E-Safety policy

Member of Staff Responsible	**CEO** (statement of intent for trust), **Headteacher** for procedure and implementation of e-safety at school.
Relevant guidance/advice/legal reference	KCSiE (2021)
Adopted by	Individual schools and trust office
Date of Policy	November 2021
Review Cycle	3 years
Date of Next Review	November 2024
Website	Yes (published annually)

Section 1 (Trust)

Statement of Intent (from the Trust)

This policy is not a statutory requirement, but its existence recognises the significance of students and staff remaining safe whilst accessing resources online.

The 3-18 Education Trust has the highest regard for E-safety in its schools in order to promote safe and responsible use of technology. We are committed to using new technology to enhance the curriculum and educational opportunities whilst equipping our children and young people with the knowledge and understanding to stay safe and vigilant when online, both in school and outside.

E-safety infolves 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).

E-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 shouldn't 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, is integral to a school's ICT curriculum. It may also be embedded in Personal Social and Health Education (PSHE) and Relationships, Sex and Health Education and include how staff and students should report incidents

Advice and resources on internet safety are available at: https://www.saferinternet.org.uk/

In association with the relevant 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 and Behaviour policies

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 sanctions 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.

Schools 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.

The Prevent Duty (See Preventing Radicalisation and Extremism Policy)

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 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

https://www.educateagainsthate.com/

The use of devices in school, which are not owned by school

Mobile phones: If a student wishes to bring these into school, they must be switched off and put away. The trust recognises the value that a mobile phone can have at the start and finish of the school day, but also the significant distraction and potential harm that the use of a mobile phone can bring when used in school.

Student devices such as mobile phones, should be switched to silent whilst on the school premises and kept out of sight. Students found to be in breach of this requirement will have their device confiscated. These can be collected at the end of the 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 (see below).

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*.'

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.

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

Section 2: School-based implementation and policy.

Individual schools are responsible for their E-Safety procedures and are given freedom to manage their provision. This is due to their different contexts with respect to key stages. Day to day responsibility for educating pupils in E-safety settings lies with the Headteachers and other staff with responsibility for the IT provision in schools.

The E-safety 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.

Coleham Primary School

E-Safety Procedure

Guidance: DFE Teaching online safety in school

(https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf)

Appendices

	Title
1	**AUP for staff**
2	**AUP for learners in KS1**
3	**AUP for learners in KS2**
4	**E-safety Roles & Responsibilities: List of duties**
5	**Legislation - Overview of relevant legislation governing e-Safety**
6	**Examples of potential E-safety concerns (Students)**
7	**Recording and Responding to incidents of misuse – flow chart**
8	**Cyberbullying: further advice and guidance**
9	**Examples of potential E-safety concerns (Students)**

1.   Introduction

We want to equip our pupils with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way, so they are able to reap the benefits of the online world.

We are committed to delivering online safety content within the curriculum and embed this within their wider whole school approach.

This procedure has been created to support school in addressing e-safety issues consistently across school.

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, 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, is integral to a 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 procedure 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 policy, Behaviour and Anti-Bullying policies.

This procedure will be reviewed regularly 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 procedure applies to all members of the school community, including staff, governors, pupils, volunteers, parents, carers and visitors 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 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 Disciplinary Procedure and Behaviour Policy.

3.   The Prevent Duty

Staff 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 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 trust's ICT department.

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 (020 7340 7264) 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.

All staff should complete the online Prevent training and all Designated Safeguarding Leads should also complete the Channel Training. The School Business Manager is responsible for monitoring this staff training. As best practice, this training should be refreshed every 3 years.

https://www.elearning.prevent.homeoffice.gov.uk/edu/screen1.html

https://www.elearning.prevent.homeoffice.gov.uk/channel_awareness/01-welcome.html

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.

Computer Misuse Act 1990
Data Protection Act 2018
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 5.

5. Roles & Responsibilities

E-safety is seen as a 'whole school' issue, with specific responsibilities delegated as follows:

Head/Deputy	Ms C Jones/Mr T Larkham
Business Manager	Miss T Othen
ICT Co-ordinator	Mrs K Harrison
Head of Trust ICT	Mr T Goodman
ICT Technician	Mr D Williams

A full description of the responsibilities associated with these roles may be found in Appendix 4.

