Schools HR Policy & Procedure Handbook

St Thomas & St Anne's Primary School

KCSiE: Model Online Safety Policy (Whole School)

This Policy has been **shared with** the following professional associations and Trade Unions representing Teachers, Headteachers and Support Staff:

- National Education Union
- National Association of Schoolmasters Union of Women Teachers
- National Association of Headteachers
- Association of School and College Leaders
- Unison
- GMB

This policy has been adopted by the governing body

In

November 2023

and will be ordinarily reviewed every year

CONTENTS

Appendices

Shropshire HR – (HR)

Shirehall
Abbey Foregate
Shrewsbury
Shropshire
SY2 6ND
shropshirehr@shropshire.gov.uk

EIS – Education Improvement Service

Shirehall
Abbey Foregate
Shrewsbury
Shropshire
SY2 6ND
jane.parsons@shropshire.gov.uk /
emma.harding-safeguarding@shropshire.gov.uk

Online Safety Policy

1. Introduction

This policy has been produced by Shropshire HR in consultation with colleagues from 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, in line with expectations of behaviour set out in Shropshire HR's **KCSiE: Code of Conduct for Staff Working in Schools 2023/24** and associated statutory guidance.

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.

Online safety and the school or setting's approach to it should be reflected in the **Child Protection Policy** which, amongst other things, should include **appropriate filtering and monitoring** on school devices and school networks.

The school has a filtering and monitoring system in place and its effectiveness is continuously monitored by Amy Taylor (School Business Manager) and Hannah McGrath (Headteacher).

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 students to access material they shouldn't and/or be treated by others inappropriately.

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 students 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 Child Protection/ Safeguarding, 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.

Schools will find reference to the statutory expectations in relation to protecting children online and offline in Keeping Children Safe in Education 2023. Schools should also refer to the Ofsted School Inspection Handbook, updated July 2022 and which came into force on 1 September 2023.

This policy will be reviewed annually and/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.

The Online Safety Policy is a statutory element of staff induction.

2. Scope

This policy applies to all members of St Thomas & St Anne's community, including staff, governors, students, 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.

School Staff

All staff should receive appropriate safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring – see **KCSiE 2023, para 141** for further information) at induction. The training should be regularly updated.

In addition, all staff should receive safeguarding and child protection (including online safety) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively.

Shropshire Council's **Schools and Early Years Settings Safeguarding Training Statement** is accessible via the SLG here.

Students

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students 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 Behaviour Policy.

The school will keep a record of all staff and students who are granted Internet access. The record will be kept up-to-date and reflect changes or amendments such as a member of staff who has left the school or a student whose access has been withdrawn.

3. The Prevent Duty

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 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.

Prevent and schools - guidance, key legislation, campaigns and links

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.

NaCTSO | Crowded Places Guidance
Although not strictly Prevent, the above document gives guidance on the increasing protection of crowded places from a terrorist attack.

REsilience Gateway | REC Gateway guide (pdf)
REsilience Gateway documents are designed to provide information to an individual school or teacher on a specific issue or concern. The linked document signposts answers to some of the key questions that pupils need to engage with in preparation for understanding the complexity of religious and theological contentious issues.

Each Gateway has been revised and approved by the Department for Education.

Reporting extremism poster July 2015 (gif)

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 1998
- 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
- The Education and Inspections Act 2011
- The Protection of Freedoms Act 2012
- The Schools Information Regulations 2012
- Serious Crime Act 2015
- Terrorism Act 2000

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

5. Roles & Responsibilities

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

Headteacher	Hannah McGrath head@hanwood.shropshire.sch.uk
School Business Manager	Amy Taylor sbm@hanwood.shropshire.sch.uk
ICT Technicians	James Ritch and Mike Foden Ict.support@mmat.co.uk

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 judgment in determining what might constitute a device or a technology and should seek guidance and/or clarification from the Headteacher should they be unsure.

Device(s)	Examples include but are not limited to: • Personal computers

	• Laptops • Tablets • 'Smart'/Mobile phones • 'Smart' watches • Cameras • USB sticks/flash drives
Technology(ies)	Examples include but are not limited to: • Internet search engines • Websites • Social media platforms, e.g., Facebook, Twitter, Instagram, Snapchat, YouTube, TikTok etc • Real time communications e.g., texts, WhatsApp messages, chat rooms, email, instant messaging, Skype, FaceTime, 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 school.

The AUP for staff has been created by Shropshire HR. 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/or emerging trends in online behaviour.

