ONLINE SAFETY

Frequency of Review	Annually
Date of Approval	March 2026
Date of Next Review	March 2027
Adopted by the Board of Empower Trust	

Summary of main updates:

Major additions:

- Four Categories of Online Risk framework (Content, Contact, Conduct, Commerce) - Section 1
- NEW Section 14A: Sharing of nudes and semi-nudes - comprehensive UKCIS-aligned procedures
- NEW Section 14B: Peer-on-peer abuse online including AI-generated images
- Enhanced incident response procedures with 8-step process - Section 19
- Strengthened filtering, monitoring and cyber security standards - Sections 16-17
- Comprehensive generative AI guidance - Section 18

Key updates:

- Updated to KCSIE 2025 throughout
- Enhanced staff training requirements aligned with current statutory guidance
- Strengthened review arrangements
- Updated Prevent Duty references
- All appendices reviewed and updated where required

Policy now fully compliant with KCSIE 2025, DfE filtering and monitoring standards, and DfE cyber security standards for schools.

Contents	
1.	Introduction
2.	Scope
3.	The Prevent Duty Prevent and schools - guidance, key legislation, campaigns and links
4.	Governing Legislation
5.	Roles & Responsibilities
6.	Definitions: Devices & Technology
7.	School staff, Governors and Volunteers • OVERVIEW: Acceptable Use Policy (AUP) for Staff • OVERVIEW: Acceptable Use of Devices and Technologies: Staff • Staff breaches of the AUP
8.	Pupils • Overview of Acceptable Use Policy (AUP) for Pupils • Overview of Acceptable Use of Devices and Technologies: Pupils • Pupil Breaches for AUP
9.	Using non-School Equipment – 'Bring Your Own Device/Bring Your Own Technology' (BYOD/BYOT)
10.	Security and passwords
11.	Data storage
12.	Mobile phones, cameras and other devices (Staff) Mobile phones, cameras and other devices (Pupils)
13.	Social Media & Networking
14.	Cyberbullying • Cyberbullying against staff
15.	Mental Health
16.	Filtering and Monitoring; Online Safety Audit
17.	Cyber Security
18.	Generative artificial intelligence (AI)
19.	Staff Reporting of Online Incidents and Concerns
20.	Staff training and updates
21.	Communicating the Online Safety Policy
22.	Shropshire Safeguarding Contact details
23.	Monitor & Review
	Title
A	**AUP for Staff, visitors and governors**
B	**AUP for learners in KS1**
C	**AUP for learners in KS2**
D	**Home-school Online Safety Agreement; ICT, Mobile Phones, Personal Photographs and Social Media**
E	**Online Roles & Responsibilities: List of duties**
F	**Legislation -Overview of relevant legislation governing online safety**
G	**Online Incident Reporting Log**
H	**Examples of potential online concerns (Pupils)**
I	**How to Manage Pupil Breaches of the Acceptable Use Policy**

J	**Recording and responding to incidents of misuse – flow chart**
K	**Cyberbullying: further advice and guidance**
L	**Online Safety in the Curriculum**
M	**Online Safety Training Needs Audit**

1. Introduction

This policy has been written by colleagues from Human Resources (HR) and the Education Improvement Service (EIS). It has been created to support school leaders in addressing whole-school issues in the use and application of new and emerging technologies across the school community. Shared ownership of this policy ensures both consistency of approach, and efficiency in relation to its ongoing review, update and/or revision to content.

Online safety is often defined as the safe and responsible use of technology. This includes the use of the internet and other means of communication using electronic media (e.g. text messages, WhatsApp, email, gaming devices etc.).

Online safety is not just about technology; it is also about people and their actions.

Technology provides unprecedented access to new educational opportunities, online collaboration, learning and communication. At the same time, it can provide the potential for staff and pupils to access material they shouldn't and/or be treated by others inappropriately.

The use of information and communication technology (ICT) is a vital part of the everyday functioning of and life in school. We also recognise the important role ICT plays in the lives of our children and their families.

Whilst there are many benefits and strengths in using ICT, there are also a number of risks to children's welfare and safety in school when using internet-enabled technology. These risks are summarised in the following four categories:

• Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.

• Contact: being subjected to harmful online interaction with other users; for example: peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

• Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.

• Commerce: risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Online safety is part of the wider duty of care of all those who work in schools: equipping children and young people to stay safe online, both in school and outside, is integral to the school's ICT curriculum. It may also be embedded in Personal Social and Health Education (PSHE) and Sex and Relationship Education (SRE) and include how pupils should report incidents (e.g. The Child Exploitation and Online Protection (CEOP) button, via a trusted adult, Childline etc)

General advice and resources for schools on internet safety are available at: https://www.saferinternet.org.uk/

In association with the appropriate **Acceptable Use Policy** Agreement (AUP), this policy forms part of the school's commitment to educate and protect all users when accessing digital technologies, both within and outside school. It should be read in conjunction with other relevant policies, such as the Safeguarding and Child Protection, Behaviour and Anti-Bullying policies.

In England, schools are subject to an increased level of scrutiny of their online safety practices by Ofsted Inspectors during inspections. Since 2015, there have been additional duties under the Counter Terrorism and Security Act 2015, known as the 'Prevent duty', which require schools to ensure that children are safe from terrorist and extremist material on the internet, to prevent people from being drawn into terrorism.

Ofsted School Inspection Handbook Schools will find reference to expectations in relation to protecting children online and offline throughout the Education inspection framework (EIF) – for use from 10 November 2025. Schools must ensure they meet the requirements set out in Keeping Children Safe in Education (KCSIE), which includes statutory guidance on online safety, filtering and monitoring.

This policy will be reviewed every year or more frequently in line with new developments in the use of the technologies, new threats to online safety or the level and/or nature of incidents reported.

2. Scope

This policy applies to all members of the school community, including staff, governors, Pupils, volunteers, parents, carers and visitors. This includes anyone who uses and/or has access to, personal devices and technologies whilst on school site and those who have access to, and are users of, school devices and technologies, both in and outside of the school.

This policy should be read in conjunction with:
Keeping Children Safe in Education (KCSIE)
Teaching Online Safety in Schools (DfE)
Relationships Education, Relationships and Sex Education (RSE) and Health Education statutory guidance (DfE)
The UK Council for Internet Safety (UKCIS) guidance
Searching, Screening and Confiscation: Advice for Schools (DfE)

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of Pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place outside of the school but are linked to membership of the school.

The school will, where it becomes known, inform parents/carers of any such incidents of inappropriate online behaviour that takes place out of school.

The 2011 Education Act increased these powers regarding the searching for electronic devices and the examination of any files or data (even where deleted), on such devices. In the case of both, action will be taken in line with the school's published Disciplinary Procedure and/or Relationship Policy - Promoting Positive Behaviours.

3. The Prevent Duty

Update (in force since 31 December 2023): Schools must have regard to the Home Office Prevent duty statutory guidance for England and Wales (2023). https://www.gov.uk/government/publications/prevent-duty-guidance. All staff must complete Prevent awareness training as part of their safeguarding induction and receive regular updates. The Designated Safeguarding Lead (DSL) must ensure that staff understand how to identify children who may be vulnerable to radicalisation and know the appropriate referral processes, including Channel.

As organisations seek to influence young people using social media and the internet, schools and childcare providers need to be aware of the increased risk of online radicalisation and the risks posed by the online activity of extremist and terrorist groups.

The Prevent duty is the duty under the Counter-Terrorism and Security Act 2015 on specified authorities (schools and childcare providers), in the exercise of their functions, to have due regard for the need to prevent people from being drawn into terrorism. The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools.

The general risks affecting children and young people may vary from area to area, and according to their age. Schools and childcare providers are required to identify risks within a given local context and identify children who may be at risk of radicalisation and know what to do to support them.

The Prevent duty requires school monitoring and filtering systems to be fit for purpose. The school has a filtering system in place, and its effectiveness is continuously monitored by Shropshire ICT Team.

