Schools HR Policy & Procedure Handbook

KCSiE 2026: Online Safety Policy

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

- Association of School and College Leaders (ASCL)
- GMB
- National Association of Headteachers (NAHT)
- National Association of Schoolmasters Union of Women Teachers (NASUWT)
- National Education Union (NEU)
- Unison

This policy has been adopted by the governing body of the Blue Hills Federation

On

Headteacher	Kathryn Jones (1st Sept 26-31st Dec 26) Chris McKeon (from 1st January 2027)	head@bhf.shropshire.sch.uk
Chair of Governors	Mrs Di Cosgrove	Cosgrove.d@bhf.shropshire.sch.uk
HR Advisor	Mr Mathew Edwards	Mathew.edwards@shropshire.gov.uk
The Governing Body made this policy available to all staff who were notified that the policy could be viewed via GovernorHub		25.09.26

CONTENTS		Page
1.	Introduction • *Filtering and Monitoring*	4
2.	Scope • *School Staff* • *Students*	5
3.	The Prevent Duty	5
4.	Governing Legislation	9
5.	Roles & Responsibilities	7
6.	Definitions: Devices & Technology	8
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 Staff AUP: Appendix A	9 18
8.	Students • OVERVIEW Acceptable Use Policy (AUP) for Students • OVERVIEW Acceptable Use of Devices and Technologies: Students • Student breaches of the AUP **KS1 AUP: Appendix B** **KS2 AUP: Appendix C** **KS3 and above AUP: Appendix D**	10
9.	Using non-School Equipment – 'Bring Your Own Device/Bring Your Own Technology' (BYOD/BYOT)	11
10.	Filtering and Monitoring, Security and Passwords	11
11.	Data storage	11
12.	Mobile phones, cameras and other devices (Staff) • Mobile phones, cameras and other devices (Students)	12 13
13.	Social Media & Networking	13
14.	Cyber bullying • Cyberbullying against staff	13
15.	Staff Reporting of Online Incidents and Concerns	14
16.	Staff training and updates	14
17.	Communicating the Online Safety Policy	14
18.	Staff Training, Procedure Monitoring and Review	15

Appendices

Please refer to the appropriate document owner for further information or detail.

Shropshire HR – (HR)

shropshirehr@shropshire.gov.uk

EIS – Education Improvement Service

Safeguarding Team Information and Services | Shropshire Learning Gateway

	Title	Owner	Page
A	AUP for staff	HR	18
B	AUP for learners in KS1	EIS	19
C	AUP for learners in KS2	EIS	20
D	AUP for Visitors	EIS	
E	Sample Home-school Online Safety Agreement; ICT, Mobile Phones, Personal Photographs and Social Media	EIS	
F	Online Roles & Responsibilities: List of duties	HR	
G	Legislation - Overview of relevant legislation governing online safety	HR	
H	Online Incident Reporting Log	EIS	
I	Examples of potential online concerns (Students)	EIS	
J	How to Manage Student Breaches of the Acceptable Use Policy	EIS	
K	Recording and Responding to incidents of misuse – flow chart	HR/EIS	
L	Cyberbullying: further advice and guidance	HR/EIS	

Online Safety Policy

1. Introduction

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

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 2026**, **Keeping Children Safe in Education 2026** 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 is reflected in the **Child Protection Policy** which, amongst other things, should include **appropriate filtering and monitoring** on school devices and school networks. This includes consideration of online risks arising from mobile and smart technology, cloud-based platforms, apps, artificial intelligence, AI-generated content, deepfakes, synthetic media and other emerging technologies.

Filtering and Monitoring

The school has appropriate filtering and monitoring systems in place. The effectiveness of these systems will be reviewed at least once every academic year by the senior leader responsible for filtering and monitoring, with support from the **Designated Safeguarding Lead** and **IT support** or the school's managed service provider. The review will consider all relevant internet-connected devices and locations, including school-owned devices used off site where applicable, and will include consideration of mobile apps, cloud services, encrypted traffic where relevant, user identification, AI-generated content and other dynamic or personalised online content. Records of checks, issues identified and actions taken will be retained.

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 2026. The school complies with the requirements of the following statutory guidance:

- DfE's digital and technology standards, including filtering and monitoring standards
- Mobile phones in schools
- Data protection in schools and any current local safeguarding partnership or trust requirements.

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.

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)	

2. Scope

This policy applies to all members of the school community, including staff, governors, students, volunteers, parents, carers, 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.