Access to online services and school devices will not be approved until new staff have signed and returned the Staff AUP. Access may be suspended or restricted for serving staff who do not return an AUP issued on a periodic basis.

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 students, is primarily intended to support the teaching and learning of students. 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. Students

Acceptable Use Policy (AUP) for Students
The student AUPs have been created by the Education Improvement Service (EIS). They 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 student AUP should be sent to parents/carers with a covering letter at the start of the academic year, and to those of new students when they enrol. Students will not be given online access or allowed to use school devices before the AUP has been signed and returned to the school office.

The student AUP will form part of the first lesson of ICT for each year group.

Acceptable Use of Devices and Technologies: Students

Student breaches of the AUP

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

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 management. 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)

In some circumstances, staff, governors and students 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 also allow a PC to be 'locked'.

All users should be aware that the ICT system is filtered and monitored by the school.

The school has a filtering and monitoring system in place and its effectiveness is continuously monitored by Amy Taylor (School Business Manager).

11. Data storage

Only encrypted USB pens are to be used in school. For further clarification, please contact Hannah McGrath, Headteacher.

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 school policy and procedures, such as confidentiality, child protection, data protection, staff code of conduct and Acceptable Use Policies.

Staff are required to:

- keep mobile phones and personal devices in a safe and secure place, such as a locked drawer/cupboard or in the staff room, during lesson time.
- keep personal mobile phones and devices switched off or set to 'silent' mode during lesson times.
- ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times.
- not use personal devices during teaching periods unless written permission has been given by the headteacher, such as in emergency circumstances.

- ensure that any content bought onto site via personal mobile phones and devices is compatible with their professional role and the school's behaviour expectations.

Staff will only use equipment provided by the school (i.e. not personal devices):

- to take photos or videos of children/pupils/students in line with the school's image use policy.
- to work directly with children/pupils/students during lessons/educational activities.
- to communicate with parents/carers.

Staff are not permitted to use their own personal phones or devices for contacting children/pupils/students or parents and carers. Any pre-existing relationships or circumstance, which could compromise a staff member's ability to comply with this, should be discussed with the Designated Safeguarding Lead (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 2023.

The school's policy relating to the use of devices such as mobile phones, is set out in the relevant AUP.

Mobile phones, cameras and other devices (Students)

Student devices such as mobile phones, should be switched off and handed in to the school office.

If a member of staff suspects that a mobile phone has been misused within the school, then it should be confiscated and the matter dealt with in line with normal school procedure and/or the Behaviour policy.

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

Staff should always use a school camera to capture images and should not use their personal devices.

Photos taken by the school are subject to the GDPR and all other relevant data protection legislation.

13. Social Media and Networking

The expectations around the use of social media are set out in the relevant AUP.

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 behaviour policy which must be communicated to all pupils, school staff, governors and parents.

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 students.

15. 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 Headteacher via the school 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 Headteacher 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 the SLT, immediately.

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

16. Staff training and updates

All staff have online safety training included as part of their safeguarding induction to the school and receive regular training in the safeguarding students. Online is included as part of this.

Online incidents and concerns are a standing item at staff briefings.

17. 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 essential at all times.

Introducing the Online Safety policy to students

- The Online Safety Policy/**Acceptable Use Policy** Agreement is/are posted in all classrooms, as appropriate, and its content referred to on a regular basis. The aim is to make the policy familiar and accessible to all students at all times.
- Students are made aware that network and Internet use is monitored.

Home-School Communication 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.
- The school holds online safety events to brief parents and carers about online safety developments and policies; (possibly) as part of events such as 'Safer Internet Day'/event.

Shropshire Safeguarding Contact details:

Local Authority Designated Officer (LADO)	lado@shropshire.gov.uk
Emergency Duty Team	0345 678 9040
01743 249544 (Out of hours only)	

18. Monitor & review

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

Appendix A - AUP for Staff {Governors & Volunteers}* *include or delete as appropriate*

All members of staff* 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 [pupils/students/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, at all times 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, tablets, digital cameras, and school email accounts 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: [include any specific policies/amend/delete as appropriate]

    - KCSiE child protection and online safety guidance
    - staff expectations of behaviour policy/professional Code of Conduct
    - remote/online learning AUP

    If a member of staff breaches our policy, action will be taken in line with our staff behaviour policy/code of conduct and allegations policy. [add to/amend as appropriate]

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, email accounts and internet access

in the course of my professional duties and job description, such as when working directly with children or in a support capacity as part of the wider school workforce.
Where staff use of personal devices is permitted, clear boundaries and expectations should be detailed. School leaders should make informed, risk-assessed decisions and be able to evidence the rationale for their approach.

