Academy networks and systems will be protected by secure passwords. Passwords must not be shared with anyone.
- There is a risk-based approach to the allocation of pupil usernames and passwords.
- There will be regular reviews and audits of the safety and security of Academy technical systems by leaders.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of each Academy's systems and data. These are tested regularly. Academy infrastructure and individual workstations are protected by up-to-date endpoint software.
- There are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud.
- A designated member of staff is responsible for ensuring that all software purchased by and used by the Academy is adequately licenced and that the latest software updates (patches) are applied.
- Use of Academy devices out of school and by family members is regulated by an acceptable use statement that a user (or parent on their behalf, depending on the age and maturity of the pupil) consents to when the device is allocated to them.
- Personal use of any device on the Academy network is regulated by acceptable use agreements that a user consents to when using the network.
- Staff members are not permitted to install software on a Academy-owned devices without the consent of the SLT and advice of the IT service provider.
- Systems are in place to control and protect personal data and data is encrypted at rest and in transit.
- Mobile device security and management procedures are in place (where mobile devices are allowed access to Academy systems).
- Guest users are provided with appropriate access to Academy systems based on an identified risk profile.
- Systems are in place that prevent the unauthorised sharing of personal / sensitive data unless safely encrypted or otherwise secured.
- Care will be taken when using Artificial Intelligence services to avoid the input of sensitive information, such as personal data, internal documents or strategic plans, into third-party AI systems unless explicitly vetted for that purpose. Staff must always recognise and safeguard sensitive data.
- Dual-factor authentication is used for sensitive data or access outside of a trusted network
- Where AI services are used for technical security, their effectiveness is regularly reviewed, updated and monitored for vulnerabilities.
- Where AI services are used, the school will work with suppliers to understand how these services are trained and will regularly review flagged incidents to ensure equality for all users e.g. avoiding bias.

9. Mobile Technologies

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

Mobile phones in schools

In accordance with the Department for Education's statutory guidance *Mobile phones in schools*, Academies will operate as mobile phone-free environments by default. Pupils will not have access to or use mobile phones or other personal smart technology with similar functionality throughout the school day, including during lessons, transitions between lessons, breaktimes and lunchtimes. Each Academy will set out its arrangements for achieving this within its Behaviour Policy and/or associated mobile phone procedures. These arrangements will be communicated clearly to pupils, parents/carers and staff and will include the consequences and sanctions that may apply where the policy is not followed.

Academies will make appropriate exceptions, adaptations and reasonable adjustments where required by law or where justified by an individual pupil's circumstances. This may include, for example, pupils who require access to a mobile phone to manage a medical condition or disability, where this constitutes a reasonable adjustment, or where there are other exceptional circumstances which have been considered and agreed by the Academy.

Where an exception is agreed, the Academy will determine the specific purpose, times and locations in which the device may be used. An agreed exception does not provide unrestricted access to a mobile phone during the school day.

Staff are expected to model the Academy's expectations and should not use personal mobile phones for personal reasons in front of pupils during the school day, except where there is an appropriate operational, safeguarding or other authorised reason.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The use of mobile technologies should be consistent with and inter-related to other relevant Academy polices including but not limited to the Safeguarding Policy, Behaviour Policy, Anti-Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of Academy online safety education programme.

The possible issues and risks of using mobile technologies include:

- Security risks in allowing connections to Academy networks.
- Filtering of personal devices.
- Breakages and insurance.
- Access to devices for all pupils/students.
- Avoiding potential classroom distraction.
- Network connection speeds.
- Types of devices.
- Charging facilities and electrical compliance.
- Total cost of ownership.
- Incompatibility with Academy systems.
- Data loss.
- Academy systems may enforce admin rights over devices and amend device settings.

For Academy owned/provided devices, each setting should define for users:

- 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.
- How to access technical support.
- Filtering and monitoring of devices.
- Access to cloud services.

- Data protection requirements.
- Taking/storage/use of images.
- Exit processes – what happens to devices/software/apps/stored data if user leaves the Academy.
- Liability for damage.
- Staff training.

The following information should be provided surrounding the use of personal devices:

- Which users are allowed to use personal mobile devices in school (staff/pupils/students/visitors).
- Restrictions on where, when and how they may be used in school.
- Storage.
- Staff are not permitted to use personal devices for Academy business. Personal data must not be accessed on or downloaded to personal devices.
- 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 requirements.
- The right to take, examine and search users' devices in the case of misuse.
- Taking/storage/use of images.
- Liability for loss/damage or malfunction following access to the network.
- Identification/labelling of personal devices.
- How visitors will be informed about Academy requirements.
- How education about the safe and responsible use of mobile devices is included in Academy online safety education programmes.