The Prevent duty means that all staff have a duty to be vigilant, and where necessary, report concerns about internet use that includes, for example, the following:

- Internet searches for terms related to extremism
- Visits to extremist websites
- Use of social media to read or post extremist material
- Grooming of individuals

All staff should be aware of the Prevent Duty. All schools should have a Prevent Risk Assessment in place.

Government publications

Home Office | Prevent duty guidance

The Counterterrorism and Security Act 2015 contains a duty on schools, colleges, and other specified authorities, to have due regard to the need to prevent people from being drawn into terrorism. These authorities must have regard to the attached guidance when complying with the duty.

Home Office | Prevent Strategy

The Prevent Strategy contains three objectives: to respond to the ideological challenge of terrorism; to prevent people from being drawn into terrorism and ensure that they are given appropriate support; and to work with sectors and institutions where there may be risks of radicalisation that need to be addressed.

Home Office | Channel guidance

Channel is a programme which focuses on providing support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. This guidance has been issued under sections 36(7) and 38(6) of the Counter Terrorism and Security Act and sets out the duty on local authorities and partners of local panels (including schools) to provide support for people who are vulnerable to being drawn into any form of terrorism.

Department for education | Learning Together to Be Safe (pdf 1MB)
The DfE's Learning Together to Be Safe report presents the findings from a large-scale, in-depth research study into teaching methods – knowledge, skills, teaching practices and behaviours – that help to build resilience to extremism. The focus is on teaching methods to be used in a general classroom setting rather than as part of interventions targeted at those deemed at risk of extremism.

Reporting extremist content online
Everyone who uses the internet can help to make it safer. The Home Office hosts a dedicated webpage where you can report online content that you think might be illegal, or which you find offensive.

4. Governing Legislation
It is important to note that in general terms an action that is illegal if committed offline, is also illegal if committed online. The principle governing legislation is listed as follows:

- Computer Misuse Act 1990
- Data Protection Act 2018 &UK GDPR
- Freedom of Information Act 2000
- Communications Act 2003
- Malicious Communications Act 1988
- Regulation of Investigatory Powers 2000
- Copyright, Designs and Patents Act 1988
- Telecommunications Act 1984
- Criminal Justice & Public Order Act 1994
- Racial and Religious Hatred Act 2006
- Protection from Harassment Act 1997
- Protection of Children Act 1978
- Sexual Offences Act 2003
- Public Order Act 1986
- Obscene Publications Act 1959 and 1964
- Human Rights Act 1998
- The Education and Inspections Act 2006 & 2011
- The Protection of Freedoms Act 2012
- Serious Crime Act 2015
- Terrorism Act 2000
- Online Safety Act 2023
- Keeping Children Safe in Education (statutory guidance)

Schools must comply with the statutory guidance set out in Keeping Children Safe in Education (KCSIE), which includes specific requirements for:

- Filtering and monitoring systems
- Staff training on online safety
- Teaching pupils about online safety
- Responding to online safety incidents

- Managing allegations against staff involving online conduct

Further explanatory detail about governing legislation can be found in **Appendix G**.

5. Roles and Responsibilities

Online is seen as a 'whole school' responsibility with specific tasks and duties delegated as follows at each academy school:

Executive Headteacher	
Headteacher/ head of School	
Online Safety Lead	
IT lead	
Network Manager/Technician	Roartech
Governing Body/Board of Trustees	Paul Bunting

A full description of the responsibilities associated with these roles may be found in **Appendix F**.

6. Definitions: Devices & Technology

Due to the pace and change in the advent of digital technology, it is not possible to maintain an up-to date list of devices and technologies that may be relevant to this policy.

All individuals within the scope of this policy should apply reasonable judgement in determining what might constitute a device or a technology and should seek guidance and/or clarification from the Online Safety Lead should they be unsure.

Device (s)	Examples include but are not limited to: • Personal computers • Laptops • Tablets • Smart/Mobile Phones • Smart watches • Cameras • USB stick/flash drives
Technology(ies)	Examples include but are not limited to: • Internet search engines • AI e.g. ChatGPT, Gemini, CoPilot • Websites • Social media platforms, e.g. Facebook, X, Instagram, Snapchat, YouTube, TikTok etc • Real time communications e.g. texts, WhatsApp messages, chat rooms, email, instant messaging, Skype, Face Time, video chat • Online gaming e.g. Xbox, PlayStation

7. School, Staff, Governors and Volunteers

Acceptable Use Policy Agreements

Before being granted access to school devices and technologies, all members of the school community are required to read and sign an Acceptable Use Policy Agreement (AUP), appropriate to their role and status in the school.

The AUP for staff may be used and/or adapted for any user, to include governors and volunteers.

Acceptable Use Policy (AUP) for Staff

The AUP for staff can be found in Appendix A.

All staff must read and sign the 'Acceptable Use Policy Agreement for Staff' (AUP) before using any school IT resource. Variations of this agreement may be used to match the personal and professional roles of staff members.

A copy of the Staff AUP will be issued to all new members of staff during Induction. The school will also issue the AUP to staff, periodically, in response to the nature and/or volume of reported incidents, changes in legislation and emerging trends in online behaviour. It will also be issued to staff following any updates or amendments.

Access to online services and school devices will not be approved until new staff have signed and returned the Staff AUP.

All staff must:

- Complete online safety training as part of their induction, which includes understanding the school's filtering and monitoring systems, the risks posed to pupils online, and their responsibilities under KCSIE
- Receive regular updates on online safety issues and emerging risks
- Understand how to recognise and respond to online safety concerns, including those that may indicate a child is at risk of harm
- Know how to report concerns through the school's safeguarding procedures

Access may be suspended or restricted for serving staff who do not return an AUP issued on a periodic basis as requested.

Staff are required to accept the general principles of acceptable use of school devices and technologies each time they log in to a school device.

Online safety and the AUP are included in the statutory induction for all new staff and forms part of the contract of employment.

Acceptable Use of Devices and Technologies: Staff

Any device provided by the school, to or for staff or Pupils, is primarily intended to support the teaching and learning of Pupils. Discretion and the highest professional standards of conduct are expected of staff using school devices for personal use.

Where remote access to the school network via a personal device is approved by the Headteacher, staff confirm their acceptance of the terms set out in the Acceptable Use Policy in relation to that

device. Staff should seek clarification of any policy, procedure, terms and conditions they do not understand.

Staff breaches of the AUP

Where a staff member is found to be in breach of the Staff AUP, the matter will be dealt with in accordance with appropriate school policies such as the Disciplinary procedure, and /or with reference to external agency guidance.

8. Pupils

Acceptable Use Policy (AUP) for Pupils

The Pupil AUPs have been written to be relevant to and appropriate for different age groups, and can be found in **Appendices B C and D**.

A copy of the AUP will be shared with and signed by pupils at the start of every school year and when new pupils join. Pupils will not be given online access or allowed to use school devices before the AUP has been signed. This will be referred to at the start of any online lessons.

The Pupil AUP will form part of the first lesson of computing for each year group.

Pupil breaches of the AUP

Where a Pupil is found to have breached the AUP, this will be dealt with in line with the appropriate school policies, such as the Relational Policy -Promoting Positive Behaviour.

Examples of scenarios which may give rise to an online safety concern are set out in **Appendix I.**

Remedial action and sanctions are at the discretion of school leadership team. Outline guidance for teaching and leadership staff is set out in **Appendix J.**

9. Using non-School Equipment – 'Bring Your Own Device/Bring Your Own Technology' (BYOD/BYOT)

Under some circumstances, staff, governors and pupils can use their own devices in school and connect to the school network. This is normally referred to as 'Bring Your Own Device'/'Bring Your Own Technology' (BYOD/BYOT).

Regardless of the ownership of the device, the rules and expectations of online behaviour are as set out in the relevant AUP.

10. Security and passwords

Passwords should be changed regularly and must not be shared. The school system will inform users when the password is to be changed. In line with relevant Data Protection protocols and procedure, staff must always 'lock' a device (e.g. a classroom PC) if they are going to leave it unattended.