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, Twitter, Instagram, Snapchat, WhatsApp, YouTube
- Real time communications e.g. texts, chat rooms, email, instant messaging, video calls
- On-line gaming, e.g. Xbox, PlayStation

7. Curriculum

School uses National Online Safety curriculum lesson scheme as trusted, reputable content and good quality, age appropriate, up to date resources. We follow the Education for a Connected World Framework which includes age specific advice about the online knowledge and skills that pupils should have the opportunity to develop at different stages of their lives, including how to navigate online safely. This was developed by the UK Council for Internet Safety.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/89 6323/UKCIS_Education_for_a_Connected_World_.pdf

External Resources and Visitors

School uses National Online Safety as a trusted, reputable source for E-safety support guides and training for staff, parents and pupils. School uses West Mercia Police as a trusted and reputable external visitor to provide a useful and engaging approach to deliver online safety messages, which enhances our e-safety approach. Pupils from local secondary schools also work on a peer on peer basis with our year 5/6 pupils to share their experiences about e-safety and personal experiences.

8. Whole school approach

At Coleham School we aim to deliver a whole school approach to E-safety. This goes beyond teaching to include all aspects of school life, including culture, ethos, environment and partnerships with families and the community.
In practice, this means:
• Creating a culture that incorporates the principles of online safety across all elements of school life. The principles should be reflected in the school's policies and practice where appropriate, and should be communicated with staff, pupils and parents. This will include, for example, in the child protection policy clear processes for reporting incidents or concerns.
• Proactively engaging staff, pupils and parents/carers in school activities that promote the agreed principles of online safety. This includes peer-to-peer support from a local secondary school.
• Reviewing and maintaining the online safety principles. This includes making sure that school staff have access to up to date appropriate training/CPD and resources, so that they are confident in covering the required content in a way that is relevant to their pupils' lives. It could also include using information available to the school to review practices and ensure the issues facing their pupils are covered in a timely manner.
• Embedding the online safety principles: When teaching curriculum subjects and other teaching opportunities to Reinforcing what is taught in lessons by taking appropriate and consistent action when a pupil makes a report of unacceptable online behaviours from another pupil, including cyberbullying, or shares a concern about something they have seen online. Modelling the online safety principles

consistently. Schools should also ensure they extend support to parents, so they are able to incorporate the same principles of online safety at home.

9.   School Staff, Governors and Volunteers

Acceptable Use Policy Agreements

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. This is covered at the Individual's induction.

Acceptable Use Policy (AUP) for Staff

The AUP for staff can be found in **Appendix 1**

All staff must read and sign the 'Acceptable Use Policy Agreement for Staff' (AUP) before using any school IT resource. This will take place at induction with the School Business Manager.

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.

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.

E-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 HR policies such as the Disciplinary procedure, and /or with reference to external agency guidance.

10.   Pupils

Acceptable Use Policy (AUP) for Students

The AUP KS1 and KS2 for students can be found in **Appendix 2 & 3.**

A copy of the pupil AUP for information is sent to all new Reception parents, in the induction pack for starting school and to new students when they enrol in the mid-term induction pack.

The pupil AUP will form part of the first Autumn term lesson of ICT for each year group.

Acceptable Use of Devices and Technologies: Pupils

Pupils 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.

Pupil 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.

Where staff identify an E-safety concern (in school or at home) they should log this separately on CPOMS. This enables school to effectively record and monitor all e-safety concerns and identify any trends or curriculum work needed. (see section 17 below)

Examples of scenarios which may give rise to an E-safety concern are set out in Appendix 9

Remedial action, sanctions and support are at the discretion of SLT. Outline guidance for teaching and leadership staff is set out in Appendix J.

11.   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. Staff must always 'lock' a device (e.g. a classroom PC) if they are going to leave it unattended.

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

12.   Data storage

Only encrypted laptops are school devices to be used in school.

13.   Use of e-mails

Pupils and staff should only use e-mail addresses that have been issued by the school and the 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.

14.   Mobile phones, cameras and other devices

The school's policy relating to the use of devices such as mobile phones, is set out in the relevant AUP and school Mobile Phone Procedure and Child Protection Policy.