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 personal use of the school's IT systems and/or devices by staff is/is not allowed.

   Amend as appropriate; if the setting allows staff to use work internet access/devices for personal use, clear boundaries should be detailed. Occasional personal use of the settings devices could be considered as beneficial to the development of staff IT skills and can enable staff to maintain a positive work-life balance. However, this is at the setting'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 that relates to remote/online learning AUP.

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 [name], [job title] or more frequently, as required.
   - I will take all reasonable steps and measured to protect the devices in my care from unauthorised access or theft.
   - I will not disclose my password or security information to others.

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 [IT manager] / [name], [job title].

9. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the [job title, eg IT manager.]

10. I will ensure that any personal data relating to staff, governors and pupils is kept in accordance with the Data Protection legislation, including GDPR and 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 as directed by [name], [job title].

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 learning platform to upload any work documents and files in a password protected environment or school VPN. [Amend as appropriate.]

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, that 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 [ICT Support Provider/Team/lead] [named contact] as soon as possible.

15. If I lose any school-related documents or files, I will report this to the [ICT Support Provider/Team/lead], [named contact] and school's Data Protection Officer, [named contact] as soon as possible.

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

Online safety in the classroom

17. I will promote online safety with the children/pupils/students 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/pupils/students 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) [name] or a deputy [name] as part of planning online safety lessons or activities to ensure support is in place for any children/pupils/students who may be impacted by the content.
    - make informed decisions to ensure any online safety resources used with children/pupils/students is appropriate.

18. I will report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the Designated Safeguarding Lead (DSL) in line with the school's child protection/online safety policy.

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 behaviour policy/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. I will keep my personal phone numbers private and not use my own mobile phone, or other device, to contact students or parents in a professional capacity.

23. I will keep my mobile phone secure whilst on school premises. It will be switched off 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 students.

24. I will keep mobile devices switched off 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 students which could be viewed as inappropriate. I will not use a personal device to photograph a student(s), except with the written permission of the [Headteacher.]

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 [Headteacher]. 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 child protection/online safety policy, staff behaviour policy/code of conduct, social media policy and the law. [Amend as appropriate.]

32. As outlined in the staff behaviour policy/code of conduct and school/setting social media policy: [Amend as appropriate.]

    - 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, that 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/pupils/students, staff, school or parents/carers on social media.
- I will never send or accept a 'friend request' made through social media from a student at school. I understand that such requests should be raised formally as an incident with the Designated Safeguarding Lead (DSL) and/or [Headteacher].
- I will not, under any circumstances, make reference to any staff member, student, 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 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/pupils/students 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/pupils/students, 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/pupils/students and/or their parents/carers.
    - I will notify the Headteacher of any current or future, direct or incidental contact with students, 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/pupils/students or parents/carers, I will not respond and will report the communication to my line manager and [name], 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 Designated Safeguarding Lead (DSL) and/or headteacher/manager. [Amend as appropriate.]

Professional conduct

34. 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 Designated Safeguarding Lead (DSL) and/or the headteacher/manager.

35. 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/pupils/students and staff. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

36. 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 behaviour policy/code of conduct.

37. 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 behaviour policy/code of conduct.

38. 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.

39. 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.

40. 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.

41. I will report and record any concerns about the welfare, safety or behaviour of children/pupils/students or parents/carers online to the Designated Safeguarding Lead (DSL) in line with the school's child protection policy.

42. I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher/manager, in line with school's protection policy and/or the allegations against staff policy. [Amend as appropriate.]

43. I understand that if the school suspects criminal offences have occurred, the police will be informed.

44. I understand that in the event of any query or concern about this Agreement, I should contact [name], [job title].

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:
……

Appendix B - AUP for learners in KS1

{The school must detail the acceptable use of ALL devices and technologies as relevant to their setting. The following wording has been provided by way of suggested acceptable use but can be amended as applicable.}

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
- 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
- only use my school email
- talk to my teacher before using anything on the internet
- not tell people about myself online (I will not tell them my name, anything about my home, my family or my pets)
- not upload photographs of myself without asking a teacher
- never agree to meet a stranger

Signed _____ ***Date*** _____

Appendix C - AUP for learners in KS2

{The school must detail the acceptable use of ALL devices and technologies as relevant to their setting. The following wording has been provided by way of suggested acceptable use but can be amended as applicable.}

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 websites 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
- never meet an online friend without taking a responsible adult that I know with me

Signed _____ ***Date*** _____

Appendix D - AUP for learners in KS3 and above

{The school must detail the acceptable use of ALL devices and technologies as relevant to their setting. The following wording has been provided by way of suggested acceptable use but can be amended as applicable.}

The policy aims to ensure that any communications technology is used without creating unnecessary risk to others.