NB. The picture 'mute' or picture 'freeze' option on a projector will allow an image to remain on the screen and allow a PC to be 'locked'.

All users should be aware that the IT system is filtered and monitored Roartech and Lightspeed.

11. Data storage
Data across the trust is stored on Microsft Office platform.

Where USB pens are needed, only encrypted USB pens are to be used in school

For further clarification, please contact the Online Safety lead.

12. Mobile phones, cameras and other devices (Staff)
Members of staff will ensure that use of any mobile and smart technology, including personal phones and mobile devices, will take place in accordance with the law, as well as relevant trust/school policy and procedures, such as Safeguarding and Child Protection, Staff Code of Conduct and Acceptable Use Policies.

See mobile phone policy.

Staff are permitted to use their own personal phones or devices for contacting parents and carers, but they must block their number. Any pre-existing relationships or circumstance, which could compromise a staff member's ability to comply with this, should be discussed with the DSL and/or headteacher.

Where remote learning activities take place, staff will use equipment provided by the school. If this is not available, staff will only use personal devices with prior approval from the headteacher, following a formal risk assessment. Staff will follow clear guidance outlined in the Acceptable Use Policy.

If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence using a personal device or mobile phone, the police will be contacted, and the LADO (Local Authority Designated Officer) will be informed as part of our statutory duties under KCSIE.

All staff are required to adhere to the AUP which sets out the expected use of mobile phones and smart watches whilst on duty.

Staff should always use a school device to capture images and should not use their personal devices. Photos taken by the school are subject to the Data Protection Act 2018 &UK GDPR.

13. Social Media and Networking
The expectations around the use of social media are set out in the relevant AUP. For further detail, see the Social Media Policy.

14. Cyber bullying
Cyber bullying is defined as '*the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control over them*.'

All forms of bullying (including cyberbullying) should be handled as a community issue for the whole school. Every school must have measures in place to prevent all forms of bullying. These measures should be part of the school's Relational Policy - Promoting Positive Behaviour which must be communicated to all pupils, school staff, governors and parents.

14A: Sharing of Nude and Semi-Nude Images and Videos

The school follows the UK Council for Internet Safety (UKCIS) guidance 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'.

Definition: The term 'sharing nudes and semi-nudes' refers to the sending or posting of nude or semi-nude images, videos or live streams by young people under the age of 18 online. This is also known as 'youth produced sexual imagery' or 'sexting'. Creating and sharing sexual photos and videos of children under 18 is illegal.

This is a 'conduct' risk – online behaviour that increases the likelihood of, or causes, harm through the making, sending and receiving of explicit images.

If a pupil discloses that they have shared, or have been asked to share, a nude or semi-nude image, or if staff become aware of such an incident, they must:

- Report it immediately to the Designated Safeguarding Lead (DSL)
- Not view, copy, print, share, store, or save the imagery under any circumstances
- Not ask the pupil(s) to share the image(s) or video(s) with them or describe the content in detail
- Explain to the pupil that the incident will need to be reported to help keep them safe
- Not delete the imagery from the device it is held on (unless directed to do so by the DSL or police)
- Reassure the pupil that they are not in trouble and that they will be supported

The DSL will:

- Assess the incident using the UKCIS framework to determine whether it is 'experimental' or 'aggravated' in nature
- Consider the age, developmental stage, and vulnerability of all pupils involved
- Determine whether the incident can be managed internally or requires external referral to police and/or children's social care
- Inform parents/carers unless there is good reason not to (e.g., this would put the child at greater risk)
- Report to the police and/or children's social care if:
    - The image involves a child under 13
    - There is evidence of coercion, blackmail, grooming, or exploitation
    - The image shows sexual acts beyond that which is considered 'experimental' for the child's developmental stage
    - The image involves a young person at risk, or a vulnerable child
    - There is a significant age gap between those involved
    - There are concerns about capacity to consent
    - The image has been shared widely or published online
    - The situation involves an adult (over 18)
    - There are aggravating features such as threats, malicious intent, or links to other safeguarding concerns

Support will be provided to all pupils involved, including those who have shared images and those who have received them. This may include counselling, pastoral support, and education about the risks and consequences.

Parents/carers will be informed (unless doing so would put the child at greater risk) and supported to understand the incident and the school's response.

Sanctions may be applied in line with the school's Relational Policy - Promoting Positive Behaviour, but the primary focus will be on safeguarding and education rather than punishment.

All incidents will be recorded in the Online Incident Reporting Log (Appendix G)/and/or and reported to the Board of Trustees as appropriate.

14B: Peer-on-Peer Abuse Online

The school recognises that children can abuse their peers online. This can take many forms, including:

- Cyberbullying (covered in Section 14)
- Sharing of nude or semi-nude images (covered in Section 14A)
- Sexual harassment and sexual violence online
- Upskirting (taking photos under clothing without consent)
- Coercing others to engage in sexual activity online
- Initiation/hazing type activities online
- Creating or sharing AI-generated sexual images of peers

All peer-on-peer abuse is unacceptable and will be taken seriously. The school will follow the procedures set out in the Child Protection and Safeguarding Policy and will have regard to the DfE's guidance 'Sexual Violence and Sexual Harassment Between Children in Schools and Colleges' (2021, updated September 2024).

Staff must report all incidents of peer-on-peer abuse online to the DSL immediately. Even if the abuse occurred outside school hours or off school premises, if it involves members of the school community or has an impact on pupils' wellbeing or the school environment, the school will take action.

The DSL will:

- Assess the incident and determine the appropriate response
- Consider whether a referral to children's social care and/or police is required
- Ensure appropriate support is provided to all pupils involved
- Inform parents/carers unless there is good reason not to
- Record the incident and report to the Board of Trustees as appropriate

The school will take a contextual approach, considering the wider environmental factors that may be contributing to the abusive behaviour, and will work with external agencies where appropriate to address these.

Cyberbullying against staff

The DfE state that '*all employers, including employers of school staff in all settings, have statutory and common law duties to look after the physical and mental health of their employees. This includes seeking to protect staff from cyberbullying by pupils, parents and other members of staff, and supporting them if it happens*'.

Cyberbullying: Advice for headteachers and school staff is non-statutory advice from the Department for Education for headteachers and all school staff on how to protect themselves from cyberbullying and how to tackle it if it happens.

Please refer to **Appendix L** for further guidance and support in dealing with instances of cyberbullying against staff and/or Pupils.

15. Mental health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

16. Filtering and Monitoring

The school complies with the DfE's filtering and monitoring standards for schools and colleges. Our filtering and monitoring systems are designed to:

- Identify and block illegal content, including child sexual abuse images
- Filter content appropriate to the age and maturity of pupils
- Allow for differentiated filtering based on user groups (e.g., staff vs pupils)
- Monitor for safeguarding concerns and generate alerts
- Be regularly reviewed and updated

The school has appointed a senior leader with the responsibility for ensuring filtering and monitoring systems are effective and appropriate. This person works with the DSL, IT service provider, and a governor to:

- Review filtering and monitoring reports regularly (at least termly)
- Respond to alerts and breaches
- Ensure systems are updated to reflect emerging risks
- Conduct an annual review of the effectiveness of the systems

The filtering and monitoring provision is reviewed (at least annually) by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider. The IT Service Provider and Online Safety Lead will meet annually in line with policy and/or if there are required changes or updates to policy or systems.

Checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or BYOD or new technology is introduced e.g. using SWGfL Test Filtering.

Filtering

- Each school manages access to content across its systems for all users and on all devices using the school's internet provision. The filtering provided meets 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.
- There is a clear process in place to deal with, and log, requests/approvals for filtering changes (see Appendix for more details).

- Filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- The school has differentiated user-level filtering for example staff and learners.
- Younger learners will use child friendly/age-appropriate search engines e.g. SWGfL Swiggle.
- The school has a mobile phone policy and where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.
- If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.
- SLT will use the DfE "Plan technology for your school" self-assessment to evidence compliance and get tailored recommendations. https://www.gov.uk/guidance/plan-technology-for-your-school
- Policy and procedures will align with DfE "Filtering and monitoring: core standard" and be reviewed at least annually, documenting roles, change control and regular log reviews. https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-core-standard

Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- The school 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 school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems using the appropriate blend of strategies informed by the school's risk assessment. These may include:
    - Physical monitoring (adult supervision in the classroom).
    - internet use is logged, regularly monitored and reviewed.
    - filtering logs are regularly analysed, and breaches are reported to senior leaders.
    - pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
    - where possible, school technical staff regularly monitor and record the activity of users on the school technical systems.
    - use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s).
- Use the DfE "Plan technology for your school" service to baseline cyber posture and track improvements. https://www.gov.uk/guidance/plan-technology-for-your-school
- Align with DfE "Cyber security: core standard" (governance, user account control with MFA where available, secure configuration, patching, anti-malware, backups, incident response) https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges

Online Safety Audit

Online Safety Self-Review Tool for Schools will be completed annually using the 360 degree safe audit.

360 degree safe is intended to help schools review their online safety policy and practice. The review takes you through each aspect of online safety, helping you to collaborate, report and progress. This will then be reviewed against actions at least termly.

17. Cyber Security

The school recognises that cyber security is a critical aspect of online safety and safeguarding. We comply with the DfE's cyber security standards for schools and colleges, which include:

- Governance: Clear accountability for cyber security at senior leadership and governance level
- User access control: Robust password policies and multi-factor authentication where possible
- Secure configuration: All devices and systems are configured securely
- Patching: Regular updates and patches are applied to all systems
- Anti-malware: Up-to-date anti-malware protection on all devices
- Backups: Regular backups following the 3-2-1 rule (3 copies, 2 different media, 1 off-site)
- Incident response: Clear procedures for responding to cyber incidents

Cyber security is the safe and responsible use of information and communication technology. It is not just about keeping information safe and secure, but also about being responsible with that information, being respectful of other people online, and practising good 'netiquette' (internet etiquette). All staff and governors who have access to the systems must complete Cyber Security training annually. Failure to do so can result in access being closed down.

The DfE Cyber Security Standards for Schools

- Protect all devices on every network with a properly configured boundary or software firewall.
- Network devices should be known and recorded with their security features enabled, correctly configured and kept up to date.
- Using the security features that devices already have is the most basic form of cyber security.
- Ensure filtering/monitoring arrangements explicitly cover AI chat and image tools across school-owned and BYOD devices used on the school network.
- When procuring or enabling AI tools, check against DfE "Generative AI: product safety standards/expectations" (latest update January 2026), and ensure no personal/sensitive data is entered into AI tools unless a DPIA and contracts allow. https://www.gov.uk/government/publications/generative-ai-product-safety-standards
- Follow DfE policy paper "Generative AI in education" (2025) for safe, effective and responsible use; include staff training and local risk assessments. https://www.gov.uk/government/publications/generative-artificial-intelligence-in-education
- Accounts should only have the access they require to perform their role and should be authenticated to access data and services.
- Successful cyber-attacks target user accounts with the widest access and highest privileges on a network.
- Maintain up-to-date anti-malware and anti-virus software to reduce the risk from many forms of cyber-attack.
- All online devices and software must be licensed for use and should be patched with the latest security updates.
- At least 3 backup copies of important data, on at least 2 devices, at least one must be off-site. Train all staff with access to school IT networks in the basics of cyber security.

18. Generative artificial intelligence (AI)

The school follows the DfE's guidance on generative AI in education (2025), which includes:

- Conducting risk assessments before introducing AI tools
- Ensuring filtering and monitoring systems cover AI chat and image tools
- Providing staff training on the safe and effective use of AI
- Teaching pupils about AI, including its benefits, risks, and limitations
- Ensuring no personal or sensitive data is entered into AI tools unless a Data Protection Impact Assessment (DPIA) has been completed and contracts permit
- Checking AI tools against the DfE's generative AI product safety standards

The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.
The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.
The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.
The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.
The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

19. Staff Reporting of Online Incidents and Concerns

The school takes the reports of incidents and concerns extremely seriously. Any subsequent action or remedy to be taken following the investigation of an incident or concern, will depend on its nature, situational and circumstantial factors.

All incidents that come to the attention of school staff should be notified to the DSLs via the school's reporting mechanism set out in **Appendix K**, or, where applicable, via the **Whistleblowing Policy.**

Any incident that raises child protection or wider safeguarding questions must also be communicated to the Designated Safeguarding Lead(s) immediately.

Incidents that are of a concern under the Prevent duty should be referred to the Executive Head/ Head of School and/or Designated Safeguarding Lead, immediately.

Incidents which are not child protection issues but may require SLT intervention (e.g. cyberbullying) should be reported to SLT, immediately.

Examples of potential online safety concerns may be found at **Appendix I**.

Response to Online Safety Incidents

When an online safety incident occurs, the school will:

1. Assess whether the incident constitutes a safeguarding concern - if yes, follow the Child Protection and Safeguarding Policy immediately
2. Preserve evidence (e.g., screenshots, URLs, messages, device logs) - do not delete or remove content until advised by the DSL or police
3. Secure any devices involved - prevent further access or deletion of evidence
4. Determine the appropriate response, which may include:
    - Internal investigation and sanctions
    - Referral to the DSL for safeguarding assessment

    - Reporting to police (for illegal content or criminal offences)
    - Reporting to CEOP (for online child sexual exploitation and abuse)
    - Reporting to the platform/service provider
    - Notification to parents/carers
5. Provide support to affected pupils, including counselling, pastoral care, and safety planning
6. Review the incident to identify lessons learned and any necessary policy or practice changes
7. Record the incident in the Online Incident Reporting Log (Appendix G)
8. Report to the Board of Trustees as appropriate, particularly for serious incidents

The DSL will determine whether an incident requires external referral based on the nature and severity of the incident, the age and vulnerability of those involved, and whether there are safeguarding concerns.

20. Staff training and updates

All staff must have online safety training as part of their safeguarding induction, which is in line with KCSIE. This training must include:

- The school's online safety policy and acceptable use agreements
- The risks posed to children online, including from peer-on-peer abuse
- How to recognise signs that a child may be at risk online
- The school's filtering and monitoring systems and how they work
- How to respond to and report online safety concerns
- The latest guidance on online safety issues

Staff must receive regular updates (at least annually) on online safety, including emerging risks and changes to guidance. The DSL must maintain records of staff training.

21. Communicating the Online Safety Policy

Staff and the Online Safety policy

- All staff will be given a copy of the Online Safety Policy during statutory induction and its importance explained.
- An **Acceptable Use Policy** Agreement is signed before access to school devices and systems is approved and the agreement forms part of the contract of employment.
- Staff are made aware that internet traffic can be monitored and traced to an individual user, including on personal devices where network access has been granted. Because of this, discretion and professional conduct are always essential.

Introducing the Online Safety policy to Pupils

- The **Acceptable Use Policy** Agreement is referred to on a regular basis. The aim is to make the policy familiar and accessible to all pupils at all times.
- Pupils are made aware that network and Internet use is monitored.

Home-School Communications of Online Safety information.

- The school website provides information on online safety and how the school can help to support and guide their child.
- Online safety advice is included as a regular feature in newsletters and as part of the ongoing dialogue between home and school. Knowsley newsletters are sent home once a month to parents.

Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects: Relationships and Health Education, PSHE, Computing and Safer Internet Day. Online safety teaching is always appropriate to pupils' age and developmental stages. The risks covered are in Appendix L.

22. Shropshire Safeguarding Contact Details

Local Authority Designated officer (LADO) lado@shropshire.gov.uk
Emergency Duty Team 0345 6789040 or 01743 249544 (out of hours only)

23. Monitor and Review

This policy will be monitored continuously. It must be reviewed at least annually and/or more frequently in line with new developments in the use of technologies, new threats to online safety, changes to statutory guidance (including KCSIE), or the level and/or nature of incidents. The board of trustees will approve the policy and receive regular reports on online safety, including filtering and monitoring effectiveness, incidents, and training compliance.

