

# Schools HR Policy & Procedure Handbook



## ***Crowmoor Primary School*** **E-Safety Policy**

This Policy has been agreed by the following professional associations and Trade Unions representing Teachers, Headteachers and Support Staff:

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

This policy has been adopted by the governing body

on

20<sup>th</sup> November 2019  
Review due November 2021

## CONTENTS

1.	<b>Introduction</b>	<b>Page 4</b>
2.	<b>Scope</b>	<b>Page 5</b>
3.	<b>The Prevent Duty</b>	<b>Page 5</b>
4.	<b>Governing Legislation</b>	<b>Page 6</b>
5.	<b>Roles &amp; Responsibilities</b>	<b>Page 7</b>
6.	<b>Definitions: Devices &amp; Technology</b>	<b>Page 7</b>
7.	<b>School staff, Governors and Volunteers</b> <ul style="list-style-type: none"> <li>• Acceptable Use Policy (AUP) for Staff</li> <li>• Acceptable Use of Devices and Technologies: Staff</li> <li>• Staff breaches of the AUP</li> </ul>	<b>Page 8</b>
8.	<b>Students</b> <ul style="list-style-type: none"> <li>• Acceptable Use Policy (AUP) for Students</li> <li>• Acceptable Use of Devices and Technologies: Students</li> <li>• Student breaches of the AUP</li> </ul>	<b>Page 9</b>
9.	<b>Using non-School Equipment – ‘Bring Your Own Device/Bring Your Own Technology’ (BYOD/BYOT)</b>	<b>Page 10</b>
10.	<b>Security and passwords</b>	<b>Page 10</b>
11.	<b>Data storage</b>	<b>Page 10</b>
12.	<b>Mobile phones, cameras and other devices</b>	<b>Page 10</b>
13.	<b>Social Media &amp; Networking</b>	<b>Page 11</b>
14.	<b>Cyber bullying</b>	<b>Page 11</b>
15.	<b>Staff Reporting of E-safety Incidents and Concerns</b>	<b>Page 11</b>
16.	<b>Staff training and updates</b>	<b>Page 12</b>
17.	<b>Communicating the e-Safety Policy</b>	<b>Page 12</b>
18.	<b>Shropshire Safeguarding Contact details</b>	<b>Page 13</b>
19.	<b>Monitor &amp; Review</b>	<b>Page 13</b>

## Appendices

	Title	Owner	
<b>A</b>	<b>AUP for staff</b>	<b>HR</b>	<b>Page 14</b>
<b>B</b>	<b>AUP for learners in KS1</b>	<b>EIS</b>	<b>Page 17</b>
<b>C</b>	<b>AUP for learners in KS2</b>	<b>EIS</b>	<b>Page 18</b>
<b>D</b>	<b>AUP for learners in KS3 and above</b>	<b>EIS</b>	<b>Page 19</b>
<b>E</b>	<b>Sample Home-school E-safety; ICT, Mobile Phones, Personal Photographs and Social Media</b>	<b>EIS</b>	<b>Page 21</b>
<b>F</b>	<b>E-safety Roles &amp; Responsibilities: List of duties</b>	<b>HR</b>	<b>Page 22</b>
<b>G</b>	<b>Legislation - Overview of relevant legislation governing e-Safety</b>	<b>HR</b>	<b>Page 26</b>
<b>H</b>	<b>E-Safety Incident Reporting Log</b>	<b>EIS</b>	<b>Page 31</b>
<b>I</b>	<b>Examples of potential E-safety concerns (Students)</b>	<b>EIS</b>	<b>Page 32</b>
<b>J</b>	<b>How to Manage Student Breaches of the Acceptable Use Policy</b>	<b>EIS</b>	<b>Page 33</b>
<b>K</b>	<b>Recording and Responding to incidents of misuse – flow chart</b>	<b>HR/EIS</b>	<b>Page 36</b>
<b>L</b>	<b>Cyberbullying: further advice and guidance</b>	<b>HR/EIS</b>	<b>Page 37</b>

### HR – Human Resources

Shirehall  
 Abbey Foregate  
 Shrewsbury  
 Shropshire  
 SY2 6ND  
[ask.hr@shropshire.gov.uk](mailto:ask.hr@shropshire.gov.uk)

### EIS – Education Improvement Service

Shirehall  
 Abbey Foregate  
 Shrewsbury  
 Shropshire  
 SY2 6ND  
[steve.compton@shropshire.gov.uk](mailto:steve.compton@shropshire.gov.uk)

## E-Safety Policy

### 1. Introduction

This policy has been written by colleagues from Human Resources (HR), the Education Improvement Service (EIS) and Shropshire Safeguarding Children Board (SSCB). 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.