When personal data is stored on any mobile device or removable media, security measures detailed in the Information Security Policy must be followed, including:

- Data must be encrypted and password protected.
- The device must be password protected and subject to secure encryption.
- The device must be protected by up to date virus and malware checking software.
- Data must be securely deleted from the device, in line with the Retention and Information Security policies once it has been transferred or its use is complete.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Can recognise a possible breach, understand the need for urgency and know who to report it to within the Academy, who will escalate potential breaches to the DPO upon immediately becoming aware of the issue.
- Can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to report it to in the Academy.
- Where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected and secured in accordance with the Information Security Policy.
- Will not transfer any Academy or personal data to personal devices.
- Access personal data sources and records only on secure devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Do not take Academy devices off site without permission of the Head Teacher / Principal.

The Academy allows: (each Academy to complete)

	Academy devices	**Personal devices**

	Academy owned for individual use	Academy owned for multiple users	Authorised device	Student owned	Staff owned	Visitor owned
Allowed in school	**Yes**	**Yes**	**Yes**	Yes/No	Yes/No	Yes/No
Full network access	Yes	Yes	Yes/No	Yes/No	Yes/No	Yes/No
Internet only				Yes/No	Yes/No	Yes/No
No network access				Yes/No	Yes/No	Yes/No

Academy owned/provided devices:

- All Academy owned devices should be managed though the use of Mobile Device Management software.
- There is an asset log that clearly states whom a device has been allocated to, in each Academy. There is clear guidance on where, when and how use is allowed.
- Any designated mobile-free zone is clearly signposted.
- Personal use (e.g. online banking, shopping, images etc.) is clearly defined and expectations are well-communicated.
- The use of devices on trips/events away from school is clearly defined and expectation are well-communicated.
- Liability for damage aligns with current policy for the replacement of equipment.
- Education is in place to support responsible use.
- The expectations for taking/storing/using images/video aligns with the Academy's acceptable use policy and use of images/video policy. The non-consensual taking/using of images and recordings of others is not permitted.

Personal devices:

- There is clear guidance covering the use of personal mobile devices on school premises for all users.
- Where devices are used to support learning, staff have been trained in their planning, use and implementation, ensuring that all pupils can access a required resource.
- Where personal devices are brought to school, but their use is not permitted, appropriate, safe and secure storage should be made available.
- Use of personal devices for Academy business is defined in the acceptable use agreements and information security policy. Personal devices commissioned onto the Academy network are segregated effectively from Academy owned systems.
- The expectations for taking/storing/using images/video aligns with the Academy's acceptable use policy and use of images/video policy. The non-consensual taking/using of images and recordings of others is not permitted.
- Liability for loss/damage or malfunction of personal devices is clearly defined.
- There is clear advice and guidance at the point of entry for visitors to acknowledge school requirements.
- Education about the safe and responsible use of mobile devices is included in the school online safety education programmes.

Technical solutions for the safe use of mobile devices include:

- Devices being managed though the use of Mobile Device Management software.
- Appropriate access control being applied to all mobile devices according to the requirements of the user (e.g. Internet only access, network access allowed, shared folder network access).

- Addressing broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices.
- Applying filtering to the internet connection and attempts to bypass this are not permitted.
- Implementing exit processes for devices no longer used in an Academy or Trust by an authorised user.
- Monitoring devices on the Academy network.
- Software/apps originally installed by the Academy must remain on the Academy owned device in usable condition and be always easily accessible. From time to time the Academy may add software applications for use in a particular lesson. Checking devices to ensure that users have not removed required apps.
- Ensuring that devices contain the necessary apps for Academy work. Apps added by the Academy remain the property of the Academy and will not be accessible to pupils on authorised devices once they leave the Academy's roll. Any apps bought by the user on their own account will remain theirs.
- Where an Academy device has been provided to support learning. It is expected that pupils will bring devices to the Academy as required.
- Changing settings that would stop the device working as it was originally set up and intended to work is not permitted.

