Meole Brace
C of E Primary School and Nursery

Keeping Children Safe in Education: Online Safety Policy

Policy: Online Safety	**Date Policy adopted/reviewed:** September 2025
	Review date: September 2026

Meole Brace
C of E Primary School and Nursery

Online Safety Policy

Contents

1.	**Introduction**
2.	**Scope**
3.	**The Prevent Duty**
4.	**Governing Legislation**
5.	**Roles & Responsibilities**
6.	**Definitions: Devices & Technology**
7.	**School staff, Governors and Volunteers** • Acceptable Use Policy (AUP) for Staff • Acceptable Use of Devices and Technologies: Staff • Staff breaches of the AUP
8.	**Students** • Acceptable Use Policy (AUP) for Students • Acceptable Use of Devices and Technologies: Students • Student breaches of the AUP
9.	**Using non-School Equipment**
10.	**Security and passwords**
11.	**Filtering**
12.	**Monitoring**
13.	**Data storage**
14.	**Mobile phones, cameras and other devices**
15.	**Photograph and Video, social media & Networking**
16.	**Cyber bullying**
17.	**Staff Reporting of E-safety Incidents and Concerns**
18.	**Staff training and updates**
19.	**Communicating the e-Safety Policy**
20.	**Shropshire Safeguarding Contact details**
21	**Education**
22.	**Monitor & Review**

Appendices

	Title	Owner	
A	AUP for staff	HR	Page 16
B	Acceptable Use Agreement for pupils in KS1	EIS	Page 18
C	Acceptable Use Agreement for pupils in KS2	EIS	Page 19
D	Sample Home-school E-safety; ICT, Mobile Phones, Personal Photographs and Social Media	EIS	Page 21
E	E-safety Roles & Responsibilities: List of duties	HR	Page 22
F	Legislation - Overview of relevant legislation governing e-Safety	HR	Page 26
G	E-Safety Incident Reporting Log	EIS	Page 30
H	Examples of potential E-safety concerns (Students)	EIS	Page 31
I	How to Manage Student Breaches of the Acceptable Use Policy	EIS	Page 32
J	Recording and Responding to incidents of misuse – flow chart	HR/EIS	Page 35
K	Cyberbullying: further advice and guidance	HR/EIS	Page 36

1. Introduction

This policy has been written initially by colleagues from Human Resources (HR), the Education Improvement Service (EIS) and Shropshire Safeguarding Children Board (SSCB). It has been adapted by SLT members and governors of Meole Brace Primary School and Nursery. It has been created to support school leaders in addressing whole-school issues in the use and application of new and emerging technologies across the school community. Shared ownership of this policy ensures both consistency of approach, and efficiency in relation to its ongoing review, update and/or revision to content.

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

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

Technology provides unprecedented access to new educational opportunities; online collaboration, learning and communication. At the same time, it can provide the potential for staff and students to access material they should not or be treated by others inappropriately.

E-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, it is integral to a school's ICT curriculum. It may also be embedded in Personal Social and Health Education (PSHE) and Relationship and Sex Education (RSE) and include how pupils should report incidents (e.g. The Child Exploitation and Online Protection (CEOP) button, via a trusted adult, Childline etc)

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

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

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

Ofsted judges schools as 'outstanding', where 'students have an excellent understanding of how to stay safe online and of the dangers of inappropriate use of mobile technology and social networking sites'.
(*Source: Ofsted School Inspection Handbook - October 2017)*

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.

2. Scope

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

All staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse and other risks online as well as face to face. In many cases abuse and other risks will take place concurrently both online and offline. Children can also abuse other children online, this can take the form of abusive, harassing, and misogynistic/misandrist messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography to those who do not want to receive such content.
(Source: Keeping Children Safe in Education -September 2023)

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 is 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 with regard to the searching for electronic devices and the examination of any files or data (even where deleted), on such devices. In the case of both acts, 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 through the use of 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 SITSS.