Artificial intelligence (AI), including generative AI tools, AI chatbots, image generation tools, deepfake technology, synthetic media and AI-enabled apps, will be treated as technologies within the scope of this policy.

The school has a separate **AI in Schools Policy** covering wider governance, curriculum, assessment, data protection, procurement, staff use and pupil use. This Online Safety Policy should be read alongside that policy.

School Staff

All staff should receive appropriate safeguarding and child protection training, including online safety and an understanding of expectations, applicable roles and responsibilities in relation to filtering and monitoring. This should be consistent with Keeping Children Safe in Education 2026. All staff should read **Part One of KCSiE 2026** in full, including staff who do not work directly with children, unless updated statutory guidance provides otherwise.

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.

Details of Shropshire Council's **Safeguarding Team Information and Services** are available 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 document, **Teaching approaches that help to build resilience to extremism among young people** 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.

Teaching approaches that help to build resilience to extremism among young people

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

The school will identify a senior leader with responsibility for filtering and monitoring. This role will work with the **Designated Safeguarding Lead** and **IT support** or the managed service provider to ensure that filtering and monitoring arrangements are understood, checked, reviewed, recorded and escalated where safeguarding concerns or technical gaps are identified.

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

Executive Headteacher	Kathryn Jones (1st Sept 26-31st Dec 26) Chris McKeon (from 1st January 2027) head@bhf.shropshire.sch.uk
Governor responsible for this policy and its effectiveness in and across the school Di Cosgrove: Safeguarding Governor	Mrs D Cosgrove Cosgrove.d@bhf.shropshire.sch.uk
Online Safety Co-ordinator *Deputy Headteacher*	Kathryn Jones Jones.k@bhf.shropshire.sch.uk
Lead teacher for ICT	Fay McGlynn Mcglynn.f@bhf.shropshire.sch.uk
Network Manager/Technician	Shropshire ICT support ictsupport@shropshire.gov.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 Mrs Kathryn Jones should they be unsure.

Device(s)	Examples include but are not limited to: • Personal computers • Laptops • Tablets • 'Smart'/Mobile phones • 'Smart' watches • 'Smart' eyewear such as 'Meta glasses' • 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, 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

Staff must not use unauthorised AI tools to process, upload, summarise or generate content from personal data, special category data, safeguarding information, SEND information, pupil assessment data, staff information, photographs, video, voice recordings or any other identifiable information. Any use of AI tools for school purposes must be approved by the school and must comply with data protection, safeguarding, copyright, assessment and acceptable use requirements.

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 is also available to download on the school website.

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

Acceptable Use of Devices and Technologies: Students

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

Student breaches of the AUP

Where a student uses AI tools, AI-generated content, deepfakes, image manipulation or impersonation technology in a way that may breach this policy, the AUP, the **Behaviour Policy**, the **Child Protection Policy** or the law, the matter will be managed through the school's safeguarding, behaviour and online safety procedures. This may include incidents involving bullying, harassment, image-based abuse, non-consensual image creation or sharing, impersonation, academic misconduct, misinformation or unsafe sharing of personal information.

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. Filtering and Monitoring, Security and Passwords

The school has appropriate filtering and monitoring systems in place. All users should be aware that the ICT system is filtered and monitored by the schools ICT services provider.

The effectiveness of these systems will be reviewed at least once every academic year by the senior leader responsible for filtering and monitoring, with support from the **Designated Safeguarding Lead** and **IT support** or the school's managed service provider.

The review will consider all relevant internet-connected devices and locations, including school-owned devices used off site where applicable, and will include consideration of mobile apps, cloud services, encrypted traffic where relevant, user identification, AI-generated content and other dynamic or personalised online content. Records of checks, issues identified and actions taken will be retained.

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'.

The school has a filtering and monitoring system in place and its effectiveness is continuously monitored by *Kathryn Jones, Deputy Headteacher.*

11. Data storage

Only encrypted USB pens are to be used in school. For further clarification, please contact *Kathryn Jones.*

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 security, staff behaviour/code of conduct and Acceptable Use Policies.

Staff are advised to:

- keep mobile phones and personal devices in a safe and secure place 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 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 pupils in line with the school's image use policy.
- to work directly with pupils during lessons/educational activities.
- to communicate with parents/carers.