E-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.).

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 Sex and Relationship Education (SRE) and include how students should report incidents (e.g. The Child Exploitation and Online Protection (CEOP) button, via a trusted adult, Childline etc)

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

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

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

Ofsted judges as 'outstanding', schools 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, students, volunteers, parents, carers, visitors {and community users/hirers}. This includes anyone who uses and/or has access to, personal devices and technologies whilst on school site and those who have access to, and are users of, school devices and technologies, both in and outside of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site, and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place outside of the school but 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 the LA.

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](mailto: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.

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

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

Head	Mr A J Parkhurst
E-safety Coordinator /LEAD TEACHER of ICT	Ms B Jones
Network Manager/Technician	Woodlands School

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: <ul style="list-style-type: none"> <li>• Personal computers</li> <li>• Laptops</li> <li>• Tablets</li> <li>• 'Smart'/Mobile phones</li> <li>• 'Smart' watches</li> <li>• Cameras</li> <li>• USB sticks/flash drives</li> </ul>
Technology(ies)	Examples include but are not limited to: <ul style="list-style-type: none"> <li>• Internet search engines</li> <li>• Websites</li> <li>• Social media platforms, e.g. Facebook, Twitter, Instagram, Snapchat, WhatsApp, YouTube</li> <li>• Real time communications e.g. texts, chat rooms, email, instant messaging, Skype, FaceTime, video chat</li> <li>• On-line gaming, e.g. Xbox, PlayStation</li> </ul>

## **7. School Staff, Governors and Volunteers**

### **Acceptable Use Policy Agreements**

Before being granted access to school devices and technologies, all members of the school community are required to read and sign an Acceptable Use Policy Agreement (AUP), appropriate to their role and status in school.

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

### **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.

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

## **8. Students**

### **Acceptable Use Policy (AUP) for Students**

The AUP for students is signed in school. One is sent home to parents with a note on stating that if they don't return it they are agreeing to accept it.

A copy of the student AUP a note is on

Copies can be requested from the ICT coordinator if necessary.

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

### **Acceptable Use of Devices and Technologies: Students**

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

#### **Student breaches of the AUP**

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

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

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

## **9. Using non-School Equipment – ‘Bring Your Own Device/Bring Your Own Technology’ (BYOD/BYOT)**

No one is allowed to do this.

## **10. Security and passwords**

Passwords should be changed regularly and must not be shared.. 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. Data storage**

Only encrypted USB pens are to be used in school

## 12. Mobile phones, cameras and other devices

Camera mobile phones are not permitted in school. The only staff who are allowed school phones are the Headteacher, SBM and Family Support Worker.

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

## 13. Social Media and Networking

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

## 14. 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](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.

## 15. 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 incidents that come to the attention of school staff should be notified to the Headteacher via the school reporting mechanism set out in Appendix K, or, where applicable, via the Whistleblowing Policy.

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

Incidents that are of a concern under the Prevent duty should be referred to the 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.

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

## **16. Staff training and updates**

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

E-safety incidents and concerns are a standing item at staff briefings.

## **17. Communicating the E-safety Policy**

### ***Staff and the E-safety policy***

- All staff will be given a copy of the E-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 E-safety policy to students***

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

### ***Home-School Communication of E-safety information***

- The school website provides information on E-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.
- The school holds E-safety events to brief parents and carers about E-safety developments and policies as part of events such as 'Safer Internet Day'/event.