Appendix A - AUP for Staff, Governors & Volunteers

All members of staff, including governors and visitors, are expected to use school IT devices and systems in a professional, lawful, and ethical manner. To ensure that members of staff understand and comply with their professional responsibilities when using technology, and to support staff in providing appropriate curriculum opportunities for children, they are asked to read and sign the **Acceptable Use of Technology Policy** (AUP) for Staff.

The AUP for Staff sets out the reasonable expectations of the safe and responsible use of information and communication technologies and the management of the potential risks posed by inappropriate use. The AUP is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally, however the AUP serves to ensure that school systems are protected from any accidental or deliberate misuse which could put the safety and security of school systems or members of the community at risk.

General Principles

1. I understand that I have personal and legal responsibilities, including treating others with dignity and respect, acting honestly, using public funds and school equipment appropriately, adhering to health and safety guidelines and safeguarding children, always having regard to national and local education guidance and the law.

2. I understand that this AUP applies to my use of the technology, systems and services provided to me or accessed as part of my role within the school, in both a professional and personal capacity. This may include use of laptops, mobile phones, all electronic devices with imaging and sharing capabilities, tablets, digital cameras, and email as well as IT networks, data and data storage, remote learning and online and offline communication technologies.

3. I am aware that this AUP does not provide an exhaustive list, but I understand that the Acceptable Use of Technology Policy (AUP) for Staff should be read and followed in line with the following key policies:

    - KCSIE child protection and online safety guidance
    - Staff Code of Conduct
    - remote learning policy

If a member of staff breaches our policy, action will be taken in line with our staff code of conduct.

Use of school devices and systems

4. I will only use the equipment and internet services provided to me by the school, for example desktops, laptops, tablets, mobile phones, and internet access, when working with children.

5. I understand that any equipment and internet services provided by my workplace is intended for education purposes and/or professional use and should only be accessed by members of staff. Reasonable/occasional personal use of the school's IT systems and/or devices by staff is allowed, as this is considered beneficial to the development of staff IT skills and can enable staff to maintain a positive work-life balance. However, this is at the school's discretion and can be revoked at any time.

6. Where I deliver or support remote/online learning, I will comply with the school's AUP and the Remote Learning Policy.

Data and system security

7. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access to that device.
   I will use a 'strong' password to access school systems and create and update my password as directed by Shropshire ICT or more frequently, as required.
   - I will take all reasonable steps and measures to protect the devices in my care from unauthorised access or theft.
   - I will not disclose my password or security information to others.
   - Where required, I will use 2-factor authentication.

8. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the digital lead.

9. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from Shropshire IT and the computing lead.

10. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with the school's information security policies.

    - All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
    - Any data being removed from school site, such as via email or on memory sticks, CDs etc will be suitably protected. This may include data being encrypted by a method approved by the school.

11. I will not keep documents which contain school-related, sensitive or personal information, including images, files, videos, and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the school's network to upload any work documents and files in a password protected environment.

12. I will not store any personal information on the school's IT system, including school laptops or any such or similar device issued to members of staff, which is unrelated to school activities. This includes personal photographs, files and personal financial information.

13. I will not attempt to bypass any filtering and/or security systems put in place by the school and will ensure that school-owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences:
    - to gain unauthorised access to computer material
    - to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

14. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the Computing Lead as soon as possible.
15. If I lose any school-related documents or files, I will report this to the Headteacher (who will report it to the Central Services Team) and school's Data Protection Officer (DPO), as soon as possible.

I understand that any images or videos of children may only be used for the purposes agreed with school leaders and as set out in the relevant policies. I understand images of children must always be appropriate and should only be taken with equipment provided by the school. I understand that images of children should only be taken and/or published where the explicit consent of parents/carers has been given.

Online safety in the classroom

17. I will promote online safety with the children in my care and will help them to develop a responsible attitude to safe, online system use and to the content they access or create by:
    - exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used.
    - creating a safe environment where children feel comfortable to report and voice concerns, without fear of getting into trouble and/or being judged for talking about something which happened to them online.
    - involving the Designated Safeguarding Lead (DSL) or deputy DSLs as part of planning online safety lessons or activities to ensure support is in place for any children who may be impacted by the content.
    - make informed decisions to ensure any online safety resources used with children is appropriate.
18. I will report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the DSL in line with the school's Safeguarding and Child Protection/Online Safety policies.
19. I will observe and adhere to copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, or distribute or use them.

Mobile devices and smart technology

20. I will ensure that my use of mobile devices and smart technology is compatible with my professional role, does not interfere with my work duties and takes place in line with the Staff Code of Conduct and the law.
21. Where it is agreed that I use my own mobile device (e.g. laptop / tablet / mobile phone / USB device) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
22. My phone number can only be shared with SLT approval otherwise, I will keep my personal phone numbers private and will only use my own mobile phone, or other device, to contact pupils or parents in a professional capacity, after I have blocked my personal number.
23. I will keep my mobile phone and Smart Watch secure whilst on school premises. It will be switched off or on silent with notification disabled whilst I am on duty unless there are good reasons that have been approved in consultation with a member of the senior leadership team, and then that is discreet and appropriate, e.g. not in the presence of the children.

24. I will keep mobile devices switched off or on silent with notification disabled and left in a safe place during lesson times. I understand that the school cannot take responsibility for personal items that are lost or stolen.
25. I will report any text or images sent to me by colleagues or pupils which could be viewed as inappropriate. I will not use a personal device to photograph a pupil(s), except with the written permission of the Executive Head / Head teacher/ Head of School.
26. I will not use personal email addresses on the school ICT systems.
27. I will not open any hyperlinks in emails or any attachments to emails if I have any concerns about the validity of the email or its source is neither known nor trusted.
28. I will, when I take and/or publish images of others, do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use any personal devices to record these images, unless I have written permission from the Executive Head / Headteacher/Head of School. Where these images are approved by the school to be published (e.g. on the school website) it will not be possible to identify by name, or any other personal information, those who are featured.
29. I will not attempt to upload, download or access any material which is illegal (for example, images of child sexual abuse, criminally racist material, adult pornography), inappropriate or may cause harm or distress to others. I will not attempt to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
30. I will not (unless I have permission) make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

Online communication, including use of social media.

31. I will ensure that my use of communication technology, including use of social media is compatible with my professional role, does not interfere with my work duties and takes place in line with the Safeguarding and Child Protection, Online Safety policy, Staff Code of Conduct and the law.
32. As outlined in the Safeguarding and Child Protection, Online Safety policy, Staff Code of Conduct Policy:
    - I will communicate with others in a professional manner, I will not use aggressive or inappropriate language, and I appreciate that others may have different opinions.
    - I will not engage in any online activity, at, or outside school, which may compromise my professional responsibilities. This includes making offensive, aggressive or defamatory comments, disclosing confidential or business-sensitive information, or information or images that could compromise the security of the school.
    - I will use social networking sites responsibly, taking care to ensure that appropriate privacy settings are in place, and ensure that neither my personal nor professional reputation, nor the school's reputation, is compromised by inappropriate postings, to include past postings.
    - I will take appropriate steps to protect myself and my reputation, and the reputation of the school when using communication technology, including the use of social media.
    - I will not discuss or share data or information relating to children, staff, school or parents/carers on social media.
    - I will never send or accept a 'friend request' made through social media from a Pupil at school. I understand that such requests should be raised formally as an incident.
    - I will not, under any circumstances, make reference to any staff member, Pupil, parent or school activity/event via personal social media or other communication technologies.

- I will not use the school's name, logo, or any other published material without written prior permission from the Executive Headteacher. This applies to any published material, online or in print.
- I will not post any communication or images which links the school to any form of illegal conduct, or which may damage the reputation of the school.