The Prevent duty means that all staff have a duty to be vigilant, and where necessary, will 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 following:

1. DfE Prevent duty
2. DfE briefing note on the use of social media to encourage travel to Syria and Iraq
3. The Channel Panel
4. Terrorism Act 2000 and the disclosure of information duty where it is believed or suspected that another person has committed an offence.

Practical advice and information for teachers, parents and school leaders on protecting children from extremism and radicalisation is available at:
https://www.educateagainsthate.com/

The Department for Education has dedicated a telephone helpline (0800 789 321) to enable staff and governors to raise concerns relating to extremism directly. Concerns can also be raised by email to:
counter.extremism@education.gsi.gov.uk

Please note that the helpline is not intended for use in emergency situations, such as a child being at immediate risk of harm or a security incident, in which case the normal emergency procedures should be followed.

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.

Online Safety Act 2023
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 safety is seen as a 'whole school' issue, with specific responsibilities delegated as follows:

Headteacher	Mr. H. Bray
Governor with responsibility for Online Safety	Mrs. S. Latcham
Filtering and Monitoring	Mr H. Bray and Mrs H. Lakin (Designated Safeguarding Leads)
E-safety Coordinator / lead teacher of Computing	Miss S. Owens
Technicians	Mr. B. Croft (Shropshire ICT)

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

6. Definitions: Devices & Technology

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, X (formerly Twitter) , Instagram, Snapchat, WhatsApp, YouTube • Real time communications e.g. texts, chat rooms, email, instant messaging, Skype, FaceTime, video chat • On-line gaming, e.g. Xbox, PlayStation

7. School Staff, Governors and Volunteers

The School Community contributes to the Online safety policy and practice through various forums such as the School Council, Governing Body and Staff meetings. All parties are regularly informed of updates and relative information.

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. All AUP's will be stored centrally in case of breaches of the Online Safety policy.

The AUP for staff has been created by HR and adapted by the School. The AUP for staff may be used and/or adapted for any user, to include governors, volunteers and visitors.

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. Differing versions of this agreement may be used to match the personal and professional roles of staff members.

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

Access to online services and school devices will not be approved until new staff have signed and returned the 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 terms and conditions they do not understand.

Staff breaches of the AUP

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

8. Students

Acceptable Use Agreement for pupils (AUA)

The AUA for students can be found in Appendix B, C & D.

A copy of the student AUA is sent to parents with a covering letter/reply slip, at the start of the academic year, and to new students when they enrol. Students will not be given online access or allowed to use school devices before the AUA has been signed and returned to the school office.

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

The student AUAs have been created by the Education Improvement Service and adapted by the school. They have been written to be relevant to and appropriate for different age groups, and can be found in Appendices B, C and D.

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 AUA

Where a student is found to have breached the AUA, this will be dealt with in line with the appropriate school policies, such as the Positive Behaviour policy. The final decision on the level of sanction will be at the discretion of the school management. Examples of infringements and sanctions are found in Appendices.

9. Using non-School Equipment

Under very rare circumstances, staff, governors and visitors are able to use their own devices in school. The headteacher should be made aware of these circumstances should they arise.

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. Pupils and staff should never share passwords and staff must never allow children to use a staff logon. 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.

11. Filtering

Web filtering is provided by Smoothwall and protects all school owned devices. Smoothwall are a member of Internet Watch Foundation (IWF) signed up to Counter-Terrorism Internet Referral Unit list (CTIRU) and block access to illegal content including child sexual abuse material (CSAM). Filtering provision is reviewed and tested annually and is designed to block harmful content without unreasonably impacting teaching and learning.

12. Monitoring

Monitoring is included with Smoothwall. Following a website search violation, the Designated Safeguarding Lead will be sent an email alert. This includes a report outlining details of the blocked issue and the user concerned. Further detailed reports can be generated by school through a request to ict.support@shropshire.gov.uk

13. Data storage

Only encrypted USB pens are to be used in school. Un-encrypted pens cannot be taken out of school and should be locked away at night securely with laptops.
In most circumstances, data is saved on the server and can only be accessed by staff after they have logged in with their unique passwords. Confidential and sensitive data such as CPOMS, is password protected with Designated Safeguarding Leads having fingerprint identification access.