Children in Years 5 and 6 are permitted to bring mobile phones to school subject to the terms and conditions of the Mobile Phone Procedure.

Pupils' mobile phones should be switched off whilst on the school premises and their phones must be handed into their class teacher. Pupil phones found to contravene this should be confiscated by the class teacher and returned 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 but staff should not 'search' the phone. The incident should be passed directly to SLT who will deal the matter in line with normal school procedures and/or the Behaviour policy.

Pupils are not permitted to bring SMART watches into school. This is to protect against them from being lost or damaged and so children cannot receive messages or phone calls, in line with the mobile phone use.

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

Staff should only use a personal mobile phone in the confinement of a childfree zone. The Caretaker and Business Manager are permitted to use mobile phones on site for the purpose of their role.

15.   Photographs and Video

The use of photographs and videos is essential for teaching and learning and should be encouraged.

We obtain two separate consents for photographs and videos for educational purposes and for promotional purposes. These are obtained on our consent form for all new starters and enrolments and refreshed annually. A list of children who do not have consent is updated by the office team.

All staff have a responsibility, to check the non-consent document to ensure that photographs are only used, if school has the photograph/video consent for the children contained in the images.

If photos/videos are to be used online then names of pupils should not be linked to pupils.

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

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

16.   Photos and videos taken by parents/carers.

Parents and carers are permitted to take photos/videos of their own children at school events. They are requested not to share photos/videos on social networking sites if they contain images of other children. Parents are reminded of this when the need arises.

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

17.   Social Media and Networking

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

Parents should support the school's approach to e-Safety and will not post, upload or add any text (including the school name or children's names), images or videos onto social media or networking groups that could upset, offend or threaten the safety of any member of the school community or bring the school into disrepute.

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

18.   Cyber bullying

All forms of bullying (including cyberbullying) will be dealt with by SLT.   Measures to prevent bullying are part of the school's behaviour and anti-bullying policy which are 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.'

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 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

Any incidents affecting staff will be dealt with by SLT, who will seek appropriate external support and guidance.

Please refer to Appendix 8 for further guidance and support in dealing with instances of cyberbullying against staff and/or students.

19.   Staff Reporting of E-safety 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 e-safety concerns/incidents that come to the attention of school staff should be logged separately on CPOMS copying in class teachers, Phase Leader or SLT/DSLs as appropriate. This enables school to effectively record and monitor all e-safety concerns and identify any trends or curriculum work needed.

E-safety concerns/investigation should be communicated to the ICT Technician and School Business Manager where appropriate, for any corrective/preventative measures, investigation, GDPR implications or support literature.

E-safety concerns will be dealt with by SLT. SLT will decide on any sanctions or support required.

Staff should support the parents and child with nay support Guides from our National Online Safety Resource Hub.

For any concern that raises child protection issues, Designated Safeguarding Leads must be alerted on the E-safety CPOMS concern. It is their responsibility to decide on appropriate action.

For any concern under the Prevent duty, Designated Safeguarding Leads must be alerted on the E-safety CPOMS concern. It is their responsibility to decide on the necessary actions regarding safeguarding and the Channel Panel.

The curriculum will cover how pupils should report incidents

- Trusted Adult
- Ceop button, https://www.ceop.police.uk/CEOP-Reporting/
- 3rd sector organisations such as https://www.childline.org.uk/ and https://www.iwf.org.uk/

Examples of potential E-safety concerns may be found at Appendix 6.

A Flowchart to assist staff reporting is found at Appendix 7

Pupils are also informed that sanctions/support can be applied to e-safety incidents that take place out of school if they are related to school.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, HR and Safeguarding professionals.

20.   Staff training and updates

School have a package with National Online safety. This provides online training, monthly updates and webinars and support guides to all staff and parents. All staff should complete the E-safety training relevant to their professional role. This E-safety procedure is included as part of the induction process to the school for all staff and volunteers. Staff receive regular training in safeguarding students-E-safety is included as part of this.

21.   Communicating the E-safety Procedure

Staff and the E-safety procedure

•   All staff will be given a copy of the E-safety Procedure during statutory induction and its importance explained. This will form part of the Health & Safety Induction by the Business Manager.

•   An Acceptable Use Policy Agreement is signed and 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 E-safety policy to pupils

•   The Pupil AUP will form part of the first lesson of ICT for each year group ad is referred to regularly.