33. My electronic communications with current and past children and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.
    - I will ensure that all electronic communications take place in a professional manner via school approved communication channels and systems, such as a school email address, user account or telephone number. Any such communication will be professional in tone and manner. At no time will I use or share a personal email address, phone number or social networking site for such communication purposes.
    - I will not share any personal contact information or details with children, such as my personal email address or phone number.
    - I will not add or accept friend requests or communications on personal social media with current or past children and/or their parents/carers.
    - I will notify the Headteacher of any current or future, direct or incidental contact with Pupils, parents or carers, for example where parents or carers are part of the same social group.
    - If I am approached online by a current or past children or parents/carers, I will not respond and will report the communication to the Executive Head/ Headteacher/Head of School, Designated Safeguarding Lead (DSL).
    - Any pre-existing relationships or situations that compromise my ability to comply with the AUP or other relevant policies will be discussed with the Headteacher.

Professional conduct

If I have any queries or questions regarding safe and professional practise online, either in school or off site, I will raise them with the Headteacher.

34. I understand that the school may exercise its right to monitor the use of its information systems, including internet access and the interception of messages/emails on our systems, to monitor policy compliance and to ensure the safety of children and staff. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.
35. I understand that if the school believes that unauthorised and/or inappropriate use of school systems or devices is taking place, the school may invoke its disciplinary procedures as outlined in the Staff Code of Conduct.
36. I understand that if the school believes that unprofessional or inappropriate online activity, including behaviour which could bring the school into disrepute, is taking place online, the school may invoke its disciplinary procedures as outlined in the Staff Code of Conduct.
37. I will not upload, download, or access any materials which are illegal, such as inappropriate images of children, criminally racist material or adult pornography covered by the Obscene Publications Act.
38. I will not attempt to access, create, transmit, display, publish or forward any material or content online that may be harmful, inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.

39. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school into disrepute.
40. I will report and record any concerns about the welfare, safety or behaviour of children or parents/carers online to the DSL in line with the school's child protection policy.
41. I will report concerns about the welfare, safety, or behaviour of staff online to the Headteacher, in line with school's allegations against staff policy.
42. I understand that if the school suspects criminal offences have occurred, the police will be informed.

Use of AI

I **may** use AI tools for:

43. Drafting emails, documents, reports, and summaries.
44. Generating ideas, outlines, or templates.
45. Administrative tasks such as scheduling help, formatting, or rewriting text.
46. Data analysis with approved AI tools.
47. Learning, training, and research.

*I **must not** use AI tools for:*

❌ Confidential or Sensitive Data

- Uploading personal data (names, addresses, health information).
- Uploading confidential corporate documents.
- Uploading internal financial or HR information.

❌ Decision-Making Without Human Oversight

- Making final decisions affecting staff, customers, finances, safeguarding, or legal matters.
- Using AI outputs as sole evidence.

❌ Unethical or harmful purposes

- Generating discriminatory, harmful, or offensive content.
- Attempting to bypass security controls or manipulate systems.
- Creating misleading or deceptive content (deepfakes, false statements, fake images).

❌ Unapproved AI Tools

- Using personal AI accounts for work-related content.
- Installing unapproved AI apps, browser extensions, or plugins.

Transparency Requirements

When AI meaningfully contributes to work, I must disclose its use in line with organisational expectations. Examples include:

- Adding an internal note such as: 'This document was drafted with assistance from AI'
- Informing managers when AI is used in analytic or high-impact tasks.

I understand that in the event of any query or concern about this Agreement, I should contact the Online Safety Lead or Headteacher.

I have read, understood and agreed to comply with this Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of staff member: ……

Signed: ……

Date: (DD/MM/YYYY) ……

Appendix B - AUP for learners in KS1

- I want to feel safe all the time.
- I know that anything I do on the computer can be seen by other people.
- I know when to use the CEOP report button.

I agree that I will:

	not use my own mobile phone, or any other device, in school, unless I am given permission.
	always keep my passwords safe and not share them with anyone.
	talk to my teacher before using anything on the internet and only open web pages which my teacher has said are OK.
	only work with people I know in real life.
	tell my teacher if anything makes me feel scared or unhappy on the internet.
	make sure all messages I send are polite.
	show my teacher if I get a nasty message.
	not reply to any nasty message or anything which makes me feel sad or worried.
	not give my mobile phone number to anyone who is not a friend in real life.
	only email people I know or if my teacher agrees using my school email.
	not tell people about myself online (I will not tell them my name, anything about my home, my family or my pets).
	only use AI with an adult

Appendix C - AUP for learners in KS2

When I am using the computer or other technologies, I want to feel safe all the time.

- I am aware of the CEOP report button and know when to use it.
- I know that anything I share online may be monitored by school.
- I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

I agree that I will:

- always keep my passwords safe and not share them with anyone.
- only use, move and share personal data securely.
- only visit sites which are appropriate.
- work in collaboration only with people my school has approved, and I will deny access to others.
- respect the school network security.
- make sure all messages I send are respectful.
- show a responsible adult any content that makes me feel unsafe, worried or uncomfortable.
- not reply to any nasty message or anything which makes me feel unhappy or worried.
- not use my own mobile phone, or any other device, in school, unless I am given permission.
- only give my mobile phone number to friends I know and trust in real life.
- only email people I know or are approved by my school.
- only use email which has been provided by school.
- obtain permission from a teacher before I order online.
- discuss and agree my use of a social networking site with a responsible adult before creating a profile or signing up for an account.
- always follow the terms and conditions when using a website
- always keep my personal details private. (My name, family information, journey to school, my pets and hobbies are all examples of personal details.)
- always check with a responsible adult before I share images of myself or others.
- only create and share content that is legal and that I have consent to share.
- never meet an online friend without taking a responsible adult that I know with me.
- tell my teacher if a site I tried to visit is blocked.
- Use AI responsibly, showing school values and behaviours.

Signed _____ *Date* _____

Appendix D– Sample Home-school Online Safety Agreement: ICT, Mobile Phones, Personal Photographs and Social Media

Child's Name	
Child's class teacher/form name	
Parent/Carer/Guardian's name	

Use of School ICT Equipment and Internet Access

As the parent or legal guardian of the above-named Pupil, I give permission for my child to access the Internet, the Virtual Learning Environment, school email and other ICT facilities, whilst at school. I understand that my child has signed an Acceptable Use Policy (AUP) confirming their understanding and acceptance of the proper use of school and personal ICT equipment. I also understand that my child may be informed, should the rules change or be updated, during the year.

I accept that ultimately, the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent them from accessing inappropriate materials. These steps include the school using a filtered internet service, providing secure access to email, employing appropriate teaching practice and teaching online skills to Pupils, across the curriculum.

I understand that the school can monitor my child's computer files and the Internet sites they visit. I also understand that the school may contact me if there are concerns about my child's online behaviour or safety. I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns about my child's online safety.

Mobile Phones and other Personal Devices

I understand that my child must be given permission by the school to have their mobile phone and any other personal device in school and that it should be switched off and handed into the class teacher. This includes during off-site activities. If my child breaks this rule, I understand that the phone or device will be confiscated and I will be asked to collect it in person, at the end of the school day.

I understand that 'Smart' watches/any other device that takes photographs or goes on the internet must treated the same as a mobile phone and handed in to the class teacher.

Personal Photographs and Social Media

I am aware that the school permits parents/carers to take photographs and videos of their own children at school events but requests that where the photos/videos contain images of other children, these are not shared on any social networking site such as Facebook, WhatsApp or Instagram etc. I will support the school's approach to online safety and will not post, upload or add any text, image or video that could upset, offend or threaten the safety of any member of the school community.