When personal devices are permitted in school:

- Personal devices commissioned onto the network are segregated effectively from school-owned systems. Personal devices are brought into the Academy / Trust entirely at the risk of the owner and the decision to bring the device into the Academy / Trust lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school.
- The Academy / Trust accepts no responsibility or liability in respect of lost, stolen or damaged devices whilst on Academy or Trust premises, or on activities organised or undertaken by the Academy (SUAT recommends insurance is purchased to cover that device whilst out of the home).
- The Academy / Trust accepts no responsibility for any malfunction of a device due to changes made to the device while on the Academy network or whilst resolving any connectivity issues.
- The Academy / SUAT recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around. Pass-codes or PINs should be set on personal devices to aid security.
- The Academy is not responsible for the day to day maintenance or upkeep of the users personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues.

Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements, in addition:

- Devices are not permitted in tests or exams.
- There is clear advice and guidance at the point of entry for visitors to understand requirements.
- Users are responsible for keeping their device up to date through software, security and app updates.
- Users are responsible for charging their own devices and for protecting and looking after their devices whilst on site.
- Confiscation and searching - the Academy has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
- Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.
- The expectations for taking/storing/using images/video aligns with the acceptable use policy and use of images/video policy. The non-consensual taking/using of images and recordings of others is not permitted.
- Devices may be used in lessons in accordance with teacher direction.

- Staff owned devices must not be used for personal purposes during teaching sessions.
- Printing from personal devices will not be possible.

10. Social Media

The use of social media should be conducted in accordance with the Social Media Policy, Acceptable Use Agreements and codes of conduct.

The following measures should be undertaken in each Academy to ensure reasonable steps are in place to minimise risk of harm to pupils through:

- Ensuring that personal information is not published.
- Education/training being provided including acceptable use, age restrictions, social media risks, the Use of Images Policy, checking of settings, data protection and reporting issues.
- Clear reporting guidance, including responsibilities, procedures, and sanctions.
- Risk assessment, including legal risk.
- Guidance for pupils, parents/carers.

Academy/Trust staff should ensure that:

- No reference is made in social media to pupils, parents/carers or any Trust employee.
- They do not engage in online discussion on personal matters relating to members of the Academy or Trust community.
- Personal opinions should not be attributed to the Academy or Trust.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- They act as positive role models in their use of social media.

When official Academy/Trust social media accounts are established, there should be:

- A process for approval by senior leaders.
- Clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff.
- A defined approval process for posts containing pupil images or videos. Before publication, the responsible member of staff will check current permissions and any safeguarding restrictions, consider whether pupils are clearly identifiable, ensure that names or other identifying information are not linked to images, remove unnecessary metadata and use an appropriately reduced image resolution where practicable.
- Periodic reviews of pupil images and videos published through official social media accounts will be undertaken. Content will be removed where it is no longer required, is no longer current or no longer meets the requirements of the Digital and Video Images section of this policy.
- A code of behaviour for users of the accounts.
- 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, or impacts on, the Academy or Trust, it must be made clear that the member of staff is not communicating on behalf of the Academy or Trust, with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon an Academy / the Trust 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, the Academy/Trust may pro-actively monitor the Internet for public postings about the Academy/Trust.
- The Academy/Trust should effectively respond to social media comments made by others according to a defined policy or process.
- When parents/carers express concerns about the academy/Trust, on social media we will urge them to make direct contact with the relevant setting, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the Trust complaints procedure.

11. 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 online bullying 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.

The Trust also recognises that images published online may be copied, downloaded, harvested, altered or repurposed by third parties without permission, including through the use of artificial intelligence. This may include the creation of fabricated, abusive or otherwise harmful imagery, and the use of images in connection with coercion, extortion or other criminal activity. Consent to take or publish an image does not remove the need to consider these wider safeguarding risks. Academies will therefore take a risk-based and proportionate approach when selecting and publishing images of pupils.

The Trust recognises that parental/carer permission or another lawful basis for publishing an image does not, in itself, remove the safeguarding risks associated with making an identifiable image of a child publicly available online. Decisions about publication will therefore consider both data protection requirements and the wider safeguarding risk to the child, including the potential for images to be copied, harvested, manipulated or misused using artificial intelligence or other technologies.

Each Academy will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

The Academy may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies. Guidance can be found on the SWGfL Safer Remote Learning web pages and in the DfE Safeguarding and remote education.

- When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images.
- Staff/volunteers must be aware of those pupils whose images must not be taken/published. Those images must only be taken on Academy devices. The personal devices of staff must not be used for such purposes.

- Parents/carers may be permitted to take photographs or videos at Academy events for their own personal or household use, subject to any safeguarding restrictions or arrangements communicated by the Academy. Academies may restrict or prohibit photography or recording at particular events where this is necessary to safeguard children, protect privacy or manage other identified risks.
- Where photographs or recordings include children other than their own, parents/carers will be asked to respect the privacy and safeguarding of others and not to publish or make those

images publicly available without appropriate permission. Parents/carers should not identify, tag or publish information about other children shown in photographs or recordings.

- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow the Use of Images and Data Protection policies concerning the sharing, storage, distribution and publication of those images.
- Care should be taken when sharing digital/video images that pupils are appropriately dressed.
- 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 the Online Safety Policy.
- Before publishing an image of a pupil on a publicly accessible website, social media account or other online platform, staff will consider whether the publication is necessary and whether the same purpose could be achieved using an image that reduces the pupil's identifiability.
- Where reasonably practicable, published images will focus on the activity, achievement or work rather than providing a clear, close-up or face-on image of an individual pupil. Wider-angle, group, side-on, rear-view or otherwise less identifiable images should be considered where these appropriately meet the purpose of publication.
- Images intended for public online publication will have unnecessary metadata removed before upload, including location and device information where present.
- Publicly available images will be uploaded at an appropriately reduced resolution and file size where this remains suitable for the intended purpose.
- Images will not be published where doing so could reveal confidential safeguarding information, a pupil's home location, regular routine or other information that could place the pupil at increased risk.
- pupils' full names will not be published on a website, social media account, blog or other publicly accessible platform. A pupil's first name, surname, initials, social media account, username or other identifying information will not normally be linked to their photograph. Any exceptional use must have a clearly documented purpose, be risk assessed and be authorised by the Principal or Headteacher following consultation with the Designated Safeguarding Lead and, where appropriate, the Data Protection Officer.
- Before images of pupils are taken, used or published, the Academy will ensure that there is an appropriate lawful basis for the processing and that pupils and/or parents/carers, as appropriate, have been provided with clear information about how the images will be used. Where the Academy relies upon consent, appropriate consent will be obtained and recorded before the image is used for that purpose. Pupils will be given an appropriate opportunity to express their wishes and, where appropriate, to opt out of the use or publication of their image.
- Parents/carers and, where appropriate, pupils will be provided with clear privacy information explaining how and why images may be used, the lawful basis relied upon, how images will be stored, who they may be shared with or made available to, and how long they will be retained, in accordance with the Trust's Data Protection Policy and Records Retention arrangements.
- Images will be securely stored in accordance with the Records and Retention Policy.
- Pupil's work can only be published with the permission of the pupil and parents/carers.

Online Publishing

Each Academy communicates with parents/carers, and the wider community, and promotes their setting through (each Academy should amend as necessary):

- Public-facing website
- Social media
- Online newsletters
- Other (to be described)

Each Academy and the Trust has a website which is managed and hosted effectively. Each Academy ensures that the Online Safety Policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of Academy calendars and personal information – ensuring that there is least risk to members of the Academy community, through such publications. Where pupil work, images or videos are published, their identities are protected, and full names are not published.

Before pupil images or videos are published through a public-facing website, social media account, online newsletter or other publicly accessible platform, the member of staff responsible for publication must follow the requirements set out in the Digital and Video Images section of this policy. This includes checking current permissions and any safeguarding restrictions, considering the identifiability of pupils, ensuring that names or other identifying information are not linked to images, removing unnecessary metadata and using an appropriately reduced image resolution where practicable.

Academies will periodically review pupil images and videos published on websites, social media accounts and other public-facing platforms. Content will be removed where it is no longer required, is no longer current or no longer meets the requirements of this policy.

Following significant changes in safeguarding advice or the identification of new technological risks, Academies will undertake a proportionate review of existing publicly available pupil images and videos. This will include consideration of whether images remain necessary, whether pupils are unnecessarily identifiable, whether identifying information is linked to images, and whether older content should be removed or replaced.

Each Academy publishes their Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc. There should be an online safety section on each Academy's website. Each website includes contact information for parents and the wider community to register issues and concerns relating to online safety.

12. Data Protection

Personal data will be recorded, processed, transferred, and made available according to the current data protection legislation and in accordance with Trust data protection policies and freedom of information policies including the Model Publication Scheme.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Can recognise a possible breach, understand the need for urgency and know who to report it.
- Can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to escalate this to.
- Only use encrypted data storage for personal data.
- Will not transfer any Academy or Trust personal data to personal devices. Procedures should be in place to enable staff to work from home (i.e. VPN access to the school network, or a work laptop provided).
- 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, a secure email account, and secure password protected devices.
- Where AI is used, data privacy is prioritised and protected.