14. Mobile Technologies

Mobile technologies refer to mobile phones, iPads, tablets, Smart watches, and digital cameras

14.1 Mobile phones

Parents, carers and visitors are asked not to use their mobile phone within the school building. Visitors that have access to the premises within the school day beyond the normal picking up and dropping off times, will be asked not to bring their mobile phone into school, or leave it in the reception office. This helps the school to ensure that it meets its safeguarding requirements.

Parents are not allowed to use mobile phones/ electronic devices on the premises

14.2 All staff mobile phones should be kept in lockers whilst on the school premises, and

should not be accessed during contact time with children. Staff may use mobile phones in the staff areas. Phones used on school trips, may only be used for communication directly relating to the safety and wellbeing of the children and staff on the trip.

14.3 Pupils in Years 5 and 6 are allowed to walk home from school with the signed permission of their parents/carers. Some parent/carers may wish for these children to have a mobile phone in school ready for the journey home. If pupils do bring phones to school, they are to be switched off throughout the school day and stored in their school bags and then in personal lockers. Any phones found outside of the lockers or switched on during the school day will be confiscated and will need to be collected by parents/carers after 3.20pm.

If a member of staff suspects that a mobile phone/ electronic device has been misused within the school then the incident must be reported to the Headteacher, Deputy Headteacher or member of the Senior Leadership Team. Staff should not 'search' the phone. The incident should be passed directly to SLT who will deal with the matter in line with normal school procedures, which may include seeking advice from the LA Safeguarding Team.

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

15. Photographs and Video

The use of photographs and videos is frequent in teaching and learning and should be encouraged. However, it is important that consent from parents is gained for all videos or photos of pupils.

Staff should always use a school camera or Ipad to capture images and should not use their personal devices. Images must be saved onto the school server. Images of pupils must not leave the school premises unless permission has been obtained from parents and carers.

If photos/videos are to be used online, and parents/ carers have consented to this, then names of pupils should not be linked to images of pupils. Where it is necessary to use the names of pupils, for example under the heading ' Headteacher 's awards' section on the weekly newsletter, first names of pupils should be used, not the child's full name.

Staff must be fully aware of the consent form responses from parents and carers when considering use of images.

The Consent form used is in appendices.

School cameras should only be removed from school in the event of a school visit, and photos downloaded onto the server, so that the memory card can be wiped as soon as possible.

Photos taken by the school are subject to the Data Protection act.

15.1 Photos and videos taken by parents/carers.

Parents and carers are not permitted to take photos/videos/recordings of children during school events. To avoid the possibility of capturing images of other children in a photograph, parents and carers are requested to take photographs at the end of the event away from other pupils.

The parental letter concerning AUP's includes a paragraph concerning posting photos on social networking sites.

Photos for personal use such as those taken by parents/carers are not subject to the Data Protection Act.

16. Social Media and Networking

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

16.1 Pupils

Pupils are not permitted to use social networking sites within school.

16.2 Staff

It is recognised that social networking sites have a major role to play in today's society. However, staff must be aware of the following:

Staff must not add pupils as friends in social networking sites.

Staff must not post pictures of school events through their personal access to social media sites.

Staff must not use social networking sites within lesson times

Staff should not use photos of other members of staff on their sites without permission.

Staff need to use social networking in a way that does not conflict with the school code of conduct, TDA Core Standards or Personnel handbook

Staff should review and adjust their privacy settings to give them the appropriate level of privacy.

16.3 Use of e-mails

Pupils and staff should only use e-mail addresses that have been issued by the school and the school e-mail system should only be used for school related matters. Pupils and staff are advised to maintain an alternative personal e-mail address for use at home in non-school related matters. When a member of staff or volunteer in school is suspected of using emails inappropriately, then a member of the SLT may need to access this person's emails to clarify issues. It is advised that if a member of the SLT feels that this is necessary, then advice from the LA Safeguarding Team should also be obtained.

17. Cyber bullying

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.

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*.'