Signature of Parent/Carer/Guardian: _____

Date: _____

Appendix E: Online Role & Responsibilities – List of Duties

Executive Headteacher/Headteacher/Head of School	• Has overall responsibility for online safety provision. • Has overall responsibility for data and data security • Ensures that the school uses an appropriate filtered Internet Service - Lightspeed • Ensures that staff receive appropriate training to enable them to carry out their online safety roles. • Can direct the whole school community including staff, pupil sand governors to information, policies and practice about online safety. • Is aware of the procedures to be followed in the event of a serious online safety incident. • Receives regular monitoring reports from the filtering and monitoring provider, Lightspeed, when applicable. • Ensures that there is a system in place to monitor and support staff who carry out internal online safety procedures and reviews (e.g. Network Manager). • Oversees the administration of the staff Acceptable Use Policy Agreements and takes appropriate action where staff are found to be in breach.
Online Safety Coordinator /Designated Safeguarding Lead/ lead teacher of ICT	• Takes day to day responsibility for online safety issues and assumes a leading role in establishing and reviewing the Online policies and supporting documents. • Ensures that the school is compliant with all statutory requirements in relation to the handling and storage of information. • Ensures that any recording, processing, or transfer of personal data is carried out in accordance with the *Data Protection Act 2018 & UK GDPR.* • Promotes an awareness of and commitment to online safety throughout the school community. • Ensures that online safety is embedded across the curriculum. • Is the main point of contact for pupils, staff, volunteers and parents who have online safety concerns beyond what can be managed at a class teacher level. • Ensures that staff and pupils are regularly updated on online safety issues and legislation, and are aware of the potential for serious child protection issues that arise from (for example): ➢ sharing of personal data ➢ access to illegal/inappropriate materials ➢ inappropriate on-line contact with adults/strangers ➢ cyber-bullying • Ensures all staff are aware of the procedures that need to be followed in the event of an online safety incident. • Ensures that an online safety incident log is kept up to date. • Liaises with school IT technical staff where necessary and/or appropriate. • Facilitates training and provides advice and guidance to all staff.

	• Communicates regularly with SLT to discuss current issues, review incident logs and filtering. • Liaises with key people to complete the annual online safety audit (360 Safe) conducted annually and with reviews at least termly and in line with relevant actions. • Liaises with key people to complete DFE Plan Technology, ensuring actions are assigned to key personnel. • Runs monthly checks using Lightspeed and actions and trends in searches and informs the headteacher of any AUP breaches, logging accordingly.
Head of ICT/Lead teacher for ICT/Computing Lead	• Oversees the delivery of the online safety element of the Computing curriculum. • Communicates regularly with the Online Safety Coordinator.
Network Manager / Technician	• Oversees the security of the school ICT system. • Ensures that appropriate mechanisms are in place to detect misuse and malicious attack (e.g. firewalls and antivirus software). • Ensures that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • Ensures that the school's policy on web-filtering is applied and updated on a regular basis. • Ensures that access controls/encryption exist to protect personal and sensitive information held on school-owned devices. • Ensures that users may only access the school networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed. • Reports any online safety incidents or concerns, to the Online Safety Co-ordinator. • Keeps up to date with the school's Online Safety policy and technical information to carry out the online safety role effectively and to inform and update others as relevant. • Keeps up-to-date documentation of the school's online security and technical procedures. • Keeps an up-to-date record of those granted access to school systems.
All Staff	• Read, understand and help promote the school's online safety policies, procedures and guidance. • Are aware of online safety issues relating to the use of any digital technology, monitor their use, and implement school policies regarding devices. • Report any suspected misuse or problem to the Online Safety Coordinator. • Maintain an awareness of current online safety issues and guidance, e. g. through training and CPD. • Model safe, responsible and professional behaviours in their own use of technology. • Ensure that any digital communications with pupils are on a professional level and through school-based systems ONLY.

	• Ensure that no communication with Pupils, parents or carers is entered into through personal devices or social media. • Ensure that all data about pupils and families is handled and stored in line with the principles outlined in the Staff AUP.
Teaching Staff	• Embed online learning into all areas of the curriculum and other school activities. • Supervise and guide pupils carefully when engaged in learning activities involving online technology (including extracurricular and extended school activities – where relevant). • Ensure that pupils are fully aware of how to research safely online and potential legal issues relating to electronic content such as copyright laws.
Pupils	• Are responsible for using the school digital technology systems in accordance with the Pupil AUP Agreement. • Have a good understanding of research skills, the need to avoid plagiarism and to uphold copyright regulations. • Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. • Understand policies on the use of mobile devices and digital cameras, the taking and use of images and cyber-bullying. • Understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions, in and out of school, if related to their membership of the school.
Parents/Carers	Parents and carers are encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of: • digital and video images taken at school events. • access to parents' sections of the website and Arbor. • their children's personal devices in the school – parents must provide a written request.
External Groups	Any external visitors to school must read and sign an acceptable use policy prior to using any equipment or accessing the school network.

Appendix F: Legislation - Overview of relevant legislation governing online safety.

Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance have 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 HR and/or legal advice is sought in the event of an online incident or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

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

Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR)

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 personal data must be:

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

Freedom of Information Act 2000

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

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.

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, or that of others. 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 person having 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 to releasing it, a criminal offence.

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/ 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.

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-onlin

https://www.gov.uk/guidance/what-academies-free-schools-and-colleges-should-publish-onlin

Serious Crime Act 2015 Introduced the new offence of sexual communication with a child. Also created new offences and orders around gang crime (including Child Sexual Exploitation (CSE)).

Appendix G: *Online Incident Reporting Log*

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

Appendix H: Examples of potential online safety concerns (Pupils)

The following are provided by way of guidance and are in no way limiting or exhaustive. You should seek advice from the Online Safety Coordinator if you are unsure about what might constitute a concern.

Inappropriate material accessed on school computers

Due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer even when filtering is in place and users abide by the rules.

Pupils are taught that they are not at fault if they see or come across something online that they find worrying or upsetting and are encouraged to alert staff to any inappropriate content. The staff member should report the incident to the Online Safety Co-ordinator who will log the problem and liaise with Shropshire ICT to make any necessary adjustment to filter settings.

Abusive messages on school computers

Pupils who receive abusive messages over school systems will be supported and advised not to delete messages. The Online Safety Co-ordinator will be informed and a formal process of investigation initiated.

Parent/Carer/Guardian reports of cyber bullying

Parents, carers and guardians may become aware that their child is concerned or upset by bullying, originating in the school but continuing via electronic means. Parents and carers should know that the school encourages them and/or pupils to approach them for help, either via a staff member or directly to the Head. Such incidents will be investigated and dealt with in accordance with the school Behaviour and Anti-Bullying policies.

Pupil disclosure of concerns or abuse

All staff receive Safeguarding and online safety training as part of their induction, and thereafter on a regular basis. Where a Pupil discloses a concern to a member of school staff, this is passed on to the Designated Safeguarding Lead and, where appropriate, the Online Safety Coordinator.

Pupil reporting outside school

Pupils are taught that if something worries them, or if they think a situation is getting out of hand, that they should share this with a trusted adult such as their parents, carers, guardians or school staff. The curriculum will cover how pupils should report incidents (e.g. CEOP button, trusted adult, Childline).

Allegations against staff

Allegations involving staff should ordinarily be reported to the Headteacher or through the Whistleblowing Policy. If the allegation is one of abuse, then it should be handled in line with the statutory DfE guidance: 'Dealing with allegations of abuse against teachers and other staff'. If necessary local authority's LADO should be informed. Evidence of incidents must be preserved and retained and where necessary, the LADO informed.

Appendix I: How to Manage Pupil Breaches of the Acceptable Use Policy

Where a Pupil is found to have breached the AUP, this will be dealt with in line with the appropriate school policies, such as the Behaviour policy.

Remedial action relating to potential sanctions is at the discretion of school management as suggested as below.

Level 1 breaches

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other devices/technologies) in lessons, e.g. to send texts to friends
- Use of unauthorised instant messaging/social networking sites

Possible Sanctions: refer to class teacher / Online Safety Coordinator/ confiscation of phone or other device.

Level 2 breaches

- Continued use of non-educational sites during lessons after being warned.
- Continued unauthorised use of email after being warned.
- Continued unauthorised use of mobile phone (or other devices/technologies) after being warned.
- Continued use of unauthorised instant messaging/social networking sites.
- Use of Filesharing software
- Accidentally corrupting or destroying others' data without notifying a member of staff.
- Accidentally accessing offensive material and not notifying a member of staff.