I agree that I will:

- respect the school network security
- set strong passwords which I will not share
- only use, move and share personal data securely
- not use my own mobile phone, or any other device, in school, unless I am given
- permission
- only visit websites which are appropriate
- always follow the terms and conditions when using a website
- respect copyright and the intellectual property rights of others
- only create and share content that is legal
- discuss and agree my use of a social networking site with a responsible adult before joining
- not access social networking sites whilst at school
- obtain permission from a teacher before I order online
- only use approved email accounts
- only use appropriate content which I have permission to use
- only communicate online with trusted users
- never meet an online friend without taking a responsible adult that I know with me
- make sure all messages/posts I send are respectful
- not respond to or forward any inappropriate message or content
- be cautious when sharing personal contact information
- only communicate electronically with people I know or have been approved by my school
- report unsuitable content or activities to a member of staff

I know that anything I share online at school via the school network may be monitored by the 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 am aware of the CEOP Report button and know when to use it.

I agree that I will not:

- act in a way that might breach the school Behaviour Policy
- forward chain letters
- breach copyright law
- do anything which exposes others to harm or danger
- visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
  - inappropriate images
  - promoting discrimination of any kind
  - promoting violence or bullying
  - promoting racial or religious hatred
  - promoting illegal acts

I accept that my use of both school and personal devices may be monitored and reported on.

Signed _____ ***Date*** _____

page 2 of 2

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

Student Name	
Student'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 student, 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 students safe and to prevent them from accessing inappropriate materials. These steps include the school using a filtered and monitored internet service, providing secure access to email, employing appropriate teaching practice and teaching online skills to students, 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 unless my child is given permission by a teacher, their mobile phone and any other personal device should be switched off and kept out of sight during the school day. 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/[list other specific devices] must not be brought to school under any circumstances. [Add to/Amend as appropriate, in line with setting's BYOD policy.]

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. 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.

Name/Signature of Parent/Carer/Guardian:

Date:

Appendix F: Online Roles & Responsibilities - List of duties [settings should add to/amend, as appropriate]

Headteacher/Principal	• 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 • Ensures that staff receive appropriate training to enable them to carry out their online safety roles • Can direct the whole school community including staff, students and 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 Online Safety Coordinator/Officer. • 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/CPO/HEAD/LEAD TEACHER of ICT	• Takes day to day responsibility for online safety issues and assumes a leading role in establishing and reviewing the school 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 GDPR and other data protection legislation. • 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 students, staff, volunteers and parents who have online safety concerns. • Ensures that staff and students 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 that 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.

Head of ICT/Lead teacher for ICT	• 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 monitoring and 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 in order 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 with regard to 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 students are on a professional level and through school-based systems ONLY. • Ensure that no communication with students, parents or carers is entered into through personal devices or social media. • Ensure that all data about students and families is handled and stored in line with the principles outlined in the Staff AUP.
Teaching Staff	• Embed online safety issues in all aspects of the curriculum and other school activities. • Supervise and guide students carefully when engaged in learning activities involving online technology (including extracurricular and extended school activities, where relevant). • Ensure that students are fully aware of how to research safely online and of potential legal issues relating to electronic content such as copyright laws.
Students / Students:	• Are responsible for using the school digital technology systems in accordance with the Student 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/ Learning Platform and on-line student/student records. • their children's personal devices in the school. (where this is allowed)
External groups	Any external individual/organisation must sign an Acceptable Use Policy prior to using any equipment or the Internet within the school.

Appendix G: 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 has been produced. It is important to note that in general terms, an action that is illegal if committed offline is also illegal if committed online.

It is recommended that 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 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that 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 students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for 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-online

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 H: *Online Incident Reporting Log* *[sample template]*

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

Appendix I: Examples of potential online safety concerns (Students)

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.

Students 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 the Network Manager to make any necessary adjustment to filter settings.

Abusive messages on school computers

Students 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 students 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/academy Behaviour/Bullying policy.

Student 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 student 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.

Student reporting outside school

Students 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.

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.

The curriculum will cover how students should report incidents (e.g., CEOP button, trusted adult, Childline)

Appendix J: How to Manage Student Breaches of the Acceptable Use Policy

Where a student 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.