17.1 Cyber bullying 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.

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

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

18. 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 breaches of the Online Safety policy need to be recorded by the Headteacher. via the school reporting mechanism set out in Appendix K, or, where applicable, via the Whistleblowing Policy.

The details of the user, date and incident should be reported.

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

Incidents that are of a concern under the Prevent duty should be referred to the Headteacher and/or designated Safeguarding Lead, immediately.

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

Allegations involving staff should be reported to the Headteacher. If the allegation is one of abuse, then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary, the local authority's LADO should be informed.

Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (eg CEOP button, trusted adult, Childline)

Online safety and reporting are taught as part of the Digital Literacy strand in Computing and in PSHE and RSE lessons.

Examples of potential Online concerns may be found at Appendix I.

19. 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 safeguarding students. Online safety is included as part of this.

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

a). A planned programme of formal online safety training is made available to all staff

b). Online Safety training is an integral part of Child Protection / Safeguarding training and vice versa

c). The Headteacher, alongside SLT members is continually auditing staff safety training needs and will address any areas of need that are identified.

d). All staff have an up-to-date awareness of online safety matters, the current school online safety policy and practices and child protection / safeguarding procedures

e). All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Policy

f). The culture of the school ensures that staff support each other in sharing knowledge and good practice about online safety

g). The school takes every opportunity to research and understand good practice that is taking place in other schools

h). Governors are offered the opportunity to undertake training.

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 the 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 Acceptable Use policy to students

- The Acceptable Use Agreement is displayed in the computer suite 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 E-safety information

- The school website provides information on online safety and how the school can help to support and guide their child
- E-safety advice is included as a regular feature in newsletters and as part of the ongoing dialogue between home and school.
- A link to CEOP and online e-safety sites for parents to follow is displayed on the school web site. Parents are also kept aware of developments through events such as 'Safer Internet Day'/event.

18. 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)

Education

Pupils

To equip pupils as confident and safe users of ICT the school will undertake to provide:

a). A planned, broad and progressive online safety education programme that is fully embedded for all children, in all aspects of the curriculum, in all years.

b). Regularly auditing, review and revision of the Computing curriculum

c). Online safety resources that are varied and appropriate and use new technologies to deliver online safety messages in an engaging and relevant manner

d). Opportunities for pupils to be involved in online safety education e.g. Online safety awareness events, Online safety assemblies, Children's Safeguarding Board, etc.

Additionally,

a). Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information

b). There are many opportunities for pupils to develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

c). The school actively provides systematic opportunities for pupils / students to develop the skills of safe and discriminating on-line behaviour

d). Pupils are taught to acknowledge copyright and intellectual property rights in all their work.

19. Monitoring and review

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

The impact of the online safety policy and practice is monitored throughout the year. This review will take into consideration an audit of e-safety incident logs, behaviour/ bullying logs and pupil voice.

The outcome of this review will be reported to governors through the Headteacher's Report. Headteacher's Reports are written every term to keep governors informed of school priorities. Outcomes could also be reported to:

- Shropshire Local Authority (where necessary)
- Shropshire Safeguarding Community Partnership (SSCP)

School Development Plans will reflect any planned action based on the above. This policy should be read in conjunction with the school's Safeguarding and Child Protection Policy.

Appendix A

Acceptable Use Policy for Staff, Governors & Volunteers

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 pupils at all times.

I understand that I must use school devices and systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of systems and other users.

I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to benefit from the use and application of appropriate digital technology.

I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with children and young people.

Professional and personal safety:

- I understand that the school has in place a filtering system and will monitor my access to digital technology and communications systems whilst using school devices, and/or access to the school network via personal devices, where such access has been granted.
- I understand that the rules set out in this agreement also apply to use of school devices and digital technologies out of school, and to the transfer of personal data (digital or paper based) out of school.

- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use in line with the general principles of this agreement and the expectations of professional behaviour set out in the Staff Code of Conduct.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should keep passwords safe and not share them with anyone.
- I will immediately report any incidence of access to illegal, inappropriate or harmful material, deliberate or accidental, by myself or others, to the appropriate person.
- I will not install or attempt to install programmes of any type on a device, nor will I try to alter computer settings, unless this is permitted by the Network Manager.
- I will not deliberately disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy).
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when required by law, or by school policy, to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving devices or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will log out of a device when I have finished using it.

Electronic communications and use of social media:

- 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 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 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.
- 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 only communicate with students and parents/carers using official school systems. 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 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.
- 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 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.

Use of school and personal mobile devices and technologies

- When I use my own mobile device (e.g. laptop / tablet / mobile phone / USB device/smart watch) 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.
- 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.
- 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 with a member of the senior leadership team, and then that is discreet and appropriate, e.g. not in the presence of students.

- 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.
- I will report any text or images sent to me by colleagues or students which could be viewed as inappropriate. I will not use a personal device to photograph a student(s), except with the written permission of the Headteacher.
- I will not use personal email addresses on the school ICT systems.
- 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.
- I will, when I take and/or publish images of others, do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use any personal devices to record these images, unless I have written permission from the Headteacher. Where these images are approved by the school to be published (e.g. on the school website) it will not be possible to identify by name, or any other personal information, those who are featured.
- 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.
- 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.

Conduct and actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school devices and digital technology in school, but also applies to my use of school systems and equipment off the premises. This Acceptable Use Policy also applies to my use of personal devices on the premises or in situations related to my employment by the school.
- I understand that should I fail to comply with this Acceptable Use Policy Agreement, I may be subject to disciplinary action in line with the school's agreed Disciplinary Procedure. In the event of any indication of illegal activity, I understand the matter may be referred to the appropriate agencies.

I have read and understood the above and agree to use school devices and access digital technology systems (both in and out of school), as well as my own devices (in school and when carrying out communications related to the school), within this agreement.

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

Staff / Volunteer Name:	
Signed:	
Date:	

Appendix B

Meole Brace
C of E Primary School and Nursery

CEOP REPORT
ceop.police.uk

Acceptable Use Agreement for pupils in KS1

I want to feel safe all the time.

I know that anything I do on the computer can be seen by other people.

I know when to use the CEOP report button

- ✓ **I will ask a teacher or suitable adult before I use a device**
- ✓ **I will ask for help from a trusted adult if I am not sure what to do or if I think something is wrong**
- ✓ **I will remember not to share personal details about myself online- name, address, anything about my home and family**
- ✓ **I will only send polite messages and use kind words**

- not use my own digital devices, in school, unless I am given permission
- only open web pages which my teacher has said are okay
- only work with people I know in real life
- tell an adult in school 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 an inappropriate message
- not reply to any messages which makes me feel sad or worried
- only email people I know or if my teacher agrees
- talk to my teacher before using anything on the internet
- not upload photographs of myself without asking a teacher
- never agree to meet a stranger

Signed _____ ***Date*** _____

Appendix C

Meole Brace
C of E Primary School and Nursery

CEOP REPORT
ceop.police.uk

Acceptable Use Agreement for pupils in KS2

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

I am aware of the CEOP report button and know when to use it.

I know that anything I share online may be monitored by school.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

I know that if I bring a mobile phone to school it needs to remain in my bag and my bag needs to be stored in my locker until the end of the school day (Y5 and Y6 only)

I agree that I will:

- always keep my passwords safe and not share them with anyone
- only visit sites which are appropriate
- work in collaboration only with people my school has approved, and I will deny access to others
- respect the school network security
- make sure all messages I send are respectful
- show a responsible adult any content that makes me feel unsafe, worried or uncomfortable
- not reply to any inappropriate message or anything which makes me feel unhappy or worried
- not use my own mobile phone, or any other personal device, in school
- not use my smart watch to message, take photographs or film during the school day
- only email people I know or are approved by my school
- only use email which has been provided by school
- 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

Signed _____ ***Date***_____

Created by School Council

Appendix D

Meole Brace
C of E Primary School and Nursery

Home-school Online Safety

Computing, Mobile Phones, Personal Photographs and Social Media

Student Name:	
Student's class teacher name:	
Parent/Carer/Guardian's name:	

Use of School Information Communication Technology 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, 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 internet service, providing secure access to email, employing appropriate teaching practice, and teaching online safety 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 if my child wears a smart watch, functionality for messaging should be switched off throughout the school day. Images and filming are strictly prohibited, and I understand that if my child breaks this rule, the watch will be confiscated and I will be asked to collect it in person, at the end of the school day.

