Online Safety Policy

Scope of the Online Safety Policy

This policy is written with regard to Keeping Children Safe in Education (KCSIE) 2025, the DfE Filtering and Monitoring Standards (2023), the DfE Mobile Phones in Schools Guidance (2024), the DfE Generative AI in Education Guidance (2025), and the UK GDPR and Data Protection Act 2018.

Policy development, monitoring and review

This Online Safety Policy has been developed by the *Online Safety Group* made up of: DSL, Bursar, Network Manager, IT Coordinator, pupil leaders.
Consultation with the whole school community has taken place through a range of formal and informal meetings.
This policy should be read in conjunction with the following policies:

Safeguarding and Child Protection Policy	Data Protection Policy
AUA: Pupil, Staff, Parents & community	Positive Behaviour Policy & Anti-Bullying Policy
PSHE Policy	

Schedule for development, monitoring and review

This Online Safety Policy was approved by the school governing body on:	Date:
The implementation of this Online Safety Policy will be monitored by:	Online Safety Group (OSG)
Monitoring will take place at regular intervals:	Termly
The governing body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Termly (within Head's Report)
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 next anticipated review date will be:	September 2026
Should serious online safety incidents take place, the following external persons/agencies should be informed:	Police Trafford First Response

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- logs of reported incidents
- Filtering and monitoring logs
- internal monitoring data for network activity

surveys/questionnaires of:

  - learners
  - parents and carers
  - staff

Roles and Responsibilities:

Online safety is a **whole-school responsibility**. All members of the community must model safe behaviour, report concerns promptly and support a culture of safeguarding. In line with *Keeping Children Safe in Education (KCSIE 2025)*, the following roles have specific duties:

Governors:

- Approves and oversees the Online Safety Policy (*KCSIE 2025*).
- Receives regular reports on incidents, monitoring and provision.
- Appoints a named **Online Safety Governor** to:
    - Meet with the DSL/Online Safety Lead.
    - Review anonymised incident/monitoring reports.
    - Check that curriculum and staff training meet KCSIE 2025 expectations.
    - Ensure filtering and monitoring are reviewed annually in line with DfE *Filtering & Monitoring Standards (2023)*.
    - Undertake basic cyber security training to support compliance with DfE *Cyber Security Standards (2023)*.
- Supports parental and community engagement in online safety.

Headteacher and Senior Leaders:

- Hold overall responsibility for safeguarding, including online safety, under *KCSIE 2025*.
- Ensure the DSL leads day-to-day online safety and receives appropriate support.
- Know procedures for responding to allegations against staff (as set out in KCSIE 2025).
- Ensure DSL/OSL, IT staff and colleagues receive training and carry out duties effectively.
- Put systems in place to support staff with monitoring responsibilities.
- Receive regular reports from the DSL/OSL.
- Work with the Online Safety Governor, DSL and IT provider on filtering and monitoring in line with DfE standards.

Designated Safeguarding Lead (DSL):

- Leads safeguarding and online safety in line with *KCSIE 2025*.
- Manages incidents, ensuring concerns are logged, escalated and referred to agencies where required.
- Liaises with the Headteacher, Online Safety Lead, IT staff, parents and external agencies.
- Ensures staff and pupils know how to report concerns.
- Provides regular updates and training to staff and governors.

Online Safety Lead (OSL):

- Works closely with the DSL to coordinate online safety.
- Leads the Online Safety Group and oversees policy review.
- Promotes online safety awareness across the school and community.
- Ensures curriculum covers the four KCSIE 2025 risk areas: **content, contact, conduct, commerce**.
- Ensures staff follow reporting procedures.
- Coordinates training for staff, governors, parents and pupils.
- Keeps up to date with developments and emerging risks.

Curriculum Leads:

- Work with the DSL/OSL to deliver a planned online safety programme in line with *KCSIE 2025*.
- Ensure provision is embedded through:
    - Discrete lessons.
    - PSHE/RSHE.

- Assemblies and pastoral activities.
- National initiatives (e.g. Safer Internet Day, Anti-Bullying Week).