Possible Sanctions: refer to Class teacher/ Online Safety Coordinator / removal of Internet access rights for a period / confiscation of phone or device / contact with parents/carers.

Level 3 breaches

- Deliberately corrupting or destroying someone's data, violating the privacy of others.
- Sending an email and/or message that is regarded as harassment or of a bullying nature (cyberbullying)
- Deliberately trying to access offensive or pornographic material.

Possible Sanctions: refer to Class teacher / Online Safety Coordinator / Executive Head, Head of School / removal of Internet rights for a period / contact with parents/carers.

Other safeguarding actions

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site
2. Inform the LA as appropriate

Level 4 breaches

- Continued sending of emails and/or messages regraded ad harassment or of a bullying nature after being warned (cyber-bullying)
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revises 1988.
- Bringing the school's name into disrepute
- Using AI to generate images without consent and guidance

Possible Sanctions: Referred to Executive Headteacher/Headteacher/Head of School/Contact with parents/possible exclusion/refer to community police officer/LA online safety officer.

Other Safeguarding Actions:

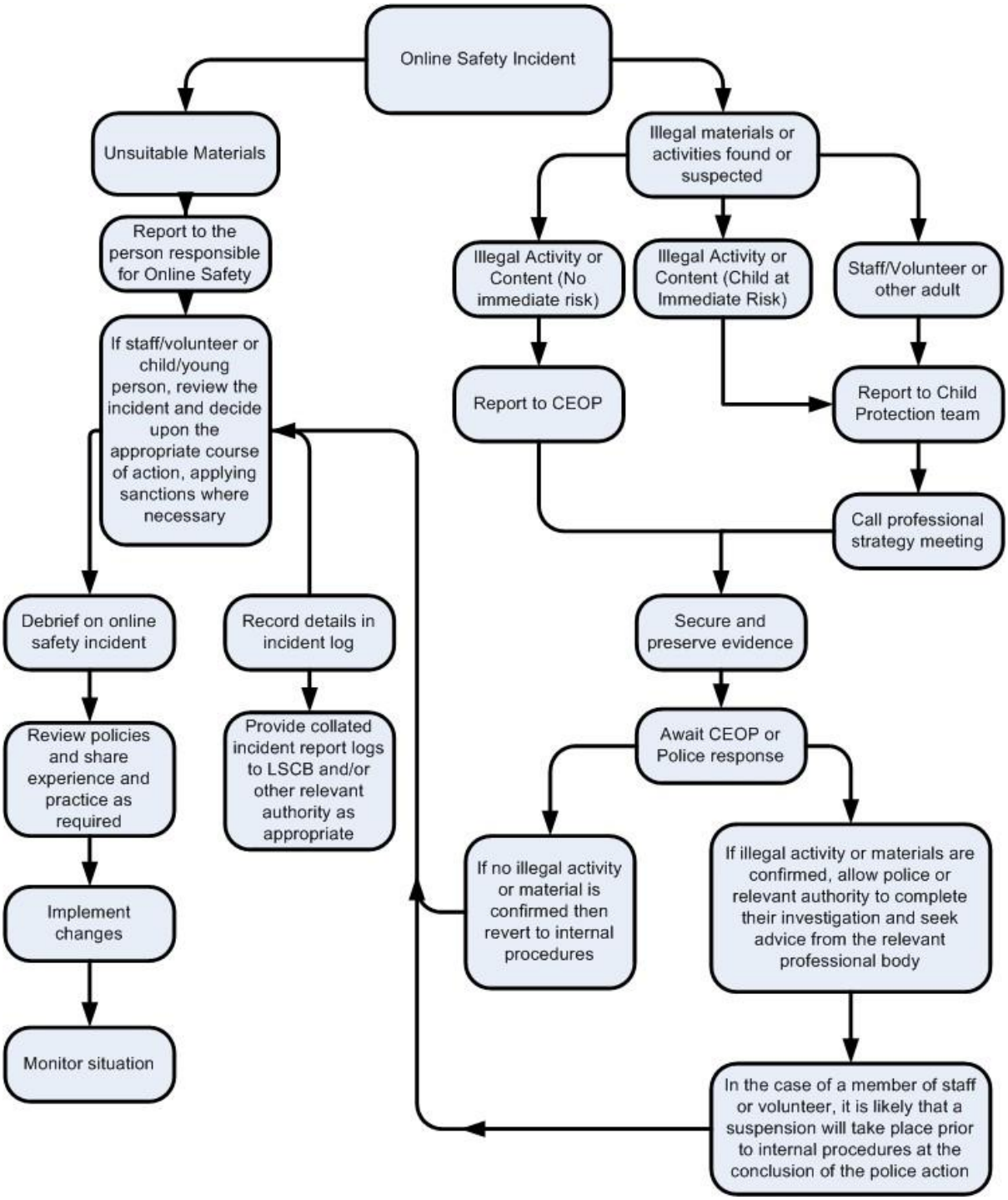
1. Secure and preserve any evidence

2. Inform the sender's e-mail service provider if a system other than the school systems used.

Pupils are also informed that sanctions can be applied to online incidents that take place out of school if they are related to school or any member of its community.

Schools are likely to involve external support agencies as part of these technical support service to investigate equipment and collect data evidence and/or the Local Authority Human Resources.

Appendix J: Recording and responding to incidents of misuse – flow chart



Appendix K: Cyberbullying: further advice and guidance

Behaviour that is classed as cyber bullying includes but is not limited to:

- **Abusive comments**, rumours, gossip and threats made over the internet or using digital communications – this includes internet trolling.
- **Sharing pictures**, videos or personal information without the consent of the owner and with the intent to cause harm and/or humiliation.
- **Hacking** into someone's email, phone or online profiles to extract and share personal information, or to send abusive or inappropriate content whilst posing as that person.
- **Creating specific websites or 'pages' on the Internet** that negatively target an individual or group, typically by posting content that intends to humiliate, ostracise and/or threaten.
- **Blackmail** or pressurising someone to do something online they do not want to do such as sending a sexually explicit image.

Cyberbullying: Advice for headteachers and school staff

The Department for Education has produced non-statutory advice for headteachers and all school staff on how to protect themselves from cyberbullying and how to tackle it if it happens.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Preventing and tackling bullying: Advice for headteachers, staff and governing bodies

This document has been produced by the Department for Education to help schools take action to prevent and respond to bullying as part of their overall behaviour policy. It outlines, in one place, the Government's approach to bullying, legal obligations and the powers schools have to tackle bullying, and the principles which underpin the most effective anti-bullying strategies in schools. It also lists further resources through which school staff can access specialist information on the specific issues that they face. This includes cyberbullying.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/623895/Preventing_and_tackling_bullying_advice.pdf

Appendix L Online Safety in the Curriculum

Pupils will be taught about online safety as part of the curriculum

Each school complies with its statutory duties to teach online safety as part of:

- Relationships Education (primary)
- Health Education (primary)
- Computing (all phases)

Online safety is also embedded across the curriculum where relevant, including in PSHE.

In **Key Stage (KS) 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Be discerning in evaluating digital content

By the **end of primary school**, pupils will know:

- That the internet can be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health
- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data are shared and used online
- How to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

- The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- Why social media, computer games and online gaming have age restrictions and how to manage common difficulties encountered online
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- Where and how to report concerns and get support with issues online
- The safe use of social media and the internet will also be covered in other subjects where relevant.

Each school uses age-appropriate resources and teaching methods to ensure pupils understand:

- How to report concerns using the CEOP 'Report Remove' tool and other reporting mechanisms
- The concept of consent in relation to sharing images and information online
- How algorithms and targeted content work
- The risks associated with live streaming and sharing location data
- How to critically evaluate online content, including recognising misinformation and disinformation

Pupils will be taught practical cyber security skills

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack

Pupils will also receive age-appropriate education on safeguarding issues such as cyberbullying and the risks of online radicalisation.

APPENDIX M -ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	