Secure access of information out of the Academy / Trust

We recognise that personal data may be accessed by users out of school or transferred to the local authority or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the Academy / Trust or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when outside of the Academy / Trust.
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should have secure remote access to the management information system or learning platform.
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.

13. Incident Reporting

If an online safety issue/event or online abuse occurs, each academy will respond to this by:

- Immediately reporting the matter to the Principal where it relates to a member of staff, or to the Designated Safeguarding Lead where it relates to a pupil. The matter will then be assessed, managed and escalated in accordance with the Academy's safeguarding, managing allegations and online safety procedures.
- copying, alteration, AI-enabled manipulation or criminal misuse of a pupil's image, including any associated coercion, extortion or threat of publication or distribution, as a potential safeguarding incident requiring immediate referral to the Designated Safeguarding Lead. Staff must not conduct their own investigation, download, copy, save, print, share or circulate suspected illegal content.
- Following the Academy's clear and robust safeguarding procedures in place for responding to abuse (including online abuse) as detailed within the Safeguarding Policy.
- Providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation as required.
- Making sure the response takes the needs of the person experiencing abuse, any witnesses and our organisation as a whole into account.
- Reviewing the policies and procedures developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

The Trust will support staff who experience online abuse, harassment, impersonation, doxxing, threats or the malicious use of images or personal information. Communications and complaints will be managed through approved Trust channels and the Trust Complaints Policy. Staff concerns will also be managed, as applicable, in accordance with the Staff Code of Conduct and Whistleblowing Policy. Nothing in this section restricts any person from raising a safeguarding concern, making a protected disclosure or contacting an appropriate external authority.

Please also see section 3.

Responding to incidents of misuse

It is hoped that all members of the SUAT community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy

could take place through careless or irresponsible, or very rarely, through deliberate misuse. Listed in Appendix 2 are the responses that will be made to any apparent or actual incidents of misuse.

If any apparent or actual, misuse appears to involve illegal activity e.g. child sexual abuse images, adult material which potentially breaches the Obscene Publications Act, criminally racist material or other criminal conduct, activity or materials the flow chart should be consulted. Actions will be followed in accordance with policy, in particular the sections on reporting the incident to the police and the preservation of evidence. If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of SUAT's 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.

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by the Trust or national/local organisation (as relevant)
    - Police involvement and/or action
    - HR consultation

If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- Incidents of 'grooming' behaviour
- The sending of obscene materials to a child
- Adult material which potentially breaches the obscene publications act
- Criminally racist material
- Promotion of terrorism or extremism
- Offences under the computer misuse act (see user actions chart above)
- 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 Academy/Trust 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.

14. Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, pupils; parents/carers and is reported to relevant groups:

- There is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training.
- There are well-established routes to regularly report patterns of online safety incidents and outcomes to Academy leadership and LAC members.
- Parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising.
- Online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate.
- The evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

Appendix 1
Online Safety Group Terms of Reference

Purpose
To provide a consultative group that has wide representation from the Academy community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives. Depending on the size or structure of the Academy, this group may be part of the safeguarding group. The group will report regularly to the LAC and will meet at a frequency proportionate to the Academy's needs and online-safety risk profile.

Membership
The online safety group will seek to include representation from a wide range of stakeholders. The composition of the group should include:

- SLT member/s
- Designated Safeguarding Lead (DSL)
- Online Safety Lead (OSL)
- Teaching staff member
- Support staff member
- LAC member
- Parent/Carer
- IT Support Provider
- Community users (where appropriate)
- Pupil representation – for advice and feedback.

Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary. Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families. Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature and discussions should be subject to the appropriate confidentiality agreements. If individual members feel uncomfortable about what is being discussed, they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities.

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

- Scheduling meetings and notifying members.
- Inviting other people to attend meetings when required.
- Guiding the meeting according to the agenda and time available.
- Ensuring all discussion items end with a decision, action or definite outcome.
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary.

Functions
The group will assist the DSL/OSL (or other relevant person), as appropriate, with the following: To keep up to date with new developments in the area of online safety.