## **18. Shropshire Safeguarding Contact details:**

Local Authority Designated Officer (LADO)  
Emergency Duty Team

[lodo@shropshire.gov.uk](mailto:lado@shropshire.gov.uk)  
0345 678 9040

**19. Monitor & review**

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

## Appendix F: E-safety Roles & Responsibilities: List of duties

<p><b>Head/Principal</b></p>	<ul style="list-style-type: none"> <li>• Has overall responsibility for E-safety provision.</li> <li>• Has overall responsibility for data and data security</li> <li>• Ensures that the school uses an appropriate filtered Internet Service</li> <li>• Ensures that staff receive appropriate training to enable them to carry out their E-safety roles</li> <li>• Can direct the whole school community including staff, students and governors to information, policies and practice about E-safety.</li> <li>• Is aware of the procedures to be followed in the event of a serious E-safety incident.</li> <li>• Receives regular monitoring reports from the <b>E-safety Coordinator/Officer.</b></li> <li>• Ensures that there is a system in place to monitor and support staff who carry out internal E-safety procedures and reviews (e.g. Network Manager).</li> <li>• Oversees the administration of the staff Acceptable Use Policy Agreements and takes appropriate action where staff are found to be in breach.</li> </ul>
<p><b>E-safety Coordinator /Designated Safeguarding Lead/CPO/HEAD/LEAD TEACHER of ICT</b></p>	<ul style="list-style-type: none"> <li>• Takes day to day responsibility for E-safety issues and assumes a leading role in establishing and reviewing the school E-safety policies and supporting documents.</li> <li>• Ensures that the school is compliant with all statutory requirements in relation to the handling and storage of information.</li> <li>• Ensures that any recording, processing, or transfer of personal data is carried out in accordance with the <i>Data Protection Act 1998</i>.</li> <li>• Promotes an awareness of and commitment to E-safety throughout the school community.</li> <li>• Ensures that E-safety is embedded across the curriculum.</li> <li>• Is the main point of contact for students, staff, volunteers and parents who have E-safety concerns.</li> <li>• 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):             <ul style="list-style-type: none"> <li>- sharing of personal data</li> <li>- access to illegal/inappropriate materials</li> <li>- inappropriate on-line contact with adults/strangers</li> <li>- cyber-bullying</li> </ul> </li> </ul>

	<ul style="list-style-type: none"><li>• Ensures that all staff are aware of the procedures that need to be followed in the event of an E-safety incident.</li><li>• Ensures that an E-safety incident log is kept up to date.</li><li>• Liaises with school IT technical staff where necessary and/or appropriate.</li><li>• Facilitates training and provides advice and guidance to all staff.</li><li>• Communicates regularly with <b>SLT</b> to discuss current issues, review incident logs and filtering.</li></ul>
--	--

<p><b>Head of ICT/Lead teacher for ICT</b></p>	<ul style="list-style-type: none"> <li>• Oversees the delivery of the E-safety element of the Computing curriculum.</li> <li>• Communicates regularly with the E-safety coordinator.</li> </ul>
<p><b>Network Manager/Technician</b></p>	<ul style="list-style-type: none"> <li>• Oversees the security of the school ICT system.</li> <li>• Ensures that appropriate mechanisms are in place to detect misuse and malicious attack (e.g. firewalls and antivirus software).</li> <li>• Ensures that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.</li> <li>• Ensures that the school's policy on web-filtering is applied and updated on a regular basis.</li> <li>• Ensures that access controls/encryption exist to protect personal and sensitive information held on school-owned devices.</li> <li>• Ensures that users may only access the school networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed.</li> <li>• Reports any E-safety incidents or concerns, to the E-safety co-ordinator.</li> <li>• Keeps up to date with the school's E-safety policy and technical information in order to carry out the E-safety role effectively and to inform and update others as relevant.</li> <li>• Keeps up-to-date documentation of the school's E-security and technical procedures.</li> <li>• Keeps an up to date record of those granted access to school systems.</li> </ul>
<p><b>ALL Staff</b></p>	<ul style="list-style-type: none"> <li>• Read, understand and help promote the school's E-safety policies and guidance.</li> <li>• 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.</li> <li>• Report any suspected misuse or problem to the E-safety coordinator.</li> <li>• Maintain an awareness of current E-safety issues and guidance, e. g. through training and CPD.</li> <li>• Model safe, responsible and professional behaviours in their own use of technology.</li> <li>• Ensure that any digital communications with students are on a professional level and through school-based systems ONLY.</li> <li>• Ensure that no communication with students, parents or carers is entered into through personal devices or social media.</li> <li>• Ensure that all data about students and families is handled and stored in line with the principles outlined in the Staff AUP.</li> </ul>