Teaching and Support Staff:

- Share responsibility for online safety as part of safeguarding under *KCSIE 2025*.
- Follow the Online Safety Policy and Staff AUA.
- Report concerns immediately to the DSL/OSL.
- Use only professional, school-approved systems for communication.
- Embed online safety in teaching, promoting safe research, copyright respect and digital resilience.
- Supervise pupil use of technology and apply school rules.
- Follow safeguarding guidance for live-streaming/video-conferencing.
- Adopt zero tolerance to online bullying, harassment, discrimination or hate.
- Model safe, professional behaviour, including use of social media.

Network Manager:

- Maintains a secure technical infrastructure, in line with *KCSIE 2025*, DfE *Filtering & Monitoring Standards (2023)* and *Cyber Security Standards (2023)*.
- Manages safe user access to networks and devices.
- Applies, reviews and updates filtering and monitoring systems.
- Monitors use of technology and reports concerns to the DSL/OSL.
- Keeps up to date with technical and safeguarding developments.

Learners:

- Use school technology responsibly, following the **Pupil Acceptable Use Agreement**.
- Report abuse, misuse or inappropriate content.
- Seek help if they or others feel unsafe online.
- Follow safe online practice outside school, recognising behaviour linked to school is covered by this policy (*KCSIE 2025*).

Parents/Carers:

- Support the school's Online Safety Policy and AUAs.
- Promote safe use of technology at home.
- Encourage open discussions and reporting of concerns.
- Engage with school guidance and initiatives (*KCSIE 2025*).

Community Users:

- Sign a **Community User AUA** before accessing school systems.
- Follow school safeguarding and data protection expectations.
- Contribute to wider community online safety and share good practice.

Online Safety Group:

- Includes: **DSL, OSL, senior leaders, Online Safety Governor, Network Manager, learner reps**.
- Supports the DSL/OSL by:
  - Reviewing policies and filtering provision.
  - Mapping and evaluating the online safety curriculum.
  - Reviewing logs and incidents.
  - Consulting staff, parents and pupils.
  - Monitoring progress against the 360-degree safe tool.

Online Safety Policy:

In line with *Keeping Children Safe in Education (KCSIE 2025)*, the Online Safety Policy:

- Sets expectations for the safe and responsible use of digital technologies.
- Allocates responsibilities for delivery and oversight.
- Is reviewed regularly to reflect incidents, trends and new risks.
- Guides staff in safe use of technology to protect themselves, the school and safeguard learners.
- Prepares learners to be safe, responsible and resilient users.
- Establishes clear procedures for reporting and responding to concerns.
- Is supported by **Acceptable Use Agreements (AUAs)** for staff, pupils, parents and community users.
- Is shared with staff at induction and published on the school website.

Acceptable Use Agreements

The Online Safety Policy and **Acceptable Use Agreements (AUAs)** set out expectations for the safe use of technology by staff, learners, parents/carers and community users.

In line with *KCSIE 2025*, AUAs are communicated and reinforced through:

- Staff induction, handbook and training.
- Pupil planners, class booklets and education sessions.
- Parent/carer communications.
- Posters and notices near technology use areas.
- The school website and peer support.

Communication Technologies:

In line with *KCSIE 2025*, the school expects:

- Staff to use only **school-sanctioned platforms** when communicating in a professional capacity.
- All digital communication with learners or parents to be professional in tone and content; personal email, messaging or social media must not be used.
- Staff to maintain professional standards on personal social media, protecting their reputation and that of the school.
- Any offensive, discriminatory, threatening or bullying communication to be **reported immediately** to the DSL/OSL; users must not respond.
- Online postings to follow relevant policies and permissions; only school email addresses should identify staff and learners.