•   Students are made aware that network and Internet use is monitored.

Home-School Communication of E-safety information

•   The school website provides information on E-safety. The National Online Safety Package contains resources and training to parents to support and guide their child.

•   E-safety advice is included as a regular feature as part of the ongoing dialogue between home and school.

•   The school includes e-safety events and 'safer internet days' as part of the curriculum.

22.   Monitor & review

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

Coleham Primary School Information & Communication Technology (ICT) Acceptable Use Agreement for Staff & 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.

I will ensure that iPads and laptops will **only** be used for teaching and learning purposes in a lesson with a teacher or TA present. They must not be used recreationally at break times or home time by **any** child.

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, in accordance with the Data Protection Act and in line with the schools policies.

- I understand that data protection legislation requires that any personal 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 only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner.

- 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

- If 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.

- 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 stored away 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/on silent 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).

- 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 policies on the use of digital/video images. I will not use any personal devices to record these images, unless I have 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.

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 any permissible 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.

Signed…………………………………………………………………   Date……………………………………………………………..

Coleham Primary School Computing

Acceptable Use Agreement for learners in KS1

I want to feel safe all the time at school.

I understand that anything I do on the laptops or iPads in school may be seen by someone else.

I agree that I will:

- only use laptops or iPads in lesson times with a teacher or TA present
- show my teacher if I get a nasty message
- not reply to any messages which make me feel sad or worried
- make sure all messages I send are polite
- not upload photographs of myself without asking my teacher
- only communicate with people I know in real life
- not tell people about myself online. (I will not tell them my name, anything about my home, my family, my school or my pets.)
- never agree to meet a stranger
- check with a teacher before using the internet
- only open website pages which a teacher has said are OK
- tell a teacher if anything makes me feel scared or unhappy on the internet
- only email people I know and if a teacher agrees it is OK

Appendix 3

Coleham Primary School Computing

Acceptable Use Agreement for learners in KS2

When I am using the laptops or iPads in school, I want to feel safe.

I know that anything I share online in lessons 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 mean for it to be used.

I agree that I will:

- only use laptops or iPads in lesson times with a teacher or TA present
- look after computing equipment including respecting the internet
- not use my own mobile phone or other electronic device in school.
- make sure all messages I send are kind and respectful.
- not reply to any nasty message which makes me feel unhappy or worried.
- show a responsible adult anything online that makes me feel unsafe, worried or uncomfortable.
- not reply to strangers and report messages from strangers straight away to my teacher.
- always keep my personal details private. (My name, family information, journey to school, my pets and hobbies are all examples of personal details.)
- talk to a responsible adult if a friend I've met online wants to meet me.
- never arrange to meet an online friend by myself.
- only share messages and images that are legal.
- always check with a responsible adult before I share images of myself or others.
- only give my mobile phone number to friends I know and trust in real life.
- always keep my passwords safe and not share them with anyone.
- in school time, only email people who my teacher has given me permission to email.
- only visit websites which my teacher has asked me to use.
- not click on 'pop-ups' on my screen. Tell my teacher about them.

Appendix 4

Coleham Primary School

E-safety Roles & Responsibilities: List of duties

Headteacher	• Has overall responsibility for E-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 E-safety roles. • Can direct the whole school community including staff, students and governors to information, policies and practice about E-safety. • Is aware of the procedures to be followed in the event of a serious E-safety incident. • Ensures that there is a system in place to monitor and support staff who carry out internal E-safety procedures and reviews.
SBM/SLT	• responsible for day to day data and physical data security. • Ensures that the school is compliant with all statutory requirements in relation to the handling and storage of information. • Ensures that any recording, processing, or transfer of personal data is carried out in accordance with the Data Protection Act 2018. • Assumes a leading role in establishing and reviewing the E-Safety procedure and supporting documents/consents. • Promotes an awareness of and commitment to E-safety throughout the school community. • Ensures that E-safety is embedded across the curriculum. • Can direct the whole school community including staff, students and governors to information, policies and practice about E-safety. • Is the main point of contact for students, staff, volunteers and parents who have E-safety concerns. • Oversees the administration of the staff Acceptable Use Policy Agreements and takes appropriate action where staff are found to be in breach. • Ensures that staff and students are regularly updated on E-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 E-safety incident. • Ensures that an E-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 <mark>SLT</mark> to discuss current issues, review incident logs and filtering.
	•	
Teacher for ICT	•	Oversees the delivery of the E-safety element of the Computing curriculum and Pupil AUP.
ICT	•	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 E-safety co-ordinator.
	•	Keeps up to date with the school's E-safety procedure 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 E-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 E-safety coordinator or ICT.
	•	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 school 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.