Pupils in Years 5 and 6 are allowed to walk home from school with the signed permission of their parents/carers. Some parent/carers may wish for these children to have a mobile phone in school ready for the journey home. I understand that if my child does bring a phone to school, they are to be switched off throughout the school day and stored in their school bags and then in personal lockers. Any phones found outside of the lockers or switched on during the school day will be confiscated and will need to be collected by parents/carers after 3.20pm.

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 that these should be taken away from the other children at the end of the event, to eliminate the possibility that it may contain images of other children. I will support the school's approach to online safety and will not post, upload or add any text, image or video that could upset, offend or threaten the safety of any member of the school community.

Signature of Parent/Carer/Guardian:

Date:

Appendix E

E-safety 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 • Ensure that monitoring of content is managed • Ensures that staff receive appropriate training to enable them to carry out their online safety responsibilities • 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. • Ensures that any recording, processing, or transfer of personal data is carried out in accordance with the *Data Protection Act* 1998. • Ensures that there is a system in place to monitor and support staff who carry out internal E-safety procedures and reviews. • Oversees the administration of the staff Acceptable Use Policy Agreements and takes appropriate action where staff are found to be in breach.
Online Safety Leader	• Takes day to day responsibility for online safety issues and assumes a leading role in establishing and reviewing the school online safety policies and supporting documents. • Ensures that the school is compliant with all statutory requirements in relation to the handling and storage of information. • Ensures that any recording, processing, or transfer of personal data is carried out in accordance with the *Data Protection Act* 1998. • Promotes an awareness of and commitment to online safety throughout the school community. • Ensures that online safety is embedded across the curriculum. • Is the main point of contact for students, staff, volunteers and parents who have online safety concerns. • Ensures that staff and students are regularly updated on online safety issues and legislation, and are aware of the potential for serious child protection issues that arise from (for example): - sharing of personal data - access to illegal/inappropriate materials

	- inappropriate on-line contact with adults/strangers - cyber-bullying • Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident. • Ensures that an online safety incident log is kept up to date. • Liaises with school IT technical staff where necessary and/or appropriate. • Facilitates training and provides advice and guidance to all staff. • Communicates regularly with SLT to discuss current issues, review incident logs and filtering.

Network Provider/Technician	• Oversees the security of the school ICT system. • Ensures that appropriate mechanisms are in place to detect misuse and malicious attack (e.g. firewalls and antivirus software). • Ensures that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • Ensures that the school's policy on web-filtering is applied and updated on a regular basis. • Ensures that access controls/encryption exist to protect personal and sensitive information held on school-owned devices. • Ensures that users may only access the school networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed. • Reports any E-safety incidents or concerns, to the online safety lead • Keeps up to date with the school's online safety policy and technical information in order to carry out the E-safety role effectively and to inform and update others as relevant. • Keeps up-to-date documentation of the school's E-security and technical procedures. • Keeps an up to date record of those granted access to school systems.
ALL Staff	• Read, understand and help promote the school's online safety policies and guidance. • Are aware of E-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 lead • Maintain an awareness of current E-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 E-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. • Deliver lessons on online safety and awareness through the Digital Literacy strand of Computing and the PSHE and RSE curriculum.
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 sound online safety practice when using digital technologies out of school and realise that the school's Online safety Policy covers their actions, in and out of school, if related to their membership of the school.
Parents / Carers:	Parents and carers are encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of: • digital and video images taken at school events. • access to parents' sections of the website and on-line student/student records.
External groups:	Any external individual/organisation must sign an Acceptable Use Policy prior to using any equipment or the Internet within the school.