Reporting and Responding:

The school takes all reasonable precautions to safeguard users but recognises that incidents may occur both in and out of school. In line with *KCSIE 2025* and safeguarding procedures, the school will:

- Maintain clear reporting routes, consistent with safeguarding, whistleblowing, complaints and managing allegations policies.
- Ensure all staff, learners and parents know how to report online safety concerns.
- Respond to reports promptly and treat them seriously.
- Ensure the **DSL, OSL and responsible staff** have the skills and training to manage incidents.
- Escalate incidents involving suspected illegal activity (e.g. CSAM, grooming, hate crime, extremism, fraud, harassment, cybercrime) through safeguarding procedures and external agencies (police, CEOP, LA, etc.).
- Report staff misuse to the **Headteacher** (or Chair of Governors if the Headteacher is implicated).
- Use safe, controlled procedures when checking devices, ensuring involvement of senior staff, accurate logging, and police referral if necessary.

- Record incidents on **CPOMS** and keep detailed logs/screenshots where appropriate.
- Provide support and feedback to those affected and ensure confidence in the process.
- Share lessons learned (anonymised) with staff, pupils, parents, governors, and external partners as appropriate.
- Regularly review outcomes through the **Online Safety Group** to update policy and education.

Filtering and Monitoring:

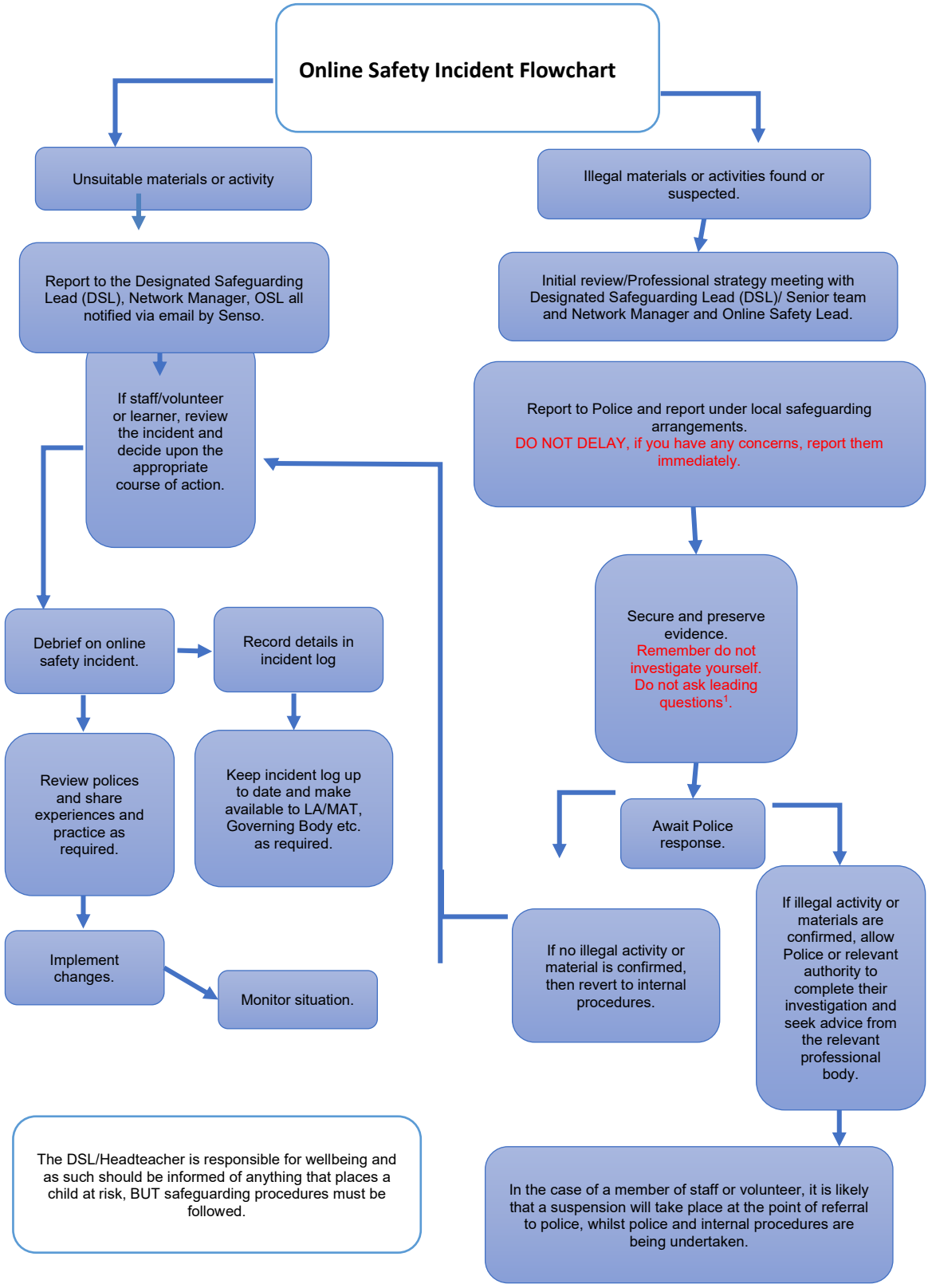
The school's filtering and monitoring arrangements are overseen by senior leaders, governors and the **Network Manager**, with day-to-day responsibilities shared between safeguarding and IT staff. Provision is reviewed at least annually, and more frequently when risks, technology or working practices change (*KCSIE 2025*).