Staff are not permitted to use their own personal phones or devices for contacting pupils 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 the 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 **Keeping Children Safe in Education 2026.**

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)

The school will implement a mobile phone and smart technology policy that prohibits pupil use of mobile phones and other communication or smart technology with similar functionality throughout the school day, including during lessons, movement between lessons, breaktimes and lunchtimes, except where a specific exception has been authorised. The policy should be aligned with the Behaviour Policy and should make clear how devices are stored, how exceptions are managed, how breaches are addressed and how expectations are communicated to pupils and parents/carers.

Confiscated phones can be collected by parents/carers at the end of the school day.

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.

Mobile phones, cameras and other devices (Staff)
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 schools Lead Teacher 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.

AI-related incidents or concerns must also be reported through the school's safeguarding or online safety reporting routes. This includes harmful AI-generated content, deepfakes, synthetic images or audio, impersonation, AI-facilitated bullying or harassment, inappropriate use of AI chatbots, the uploading of personal or safeguarding information into unauthorised AI tools, and any concern that AI has been used to create, alter, share or threaten to share images or information about a pupil, member of staff or other person.

Incidents that are of a concern under the Prevent duty should be referred to the Executive 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 and updates. Staff training includes information and details of current and updated school practice and procedure relating to safeguarding expectations, filtering and monitoring, reporting routes, use of mobile and smart technology, cyber security, data protection, online sexual harassment, harmful online content and emerging risks including artificial intelligence, AI-generated content, deepfakes and synthetic media.

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 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.

18. Staff Training, Procedure Monitoring and Review

It is the role and responsibility of the governing body to ensure that all school staff are aware of this policy and that senior leaders responsible for its effective implementation receive appropriate training and support.

The content of this policy will be reviewed annually, and/or more frequently in line with new developments in the use of technologies, statutory guidance, new or emerging threats to online safety, safeguarding concerns, data protection or cyber incidents, changes to local or trust requirements, or the level and/or nature of incidents reported.

The school and governing body will monitor this policy continuously. The effectiveness of filtering and monitoring arrangements will also be reviewed **at least once every academic year** and records of that review will be retained.

Appendix A - AUP for Staff {Governors & Volunteers}*

All members of staff including Governors and volunteers 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* 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.

If a member of staff breaches school policy, action may be taken in line with the **Code of Conduct for Staff Working in Schools**, the **Low-Level Concerns** policy, **Managing Allegations Against Staff** policy and/or any other appropriate HR guidance.

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:

    - KCSiE 2026, child protection and online safety guidance
    - staff expectations of behaviour policy and professional expectations set out in the Code of Conduct
    - Artificial Intelligence (AI) in Schools Policy
    - Data Protection Policy
    - Positive Behaviour Policy
    - Records Management/Retention Policy
    - Whistleblowing Procedure

- Low-Level Concerns Policy
- Managing Allegations Against Staff Policy.

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 (for example for medical needs, MFA purposes), clear boundaries will be discussed with the Executive Headteacher such as when the devices are used, where they are stored and appropriate school use where children are present. 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 not allowed.

6. Where I deliver or support remote or online learning, I will use school-approved systems and devices wherever possible and will comply with the school's remote learning, safeguarding, data protection and acceptable use requirements.

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 *Kathryn Jones, DHT* or more frequently, as required.

    - I will take all reasonable steps and measures to protect the devices in my care from unauthorised access, accidental disclosure, loss, theft, malware, phishing, smishing, QR-code scams, unauthorised software, unauthorised browser extensions and account compromise.

    - I will not disclose my password or security information to others.

    - I will use multi-factor authentication where required, will not reuse school passwords for personal services, and will report any suspected account compromise, phishing attempt, data breach,

cyber security incident or loss of device immediately through the school's reporting route.

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 Online Safety Co-ordinator, Kathryn Jones DHT.

9. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the *Online Safety Co-ordinator.*

10. I will ensure that any personal data relating to staff, governors, pupils, parents/carers or other members of the school community is handled in accordance with the UK GDPR, the Data Protection Act 2018 and the school's information security policies. This includes personal data, special category data, safeguarding records, SEND information, assessment data, photographs, video, audio, voice recordings and any other identifiable information.

    - 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].*
    - I will not upload, paste, input, summarise, translate, analyse or otherwise process school, pupil, staff, safeguarding, SEND, assessment, image, video, audio or other identifiable information using unauthorised websites, apps, artificial intelligence tools, cloud services or online platforms.

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.

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. I will not use VPNs, proxies, personal hotspots, anonymising services, unauthorised accounts or other methods to bypass filtering, monitoring, logging, security controls or safeguarding protections put in place by the school.

15. 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 (Claire Morgan)* as soon as possible.