Teachers	• 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. • Are responsible for using the school ICT systems in accordance with the Student AUP Agreement.
Pupils	• Are responsible for using the school digital technology systems in accordance with the Student AUP Agreement. • 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 E-Safety Policy covers their actions, in and out of school, if related to their membership of the school.
Parents	• Parents and carers are encouraged to support the school and their child in promoting good online safety practice and to follow guidelines on the appropriate use of social media and digital and video images taken at school events.
External Users	• Any external individual/organisation must sign an Acceptable Use Policy prior to using any equipment or the Internet within the school.

Appendix 5

Legislation - Overview of relevant legislation governing E-safety

Schools should be aware of the legislative framework under which this E-safety Policy template and guidance has been produced. It is important to note that in general terms, an action that is illegal if committed offline is also illegal if committed online.

It is recommended that HR and/or legal advice is sought in the event of an E-safety incident or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

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

Data Protection Act 2018

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that personal data must be:

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

Freedom of Information Act 2000

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

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence, liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority, intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this Act.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as 'fair dealing', which means, under certain circumstances, permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or

- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear, on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet), it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification, or that of others. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any person having sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view to releasing it, a criminal offence.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

• 	The right to a fair trial
• 	The right to respect for private and family life, home and correspondence
• 	Freedom of thought, conscience and religion
• 	Freedom of expression
• 	Freedom of assembly
• 	Prohibition of discrimination
• 	The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems.

The School Information Regulations 2012

Requires schools to publish certain information on its website:

https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Serious Crime Act 2015

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

Appendix 6

Examples of potential E-safety concerns Pupils)

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

Inappropriate material accessed on school computers

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

Pupils are taught that they are not at fault if they see or come across something online that they find worrying or upsetting and are encouraged to alert staff to any inappropriate content. The staff member should report the incident to SLT and ICT to make any necessary adjustment to filter settings.

Abusive messages on school computers

Students who receive abusive messages over school systems will be supported, and advised not to delete messages. A formal process of investigation will be initiated.

Parent/Carer/Guardian reports of cyber bullying

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

Student disclosure of concerns or abuse

All staff receive Safeguarding and E-safety training as part of their induction, and thereafter on a regular basis. Where a student discloses a concern to a member of school staff, this is passed on to the Designated Safeguarding Lead.

Student reporting outside school

Students are taught that if something worries them, or if they think a situation is getting out of hand, that they should share this with a trusted adult such as their parents, carers, guardians or school staff.