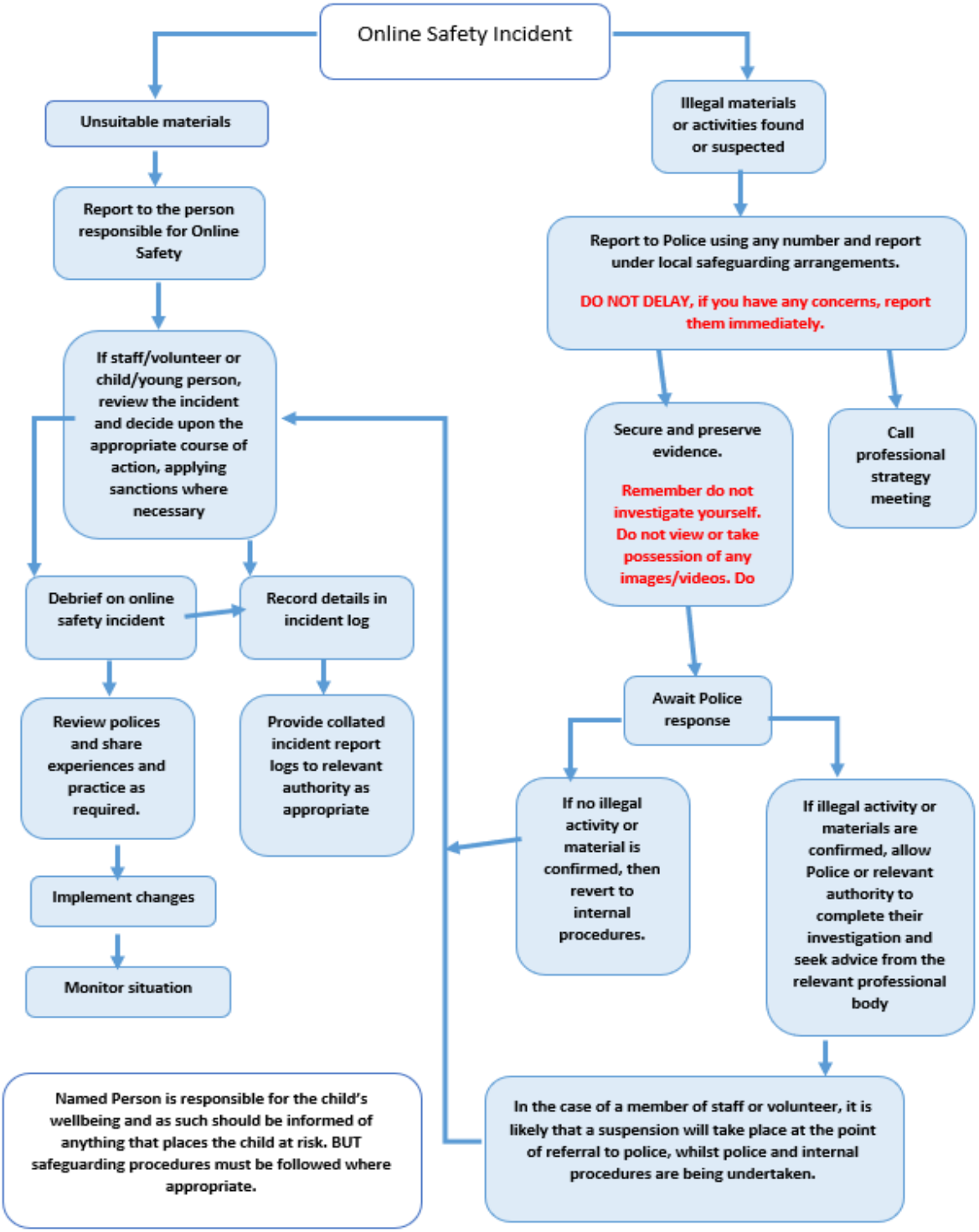
- To (at least) annually review the Online Safety Policy for their setting, considering new technologies and incidents, feeding back to the Trust surrounding policy development as relevant.
- To monitor the delivery and impact of the Online Safety Policy.
- To monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching/learning/training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety.

This may include:

- Staff meetings
- Pupil forums (for advice and feedback)
- Governors meetings
- Surveys/questionnaires for pupils, parents/carers and staff
- Parents evenings
- Website/newsletters
- Online safety events
- Internet Safety Day (annually held on the second Tuesday in February)
- Other methods
- To ensure that monitoring is carried out of Internet sites used across the schools.
- To monitor filtering/change control logs (e.g. requests for blocking/unblocking sites).
- To monitor the safe use of data across the schools
- To monitor incidents involving cyberbullying for staff and pupils

Amendments
The terms of reference shall be reviewed annually, in conjunction with the Online Safety Policy. They may be altered to meet the current needs of all committee members, by agreement of the majority.
Acknowledgement: This template terms of reference document is based on one provided to schools by Somerset County Council.

Appendix Two
Responding to Incidents of Misuse



Appendix Three
Record of Reviewing Devices/Internet Sites (when responding to incidents of misuse)

Group: .....
Date: .....
Reason for investigation: .....
.....
.....