- **Filtering**
    - Access to online content is managed across all systems and devices. Filtering meets the **DfE Filtering Standards (2023)** and the UK Safer Internet Centre guidance.
    - Illegal content (e.g. CSAM, terrorist material) is blocked using the Internet Watch Foundation and Home Office lists.
    - Users can report inappropriate content through established routes; all requests for filtering changes are logged and auditable.
    - Filtering logs are regularly reviewed; breaches alert the DSL for immediate action.
    - Differentiated filtering is applied for different ages/groups, with child-friendly search engines used for younger learners.
    - Filtering applies to all devices on the school network, including personal devices, browsers and apps.
    - Mobile phone access is managed in line with the DfE **Mobile Phones in Schools Guidance (2024)**.
    - Issues may be referred to external agencies such as **Report Harmful Content**.
- **Monitoring**
    - Monitoring software (**Senso**) is installed on all devices and configured to alert the DSL, OSL and Network Manager to concerning activity.
    - Alerts provide date, time, device, user log-in and screenshots to evidence incidents.
    - Activity before and after incidents is logged to provide context.
    - All incidents are recorded on **CPOMS**, ensuring an up-to-date record for safeguarding oversight.
    - Reports are reviewed with governors, in line with the DfE *Filtering & Monitoring Standards (2023)*.

School Actions:

Most incidents will involve **inappropriate, not illegal, misuse**. In line with *KCSIE 2025*, the school will ensure that:

- Incidents are dealt with promptly and proportionately.
- Responses follow normal behaviour and disciplinary procedures (see **Positive Behaviour Policy**).
- The school community is reassured that concerns are addressed effectively.


Online Safety Incident Flowchart
Unsuitable materials or activity
Illegal materials or activities found or suspected.
Report to the Designated Safeguarding Lead (DSL), Network Manager, OSL all notified via email by Senso.
Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team and Network Manager and Online Safety Lead.
If staff/volunteer or learner, review the incident and decide upon the appropriate course of action.
Report to Police and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Debrief on online safety incident.
Record details in incident log
Secure and preserve evidence.
Remember do not investigate yourself.
Do not ask leading questions[1].
Review polices and share experiences and practice as required.
Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.
Await Police response.
Implement changes.
Monitor situation.
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.
The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Online Safety Education Programme:

In line with *KCSIE 2025*, online safety is embedded across the curriculum. Provision is:

- Planned for all year groups against national frameworks (e.g. **Education for a Connected World**, Project Evolve).
- Age-appropriate, needs-based, and context relevant, with clear outcomes.
- Integrated into PSHE, RSHE, literacy and other subjects.
- Supported by national initiatives such as **Safer Internet Day** and **Anti-Bullying Week**.
- Accessible for all learners, including those with SEND, EAL or increased vulnerability.
- Reinforced through the **Pupil Acceptable Use Agreement (AUA)**, promoting safe, responsible and lawful use (including copyright and Computer Misuse Act 1990).
- Supported by staff modelling positive behaviours and ensuring safe search practices, supervision, and controlled exceptions when required