<b>Teaching Staff</b>	<ul style="list-style-type: none"> <li>• Embed E-safety issues in all aspects of the curriculum and other school activities.</li> <li>• Supervise and guide students carefully when engaged in learning activities involving online technology (including extracurricular and extended school activities, where relevant).</li> <li>• 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.</li> </ul>
<b>Students / Students:</b>	<ul style="list-style-type: none"> <li>• Are responsible for using the school digital technology systems in accordance with the Student AUP Agreement.</li> <li>• Have a good understanding of research skills, the need to avoid plagiarism and to uphold copyright regulations.</li> <li>• Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.</li> <li>• Understand policies on the use of mobile devices and digital cameras, the taking and use of images and cyber-bullying.</li> <li>• 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.</li> </ul>
<b>Parents / Carers</b>	<p>Parents and carers are encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:</p> <ul style="list-style-type: none"> <li>• digital and video images taken at school events.</li> <li>• access to <b>parents' sections of the website/ Learning Platform</b> and on-line student/student records.</li> <li>• their children's personal devices in the school. <b>(where this is allowed)</b></li> </ul>
<b>External groups</b>	<p>Any external individual/organisation must sign an Acceptable Use Policy prior to using any equipment or the Internet within the school.</p>

## **Appendix G: 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 1998**

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

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

### **Freedom of Information Act 2000**

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a 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, connections staff fall in this category of trust). Any person having sexual intercourse with a child under the age of 13 commits the offence of rape.

## **Public Order Act 1986**

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

## **Obscene Publications Act 1959 and 1964**

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

## **Human Rights Act 1998**

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

- The right to a fair trial
- The right to respect for private and family life, home and correspondence

- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

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

### **The Education and Inspections Act 2006**

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

### **The Education and Inspections Act 2011**

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

### **The Protection of Freedoms Act 2012**

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

### **The School Information Regulations 2012**

Requires schools to publish certain information on its website:  
<https://www.gov.uk/guidance/what-maintained-schools-must-publish-online>

### **Serious Crime Act 2015**

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

**Appendix H: E-Safety Incident Reporting Log**

<i>Date</i>	<i>Time</i>	<i>Incident</i>	<i>Action Taken</i>		<i>Incident Reported By</i>	<i>Signature</i>
			<i>What?</i>	<i>By Whom?</i>		

## **Appendix I: Examples of potential E-safety concerns (Students)**

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

### ***Inappropriate material accessed on school computers***

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

Students are taught that they are not at fault if they see or come across something online that they find worrying or upsetting and are encouraged to alert staff to any inappropriate content. The staff member should report the incident to the **E-safety Co-ordinator** who will log the problem and liaise with the **Network Manager** to make any necessary adjustment to filter settings.

### ***Abusive messages on school computers***

Students who receive abusive messages over school systems will be supported, and advised not to delete messages. The **E-safety Co-ordinator** will be informed and a formal process of investigation initiated.

### ***Parent/Carer/Guardian reports of cyber bullying***

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

### ***Student disclosure of concerns or abuse***

All staff receive Safeguarding and 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 and, where appropriate, the **E-safety Coordinator**.

### ***Student reporting outside school***

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

### ***Allegations against staff***

Allegations involving staff should ordinarily be reported to the Headteacher or through the Whistleblowing Policy. If the allegation is one of abuse then it should be handled

in line with the statutory DfE guidance: 'Dealing with allegations of abuse against teachers and other staff'. If necessary local authority's LADO should be informed.

Evidence of incidents must be preserved and retained and where necessary, the LADO informed.

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

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

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

Remedial action relating to potential sanctions is at the discretion of school management as suggested as below.

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

### Level 1 breaches

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

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

### Level 2 breaches

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

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

### Level 3 breaches

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

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

## Other safeguarding actions

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site
2. Inform 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]