Details of first reviewing person
Name: .....
Position: .....
Signature: .....

Details of second reviewing person
Name: .....
Position: .....
Signature: .....

Name and location of computer used for review (for web sites)
.....
.....

Web site(s) address/device	*Reason for concern*

Conclusion and Action proposed or taken	

Reporting Log
Group: .....

Date	*Time*	*Incident*	*Action Taken*		*Incident Reported By*	*Signature*
			What?	*By Whom?*		

Appendix Four
Training Needs Audit Log

Training Needs Audit Log				
Relevant training the last 12 months	*Identified Training Need*	*To be met by*	*Cost*	*Review Date*

Appendix Five – Searching, Screening, Confiscation and Electronic Devices

Searching, screening and confiscation, including decisions concerning electronic devices and data held on those devices, will be undertaken in accordance with the Academy Behaviour Policy and the Department for Education's current *Searching, Screening and Confiscation* guidance.

Each Academy will identify the members of staff authorised by the Headteacher to undertake searches in accordance with the statutory framework and Academy procedures. Staff must act proportionately, have regard to safeguarding, equality, SEND and privacy considerations, and make an appropriate record of searches and resulting actions.

Where an electronic device is lawfully searched or examined, staff must follow the current Department for Education guidance concerning examination, retention, deletion and disposal of data. Where material may constitute evidence of an offence, staff must preserve the device and evidence and seek appropriate safeguarding and/or police advice rather than deleting the material.

Staff must not intentionally view, copy, print, save, share or circulate suspected child sexual abuse material. Where such material is suspected, the matter must be referred immediately to the Designated Safeguarding Lead and managed in accordance with safeguarding procedures and appropriate police or specialist advice.

Any search or examination involving a safeguarding concern must be brought to the attention of the Designated Safeguarding Lead.

A record will be made of searches and examination of electronic devices where required by statutory guidance, the Academy Behaviour Policy or safeguarding procedures. Records will be retained and reviewed in accordance with the Trust's safeguarding, behaviour and records-management arrangements.

Each Academy will ensure that its Behaviour Policy clearly identifies prohibited items and any items for which authorised staff may exercise statutory search powers, and that local arrangements are communicated appropriately to staff, pupils and parents/carers.

Appendix Six
Resources and Legislation

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

It is recommended that legal advice is sought in the advent of an online safety issue or situation. A useful summary of relevant legislation can be found at: Report Harmful Content: Laws about harmful behaviours

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.

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

UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 and Data (Use and Access) Act 2025

The Trust processes personal data in accordance with the UK GDPR and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025. These requirements apply to personal data processed through digital technologies, online services, photographs and videos, monitoring systems, artificial intelligence and other technologies used by the Trust and its Academies.

Personal data must be processed lawfully, fairly and transparently; collected for specified, explicit and legitimate purposes; adequate, relevant and limited to what is necessary; accurate and, where necessary, kept up to date; retained only for as long as necessary; and processed in a manner that ensures appropriate security.

The Trust and its Academies will ensure that appropriate technical and organisational measures, accountability arrangements, privacy information and procedures are in place to protect personal data and demonstrate compliance with data protection legislation.

Particular care will be taken when processing children's personal data. The Trust and its Academies will consider the rights and interests of children, provide privacy information in a clear and accessible form and ensure that the lawful basis for processing is identified and documented.

Where artificial intelligence, automated systems or other emerging technologies are used to process personal data, the Trust and its Academies will consider the associated data protection, privacy, security and safeguarding risks before use and will implement appropriate safeguards and human oversight.

Individuals have rights in relation to their personal data under data protection legislation. These may include, depending on the circumstances, rights of access, rectification, erasure, restriction, objection and rights relating to automated decision-making. Requests to exercise data protection rights will be managed in accordance with the Trust's Data Protection Policy and relevant procedures.