16. If I lose any school-related documents or files, I will report this to the *ICT Support Provider (Claire Morgan)* and school's Data Protection Officer, *Rob Montgomery* as soon as possible.

17. 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 pupils must always be appropriate and should only be taken with equipment provided by the school. I understand that images of pupils should only be taken and/or published where the explicit written consent of parents/carers has been given.

18. I will not use AI tools, image generation tools, image enhancement tools, deepfake technology, filters or other apps to create, alter, manipulate, recreate, animate, imitate or publish images, video, audio, voices or likenesses of children, staff, parents/carers or other members of the school community unless this has been expressly approved by the school and complies with safeguarding, consent, data protection, copyright and acceptable use requirements.

Online safety in the classroom

19. I will promote online safety with the pupils 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 pupils 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) (Kathryn Jones 1st Sept-31st Dec Chris McKeon 1st Jan 2027) or a deputy (Anna Mullock – Newcastle, Rach Braybrooke – St Marys, Hannah Deane – Clunbury) as

part of planning online safety lessons or activities to ensure support is in place for any pupils who may be impacted by the content.
- make informed decisions to ensure any online safety resources used with pupils is appropriate.
- teaching children and young people, where age appropriate, about artificial intelligence, AI-generated content, misinformation, bias, copyright, privacy, deepfakes, impersonation and the importance of checking information before relying on or sharing it.

20. 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** and/or **Online Safety Policy.**

21. 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.

Use of artificial intelligence, cloud tools and emerging technologies

22. I will only use artificial intelligence, generative AI, AI chatbots, image generation tools, cloud tools, apps or online platforms for school purposes where they have been approved by the school.

23. I understand that AI outputs may be inaccurate, biased, incomplete, inappropriate or unsuitable for children. I will check any AI-generated content carefully for accuracy, bias, safeguarding risk, age appropriateness, copyright, reliability and professional suitability before using it in school.

24. I will not rely on AI to make safeguarding decisions, pastoral decisions, assessment judgements, HR-related decisions, disciplinary decisions or decisions about children, without appropriate human professional judgement and oversight.

25. I will report any AI-related concern, including harmful AI-generated content, deepfakes, synthetic images or audio, AI-facilitated bullying or harassment, impersonation, unauthorised processing of personal data or inappropriate use of AI tools, through the school's safeguarding, online safety or data protection reporting route.

Mobile devices and smart technology

26. 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.

27. 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.

28. I will not store school information locally on a personal device unless this has been expressly authorised, is necessary for my role, and appropriate security, access control and deletion arrangements are in place. I will not allow family members or others to access any device used for school work.

29. 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.

30. 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.

31. 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.

32. I will ensure that recording-enabled smart technology, including smart watches, smart glasses, voice assistants, personal cameras, location-sharing tools, Bluetooth, AirDrop or equivalent file-sharing functions, are not used in a way that records, captures, shares or transmits information about pupils, staff, parents/carers or school business without prior authorisation.

33. 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).

34. I will not use personal email addresses on the school ICT systems.

35. 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.

36. 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. 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.

37. 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.

38. If I become aware of a filtering or monitoring failure, inappropriate access, suspected bypassing of controls, unsafe online content or a pupil accessing harmful material, I will

report this immediately in line with the school's safeguarding and online safety reporting arrangements.

39. 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

40. 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 appropriate schools polices to include, **Child Protection**, **Online Safety**, **Code of Conduct for Staff.**

41. As outlined in the **Code of Conduct for Staff Working in Schools**

- 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 pupils 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 Executive 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.

42. My electronic communications with current and past pupils 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 pupils, 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 pupils 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 pupils or parents/carers, I will not respond and will report the communication to my line manager and Executive Headteacher/ 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 Executive Headteacher/Designated Safeguarding Lead (DSL).

Professional conduct

43. 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 Executive Headteacher.

44. 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 pupils and staff. This

monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

45. 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 for Staff Working in Schools**.

46. 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 **Code of Conduct for Staff Working in Schools**

47. 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.

48. 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.

49. 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.

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

51. I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher/manager, in line with school's **Child Protection** policy and/or the **Allegations Against Staff…** policy.

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

53. I understand that in the event of any query or concern about this Agreement, I should contact the Executive Headteacher.

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

I understand that this signed AUP will be stored by the school in line with Data Protection legislation and the UK GDPR.

I understand that if I have any queries or questions about this policy, I should contact my line manager in the first instance.

Name (please print)	
Job Title	
Signature	
Date	