Brown Clee C.E. Primary School

ONLINE SAFETY POLICY

Most recently reviewed: **Autumn '25**
Approved by governor: **Vikki Hurst**
Future review date: **Autumn '26**

Aspire ~ Believe ~ Persevere ~ Succeed

Contents

SUMMARY OF POLICY

Responsible individuals:

Governing Body,
Headteacher,
Class Teachers,
Teaching Assistants,
Lunchtime Supervisors,
Administrator.

Relevant documentation used in the formation of this policy:

Keeping Children Safe in Education (Department for Education)
Education Act (1996)
Children Act (1989)
Teaching Online Safety in Schools (2023)

Policy developed to help ensure that…

1. …staff are aware of their responsibilities to keep children safe whilst working online
2. …pupils understand their own responsibilities to keep themselves safe whilst working online

Implementation:

The school will…

- …ensure that all staff, governors, volunteers and visitors are aware of the following policy
- …ensure that the policy is followed at all times
- …ensure that any questions are raised with the headteacher if unsure about any aspects of the policy

Policy shared with:

The original policy that this policy was based upon 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

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 2025 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 (Fortigate/Fastvue) in place and its effectiveness is continuously monitored.

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 (2024) 2023. Schools should also refer to the Ofsted School Inspection Handbook, *updated April 2024.*

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 the school 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.

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.

All staff and students are granted access to the internet. In the case of pupils, this is monitored or supervised by staff. The school will keep a record of any students who have their internet access revoked.

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 school has a filtering system in place and its effectiveness is continuously monitored by the Headteacher.

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.

3.1 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
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
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)

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 / DSL	Danny Harley
DDSL	Ally Heath
Safeguarding Lead Governor	Steph Boxall
I.T. Technical Support	Woodlands ICT: James Ritch / Mike Foden

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

6. Definitions: Devices and 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, including staff, governors, students, volunteers, parents, carers and visitors.

Acceptable Use Policy (AUP) for Staff

The AUP for staff can be found within the staff code of conduct.

All staff, goernors and volunteers must read and sign the Staff Code of Conduct 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 code of conduct 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.

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 Code of Conduct, 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, at the start of the academic year, and to those of new students when they enrol. The student AUP is also available to download on the school website.

Acceptable Use Policy (AUP) for 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 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 and the schools ICT services provider.

11. Data storage

Only encrypted USB pens are to be used in school – and should be avoided in place of the school's virtual cloud-based alternative (OneDrive – through Office365). For further clarification, please contact the headteacher.

11. 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/required 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.
- 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..

Staff are not permitted to use their own personal phones or devices for contacting children/pupils/students or parents and carers – other than via school-assigned email account. Any pre-existing relationships or circumstance, which could compromise a staff member's ability to comply with this, should be discussed with 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/manager, following a formal risk assessment. Staff will follow clear guidance outlined in the Acceptable Use Policy and/or **remote learning AUP**.

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 2025.

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

12. Mobile phones, cameras and other devices (Students)

Students are not permitted to bring devices onto the school premises without prior consent from the headteacher. Students can hand devices into the school office at the start of the day and picked up at the end (provided this has been agreed with the headteacher and parent(s)/carer(s).

Any pupils found with devices will have the device confiscated, and parent(s)/carer(s) will be contacted. This will be dealt with in line with the appropriate school policies, such as the Behaviour policy.

13. Social Media and Networking

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

14. Cyberbullying

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*.'

Cyberbullying is covered in the school's behaviour policy.

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 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 the DSL or DDSL via the school reporting mechanism set out in **Appendix K**, or, where applicable, via the **Whistleblowing Policy.**

Incidents that are of a concern under the Prevent duty should be referred to the Designated Safeguarding Lead or Deputy Designated Safeguarding Lead, 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 ongoing item at staff meetings.

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.

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 and reviews

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.

Appendices

Appendix A: Staff, Governor and Volunteer AUP

AUP for staff, volunteers and governors forms part of their code of conduct.

Appendix B: Students in KS1 AUP

I have the right to feel safe all the time whilst online.
I know that anything I do on the computer can be seen by other people.
I know what to do when I see something that I don't like or am unsure of online

I agree that I will….

- not bring a mobile phone, or any other device from, into school
- 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 unkind 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
- only use devices as told by a teacher
- 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: Students in KS2 AUP

When I am using the computer or other technologies, I want to feel safe all the time.
I am aware what to do when I see something inappropriate or that I am unsure of
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 unkind message or anything which makes me feel unhappy or worried
- not bring a mobile phone, or any other device, into 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
- only use devices in school as directed by an adult

Signed _____ ***Date*** _____

Appendix D: Students in KS3 and above AUP

Not applicable to this setting

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

Student 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 my child should not bring mobile phone and any other personal devices to school. 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.

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.

As part of my role in ensuring an effective home-school-partnership, I will share concerns regarding my child and/or school in the correct manner (i.e. by contacting the school directly).

Signed:

Date:

Appendix F: Online Roles & Responsibilities - List of duties

Headteacher	• 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.
Designated Safeguarding Lead / Deputy Designated Safeguarding Lead	• 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 headteacher to discuss current issues, review incident logs and filtering.
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 • raising concerns in the correct manner
External groups	Any external individual/organisation must sign an Acceptable Use Policy prior to using any equipment or the Internet within the school.