The following are provided as exemplification only, and should be amended and/or confirmed by the school, as appropriate:

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 / Headteacher / 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 regarded as harassment or of a bullying nature after being warned (cyberbullying)
- 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, revised 1988
- Bringing the school name into disrepute

[Possible Sanctions – Referred to Head Teacher / Contact with parents / possible exclusion / refer to Community Police Officer / LA online safety officer]

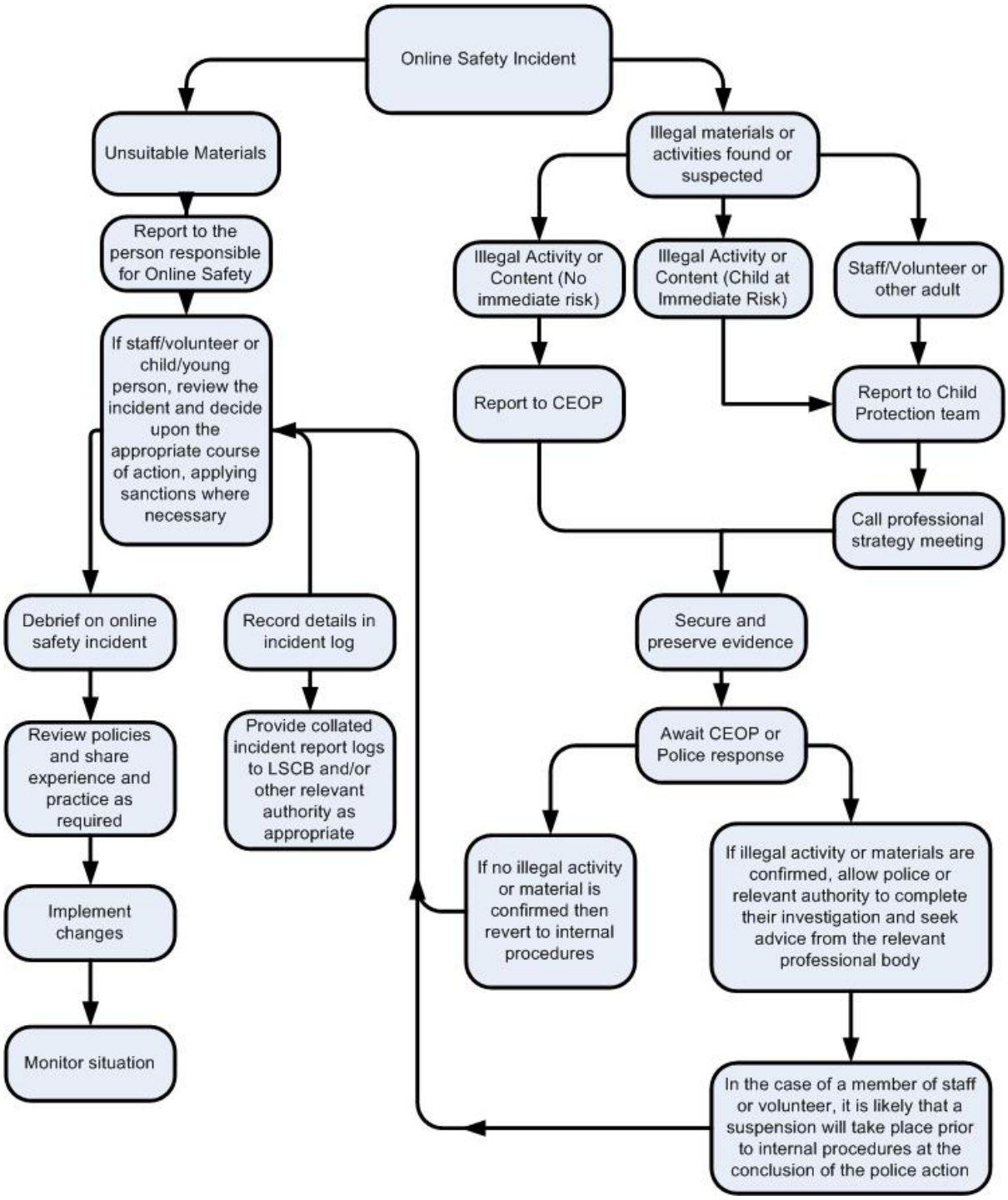
Other safeguarding actions:

1. Secure and preserve any evidence
2. Inform the sender's e-mail service provider if a system other than the school system is 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 investigations e.g., an ICT technical support service to investigate equipment and collect data evidence and/or the Local Authority Human Resources team.

Appendix K: Recording and Responding to incidents of misuse – flow chart



Appendix L: 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