Contribution of Learners:

Learners contribute to shaping the school's online safety culture through:

- Feedback and consultation.
- Roles such as **digital leaders, STEM Captains, peer mentors and ambassadors**.
- Participation in the Online Safety Group.
- Leading peer education, campaigns and parent engagement events

Staff and Volunteers:

All staff receive training as part of safeguarding, in line with *KCSIE 2025*:

- Induction covers the Online Safety Policy, AUAs, professional conduct and classroom management.
- Annual safeguarding training includes online safety and data protection, with regular updates.
- Needs audits ensure provision is relevant and reinforced through INSET and staff meetings.
- The DSL/OSL receive enhanced training and updates from national providers (e.g. UKSIC, LGfL)

Governors:

Governors receive online safety training, particularly those on safeguarding or technology committees. The **Online Safety Governor** receives enhanced training, including:

- **Cyber security awareness**.
- Understanding and reviewing the school's **filtering and monitoring provision** in line with DfE standard

Families:

Parents and carers play a vital role in online safety. The school supports them through:

- Regular communication, newsletters and workshops.
- Awareness events (e.g. Safer Internet Day).
- Learner-led sessions and home-school communication.
- Signposting to national resources (e.g. UKSIC, Childnet, SWGfL)

Adults and Agencies:

The school extends online safety knowledge to the wider community by:

- Sharing guidance and campaigns with families and local groups.

- Offering family learning opportunities.
- Providing information via the website and social media.

Artificial Intelligence (AI):

In line with the *DfE Generative AI in Education Guidance (2025)*, AI may be used to support teaching, learning and workload where **safeguarding, data protection and academic integrity** are upheld.

- Staff must not enter identifiable pupil or sensitive data into consumer AI tools.
- Only **school-approved AI platforms** may be used, following a completed Data Protection Impact Assessment (DPIA).
- Pupils are taught about AI's opportunities and risks, including **bias, misinformation and copyright**.
- Misuse of AI in assessments is treated as malpractice.

The school ensures that infrastructure and procedures are secure, compliant with *KCSIE 2025* and **UK GDPR**, and that all staff understand their responsibilities for online safety and data protection.

Technical Security:

The school's technical systems are managed in line with *DfE Cyber Security Standards (2023)*. Senior leaders hold overall responsibility, delegating tasks to IT staff where appropriate.

- Access rights to systems and devices are clearly defined and reviewed annually by SLT/Online Safety Group.
- Strong password policies are enforced; administrator passwords are securely stored.
- Servers, wireless systems and cabling are physically secured.
- Security measures protect all networks, devices, and data; endpoint software is kept up to date.
- Regular audits and testing are undertaken to assess system safety.
- Rigorous back-up routines are in place, including offline/air-gapped storage.
- All software is appropriately licensed and updated (patched) promptly.
- Incidents and breaches are reported immediately via agreed procedures.
- Staff must not install software, use removable media, or connect personal devices without authorisation.
- Use of school devices outside school is regulated by **Acceptable Use Agreements (AUAs)**.
- Personal data is protected in line with **UK GDPR**, encrypted at rest and in transit.
- Guest users are provided with restricted access based on a risk assessment

The school acceptable use agreements for staff, learners, parents, and carers outline the expectations around the use of mobile technologies.

The school allows:

	School devices			**Personal devices**		
	School owned for individual use	School owned for multiple users	Authorised device[1]	Student owned	Staff owned	Visitor owned
Allowed in school	**Yes**	**Yes**	**Yes**	No	Yes	Yes
Full network access	Yes	Yes	Yes	N/A	No	No
Internet only	N/A	N/A	N/A	N/A	Yes-Guest	Yes - Guest
No network access	N/A	N/A	N/A	N/A	N/A	N/A

Devices

School-Owned Devices:

- Managed using **Mobile Device Management (MDM)** where possible.
- Allocation recorded in an asset log; guidance on permitted use is clearly communicated.
- Personal use (e.g. banking, shopping, images) is restricted and defined.
- Expectations for use on trips/events are explained in advance.
- Liability for loss or damage follows the school's equipment replacement policy.
- Learners and staff receive education to support safe and responsible use.