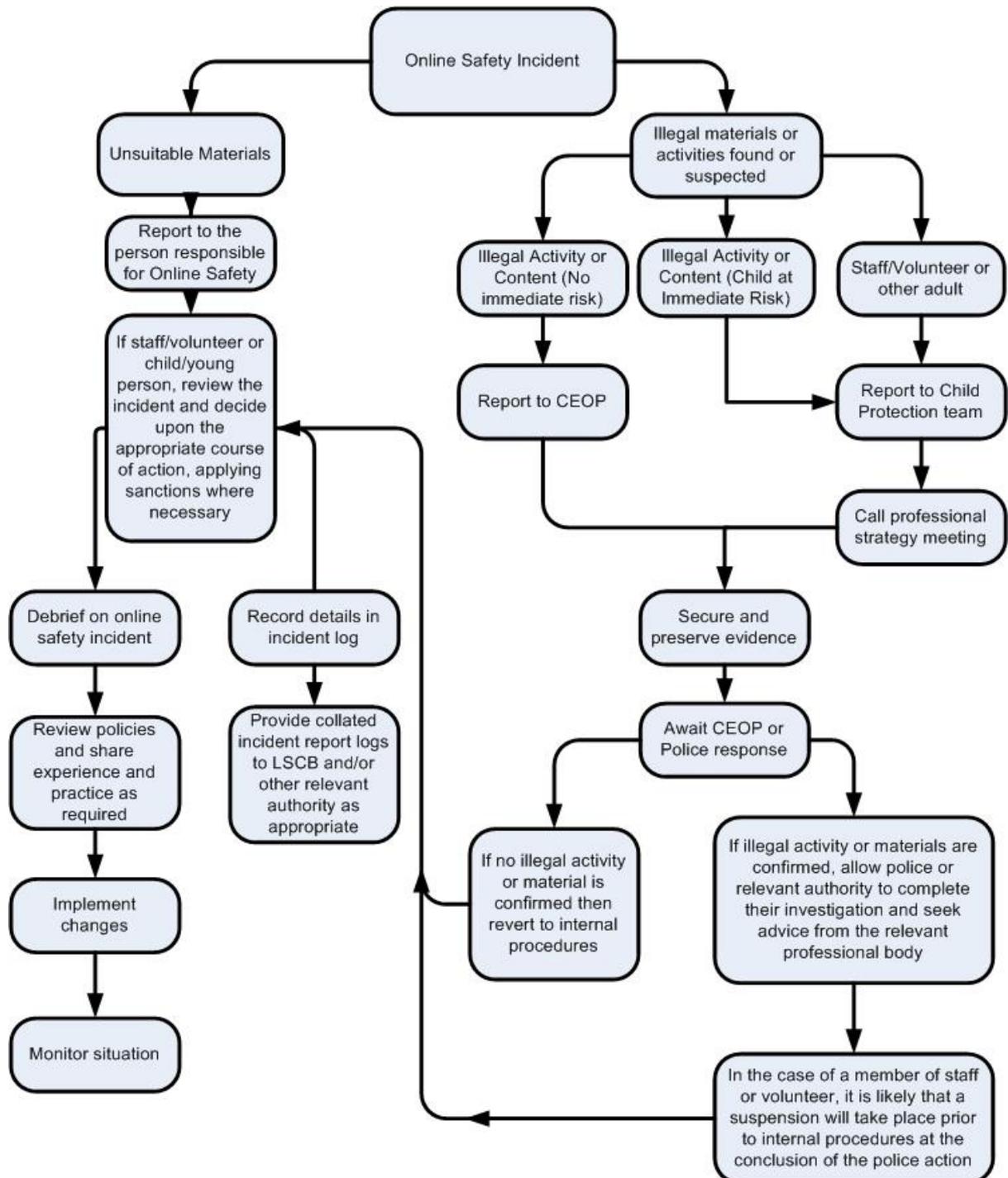
## Other safeguarding actions:

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.

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



## Appendix L: Cyberbullying: further advice and guidance

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

- **Abusive comments**, rumours, gossip and threats made over the internet or using digital communications – this includes internet trolling.
- **Sharing pictures**, videos or personal information without the consent of the owner and with the intent to cause harm and/or humiliation.
- **Hacking** into someone’s email, phone or online profiles to extract and share personal information, or to send abusive or inappropriate content whilst posing as that person.
- **Creating specific websites or ‘pages’ on the Internet** that negatively target an individual or group, typically by posting content that intends to humiliate, ostracise and/or threaten.
- **Blackmail**, or pressurising someone to do something online they do not want to do such as sending a sexually explicit image.

### Cyberbullying: Advice for headteachers and school staff

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

[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/374850/Cyberbullying\\_Advice\\_for\\_Headteachers\\_and\\_School\\_Staff\\_121114.pdf](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](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/623895/Preventing_and_tackling_bullying_advice.pdf)