Freedom of Information Act 2000
The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988
It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

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

Trade Marks Act 1994
This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

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

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Sexual Offences Act 2003
A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006
Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of 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/learnersupport/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)

Criminal Justice and Courts Act 2015
Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act

specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

For further guidance or support please contact the Revenge Porn Helpline

Resources

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

UK Safer Internet Centre

- UK Safer Internet Centre – Image Guidance for Education Settings: Protecting your setting's images from AI manipulation and abuse
- Safer Internet Centre – https://www.saferinternet.org.uk/
- South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
- Childnet – http://www.childnet-int.org/
- Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
- Revenge Porn Helpline - https://revengepornhelpline.org.uk/
- Internet Watch Foundation - https://www.iwf.org.uk/
- Report Harmful Content - https://reportharmfulcontent.com/
- Harmful Sexual Support Service

CEOP

- CEOP - http://ceop.police.uk/
- ThinkUKnow - https://www.thinkuknow.co.uk/

Others

- LGfL – Online Safety Resources
- Kent – Online Safety Resources page
- INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/
- UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety

Tools for Schools / other organisations

- Online Safety BOOST – https://boost.swgfl.org.uk/
- 360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/
- 360Data – online data protection self-review tool: www.360data.org.uk
- SWGfL Test filtering - http://testfiltering.com/
- UKCIS Digital Resilience Framework - https://www.gov.uk/government/publications/digital-resilience-framework
- SWGfL 360 Groups – online safety self review tool for organisations working with children
- SWGfL 360 Early Years - online safety self review tool for early years organisations

Bullying/Online-bullying/Sexting/Sexual Harassment

- Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/
- SELMA – Hacking Hate - https://selma.swgfl.co.uk
- Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
- Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388
- DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
- Childnet – Cyberbullying guidance and practical PSHE toolkit:

- http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit
- Childnet – Project deSHAME – Online Sexual Harrassment
- UKSIC – Sexting Resources
- Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm
- Ditch the Label – Online Bullying Charity
- Diana Award – Anti-Bullying Campaign

Social Networking

- Digizen – Social Networking
- UKSIC - Safety Features on Social Networks
- Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum

- SWGfL Evolve - https://projectevolve.co.uk
- UKCCIS – Education for a connected world framework
- Department for Education: Teaching Online Safety in Schools
- Teach Today – www.teachtoday.eu/
- Insafe - Education Resources

Data Protection

- 360data - free questionnaire and data protection self review tool
- ICO Guides for Organisations
- IRMS - Records Management Toolkit for Schools
- ICO Guidance on taking photos in schools

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/Cyber-security

- UKSIC – Appropriate Filtering and Monitoring
- SWGfL Safety & Security Resources
- Somerset - Questions for Technical Support
- SWGfL - Cyber Security in Schools.
- NCA – Guide to the Computer Misuse Act
- NEN – Advice and Guidance Notes

Working with parents and carers

- SWGfL – Online Safety Guidance for Parents & Carers
- Vodafone Digital Parents Magazine
- Childnet Webpages for Parents & Carers
- Get Safe Online - resources for parents
- Teach Today - resources for parents workshops/education
- Internet Matters

Prevent

- Prevent Duty Guidance
- Prevent for schools – teaching resources
- Childnet – Trust Me

Research

- Ofcom –Media Literacy Research
- Ofsted: Review of sexual abuse in schools and colleges

Further links can be found at the end of the UKCIS Education for a Connected World Framework

Glossary of Terms

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

A more comprehensive glossary can be found at the end of the UKCIS Education for a Connected World Framework.

This policy and appendices is built on the Online Safety Policy Templates of the SWGfL. We recognise that the copyright of the SWGfL School Online Safety Policy Templates is held by SWGfL and that educational institutions are permitted free use of the templates. Every reasonable effort has been made to ensure that the information included in the SWGfL template is accurate, as at the date of publication in September 2026.

Appendix Seven - **Academy Online Safety Arrangements**

This appendix forms part of the Trust Online Safety Policy and records the academy-specific arrangements necessary to support implementation of the policy. It should be read alongside the

Academy Cyber Response Plan, which contains detailed cyber-security contacts, escalation arrangements and incident-response information.

The core Trust Online Safety Policy must not be amended locally. This appendix should be reviewed at least annually and following any significant change to the arrangements recorded below.

Academy-specific arrangement	**Details**
Academy name	
Designated Safeguarding Lead (DSL)	
Online Safety Lead (where different from the DSL)	
SLT member responsible for filtering and monitoring	
Responsible LAC member	
Filtering system used	
Monitoring system used	
Frequency of filtering and monitoring checks	

Cyber-security and incident-response arrangements
Cyber-security contacts, IT provider details, out-of-hours arrangements, cyber incident escalation routes and detailed cyber-response procedures are maintained within the Academy Cyber Response Plan and are not duplicated within this appendix.

Safeguarding
Online-safety concerns involving the welfare or safeguarding of a child must be reported to the Designated Safeguarding Lead (or a Deputy DSL in their absence) and managed in accordance with the Trust Safeguarding Policy and the Academy's safeguarding procedures.