Personal Devices:

- A clear policy regulates the use of personal devices on school premises, in line with *KCSIE 2025* and **DfE Mobile Phones Guidance (2024)**.
- Secure storage is provided where devices are brought in but use is not permitted.
- Personal devices used for school business must follow the **Acceptable Use Policy** and are segregated from school systems.
- Use of images/video must comply with the **AUA** and the school's **Use of Images/Video Policy**; non-consensual recording is prohibited.
- Liability for loss, damage or malfunction is clearly defined.
- Visitors are made aware of device requirements on entry.
- Safe and responsible use of mobile devices is reinforced through the school's **online safety education programme**

Social Media

As part of our safeguarding responsibilities, the school recognises that social media presents both opportunities and risks for children, parents, and staff. In line with *Keeping Children Safe in Education (KCSIE) 2025*, the Online Safety Act 2023, and our Acceptable Use and E-Safety Policies, the following expectations apply:

Safeguarding Measures:

- Personal information about learners, parents/carers, or staff will not be published on school accounts.
- All pupils receive education on safe and responsible use of technology, including age restrictions, risks of **misinformation and disinformation**, digital images, data protection, privacy settings, and how to report concerns.
- Clear reporting routes exist for pupils, staff, and parents/carers, including escalation to the Designated Safeguarding Lead (DSL).
- Risk assessments cover online harms, including **cybersecurity**, legal risks, and harmful or age-inappropriate content (as defined in the Online Safety Act).
- Guidance is provided to staff, pupils, and parents/carers on positive digital behaviour and safeguarding expectations.

Expectations for Staff

- No reference should be made on social media to learners, parents/carers, or colleagues.
- Staff must not engage in online discussions relating to personal matters involving the school community.
- Personal views expressed online must not be attributed to the school; disclaimers should be used where relevant.
- Privacy and security settings on personal accounts must be regularly reviewed.
- Staff must act as positive digital role models, consistent with the Staff Code of Conduct and safer working practice guidance.

Official School Social Media Accounts

- Accounts require senior leader approval.
- At least two members of staff must administer, moderate, and monitor each account.
- A clear code of behaviour applies to all official use.
- Misuse or abuse will be reported and managed through safeguarding and disciplinary procedures.

Personal Use

- Personal communications that link to or impact upon the school fall within this policy; a disclaimer must make clear that views are personal.
- Personal use of social media unconnected to the school is outside this policy's scope.
- Excessive use during working hours, or use that undermines safeguarding responsibilities, may lead to disciplinary action.

Monitoring and Responding to Concerns

- The school may monitor public posts relating to the school as part of safeguarding and reputational protection.
- Concerns raised about the school via social media will be directed to private resolution; unresolved issues will follow the **Complaints Procedure**.
- Online incidents, including harmful content, cyberbullying, or risks from AI-generated material, will be addressed under safeguarding and child protection procedures.

Digital and Video Images

The use of digital and video images is an important aspect of school life for learning, assessment, and celebration of achievement. However, such use carries safeguarding and data protection risks. In line with *KCSIE 2025*, the UK GDPR, and ICO guidance, the school implements the following safeguards:

Education and Awareness

- Learners are taught about the risks associated with the taking, use, sharing, publication, and distribution of images.
- The school may use live-streaming or video-conferencing platforms where appropriate, ensuring compliance with national and local safeguarding policies.

Staff and Volunteers

- Staff and volunteers must be aware of learners whose images must not be taken or published; lists are held securely by the DSL/administration.
- Images must only be captured using **school devices**; personal devices must not be used.
- Images may only be taken, stored, and shared in line with school policies, including the Online Safety Policy, Data Protection Policy, and Safeguarding Policy.
- Staff must ensure learners are appropriately dressed and that content does not compromise dignity or safety.

Parents and Carers

- Parents/carers may take photographs or recordings of their own child at school events for **personal use only**, as permitted under ICO guidance.
- Such images must not be shared publicly (e.g. on social media) if they include other learners, nor should they be used to comment on activities involving other children.
- Parents/carers will be informed of the purposes, storage, and retention of any images taken by the school.