Allegations against staff

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

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

Appendix 7

Recording and Responding to incidents of misuse – flow chart
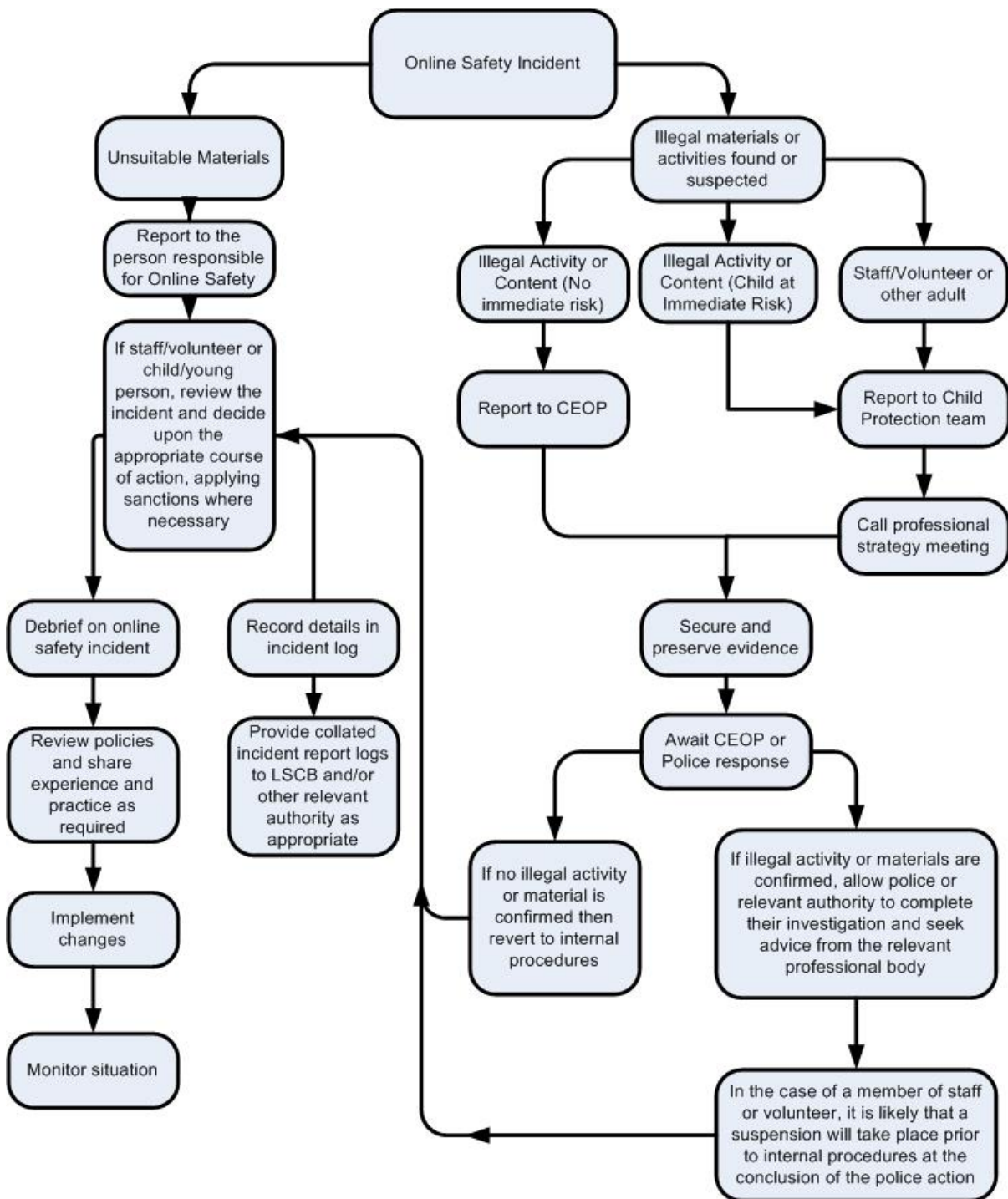
Appendix 8

Cyberbullying: further advice and guidance

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

•   Abusive comments, rumours, gossip and threats made over the internet or using digital communications – this includes internet trolling.

•   Sharing pictures, videos or personal information without the consent of the owner and with the intent to cause harm and/or humiliation.

•   Hacking into someone's email, phone or online profiles to extract and share personal information, or to send abusive or inappropriate content whilst posing as that person.

•   Creating specific websites or 'pages' on the Internet that negatively target an individual or group, typically by posting content that intends to humiliate, ostracise and/or threaten.

•   Blackmail, or pressurising someone to do something online they do not want to do such as sending a sexually explicit image.

Cyberbullying: Advice for headteachers and school staff

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

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

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

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

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

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

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

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

Level 1 breaches

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

[Possible Sanctions: refer to class teacher / confiscation of phone or other device]

Level 2 breaches

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

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

Level 3 breaches

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

[Possible Sanctions: refer to Class teacher / Headteacher / removal of Internet rights for a period / contact with parents/carers]

Other safeguarding actions

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site

2. Inform SSCB/LA as appropriate

Level 4 breaches

- Continued sending of emails and/or messages regarded as harassment or of a bullying nature after being warned (cyberbullying)
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

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

Other safeguarding actions:

1. Secure and preserve any evidence
2. Inform the sender's e-mail service provider if a system other than the school system is used.

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

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

Review Table		
Procedure created	To	March 2021
Added as section 2 to Trust policy	To	December 2021