Learners

- Learners must not take, use, share, or distribute images of others without consent.
- Learners' work and images will only be published with permission from the learner and their parent/carer.

Publication and Storage

- Photographs published on the school website, social media, or other media will be carefully selected and will not include learners' full names.
- Written parental consent is required before any learner image is published externally. Consent is not required for images used solely for internal educational purposes.
- All images are securely stored and retained only in line with the school's Data Protection and Retention Policies.

Online Publishing

The school communicates with parents, carers, and the wider community through:

- The public-facing website (hosted by **InnerMedia**)
- Social media platforms
- Newsletters
- Contributions to community and national publications

All online publishing follows the school's **Online Safety Policy** and statutory guidance, including **KCSIE 2025**. This ensures responsible use of digital content, compliance with copyright, and protection of personal information. **Learners are never identified by full name alongside images or videos.**

The website includes:

- The school's Online Safety Policy and acceptable use agreements
- Up-to-date advice and guidance on safe online practice
- News and resources for parents and carers
- A secure online reporting process for concerns, complementing internal safeguarding procedures

This approach minimises risk while ensuring effective communication and transparency with the school community.

Data Protection

The school ensures that all online safety practice complies with the **Data Protection Act 2018**, **UK GDPR**, and the statutory guidance set out in **Keeping Children Safe in Education (KCSIE) 2025**.

In line with KCSIE 2025, staff understand that data protection legislation does **not** prevent the sharing of information for the purposes of safeguarding. Where necessary, personal and special category data will be shared lawfully in order to protect children and individuals at risk.

Outcomes

- Review and audit of online safety incident logs, behaviour and bullying reports, and surveys of staff, learners, and parents/carers
- Balanced professional debate on the effectiveness of preventative measures (e.g. education, awareness, training)
- Established reporting routes for online safety trends and outcomes to senior leadership and Governors
- Informing parents/carers of patterns of online safety incidents, as part of awareness-raising activity
- Updating policies and procedures in response to evidence gathered from reviews, audits, and national guidanc

Appendix

Legislation

A summary of the legislative framework under which this policy has been produced 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.

Schools 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 UK GDPR and Data Protection Act 2018

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

The Data Protection Act 2018:

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

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

All data subjects have the right to:

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

- Prevent or query about the automated processing of their personal data.

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

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

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

Regulation of Investigatory Powers Act 2000
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:
- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The Education and Inspections Act 2006
Empowers Headteacher, to such extent as is reasonable, to regulate the behaviour of learners 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 Headteacher (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

Links to other organisations or documents

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

UK Safer Internet Centre
Safer Internet Centre – https://www.saferinternet.org.uk/
South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Revenge Porn Helpline - https://revengepornhelpline.org.uk/
Internet Watch Foundation - https://www.iwf.org.uk/
Report Harmful Content - https://reportharmfulcontent.com/
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_Headteacher_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

Move to top of document

Annex A: Staff Acceptable Use Agreement

• Use school ICT responsibly and professionally
• Use only school-approved platforms to communicate with pupils
• Do not access or share inappropriate content
• Protect passwords and data, and report concerns immediately
• Follow the Staff Code of Conduct and safeguarding procedures

Annex B: Pupil Acceptable Use Agreement

• I will use school ICT responsibly and for learning
• I will keep my passwords private
• I will not share personal information online
• I will be kind and respectful online
• I will tell an adult if I see anything worrying or upsetting

Annex C: Parent/Carer Acceptable Use Agreement

• Support the school in promoting safe online behaviour
• Supervise my child's use of technology at home
• Reinforce the school's rules for safe and responsible ICT use
• Report any online concerns to school promptly
• Use school communication channels appropriately

Annex D: Community User Acceptable Use Agreement

• Use school ICT only for authorised purposes
• Respect the school's safeguarding and data protection policies
• Do not access or share inappropriate material
• Protect login details and follow staff instructions
• Report any issues to the school immediately