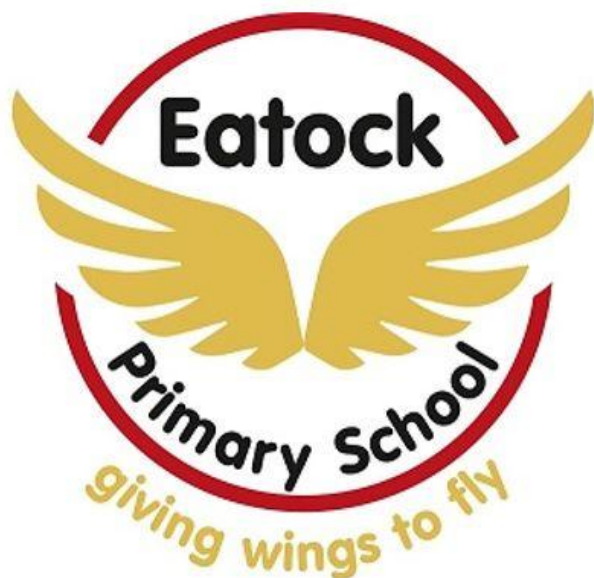


Eatock Primary School **Online Safety Policy**



2025 - 2026

Adapted from Bolton LA School Online Safety Template Policy

Safeguarding in Education Team
Bolton Safeguarding Children 

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of the school's ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of pupils 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 incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix Electronic Devices – Search and Deletion). In the case of both acts, action can only be taken over issues covered by the school's Behaviour Policy. This policy has been updated inline with KCSiE 2025.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online behaviour that take place out of school.

Contents	Page(s)
Development, Monitoring and Review of this Policy	4
Schedule for Development, Monitoring and Review	4
Online Safety Audit	5
Roles and Responsibilities: The Governors	6
Roles and Responsibilities: Head teacher and Senior Leaders	6
Roles and Responsibilities: Computing / Online Safety subject leaders	7
Roles and Responsibilities: Network Manager / Technical staff	7
Roles and Responsibilities: Teaching and Support Staff	7 - 8
Roles and Responsibilities: Pupils	8
Roles and Responsibilities: Parents / Carers	8
Roles and Responsibilities: Community Users	8
The School's Aims for delivering Online Safety Education	9
Technical – infrastructure / equipment, filtering and monitoring	10 - 11
Bring your own devices (BYOD)	12
Use of digital and video images	13
Data protection	14
Use of Cloud systems Permission	14
Social Media - Protecting Professional Identity	14 – 15
User Actions - unsuitable / inappropriate activities	15 – 16
Responding to incidents of misuse	17 – 21
Appendices -	
Appendix 1: Pupil Acceptable Use Policy Agreements – EYFS to Year 6	23 - 27
Appendix 2: Staff and Volunteers Acceptable Use Policy Agreement	28-30
Appendix 3: Community Users Acceptable Use Agreement	31-32
Appendix 4: Appendix 4: Online Safety Incident Flowchart	33
Appendix 5: Support Contacts for Bolton Schools	34
Appendix 6: Legislation	35-38
Appendix 7: Useful resources, additional guidance and contacts	39-42
Appendix 8: Glossary of terms	43

Development, Monitoring and Review of this Policy

This Online policy has been developed by the Headteacher, Senior Leaders and Computing Subject leaders. This policy is reviewed and amended where appropriate annually (at least) by teachers, TAs and the governors. Consultation with the whole school community (e.g. Premier Sport) has taken place through a range of formal and informal meetings. In addition to this policy, staff, parents and the school community should also read and follow the Technology and Remote Learning Policy. This policy was reviewed and amended September 2025.

Schedule for Development, Monitoring and Review

This Online policy was approved by the School Effectiveness Governing Committee on:	30 th January 2026
The implementation of this Online policy will be monitored by the:	Computing Subject Leads: Mrs G Thomas, Headteacher Mrs V Hickman and the SLT.
Monitoring will take place at regular intervals:	Termly, as part of subject leadership monitoring carried out by Mrs G Thomas. Online Safety Governor drop-in observation of online safety teaching
The Governing will receive a report on the implementation of the Online policy generated by the monitoring group (which will include anonymous details of Online incidents) at regular intervals:	Termly update given at the School Effectiveness Committee Meetings Annual update with Online Safety governor – updates with KCSiE (25.11.25)
The Online Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to Online or incidents that have taken place. The next anticipated review date will be:	January 2026 The review will be carried out initially by Online Safety Lead: Mrs G Thomas and will be ratified by the Headteacher Victoria Hickman and the School Effectiveness governors.
Should serious Online incidents take place, the following external persons / agencies should be informed:	Depending on the nature and severity of the incident, the following external agencies may be informed: SICT Computing lead (Deb Lyons), Integrated Front Door or the Greater Manchester Police / Manchester Prevent Coordinator.

The school will monitor the impact of the policy using:

- A log of reported incidents (CPOMS)
- The school's Computing Action Plan (through termly evaluations)
- Surveys / questionnaires of pupils (paper version), parents / carers (online) and staff

Online Safety Audit Checklist

This quick self-audit, completed by the computing leaders and senior leadership team assesses whether the online safety basics are in place.

Does the school have an Online Safety Policy that complies the latest guidance?	Yes
Date of lastest review:	October 2025
The Policy was agreed by governors on:	1 st October 2024
The Policy is available for staff:	Yes – all staff / Policies Eatock
The Policy is available for parents:	Yes – School website
The Designated Safeguarding lead is:	Mrs Victoria
The Online Safety leader is:	Mrs G Thomas
Has Online Safety training been provided for staff?	Yes. All Staff complete the annual Online Safety Training (National College) in September. Annual KCSiE update also includes Online Safety updates.
Has Online Safety training been provided for pupils?	Yes - through assemblies and lessons.
Are parents sent - An agreement that their child will comply with the School Online Safety rules? - The Acceptable User Policy (AUP) for pupils? - An agreement that their children's work & pictures may be displayed on the internet.	Yes. The Acceptable User Policies (AUP) for pupils (year group specific) are electronically shared with parents / carers every September.
Has the school got an AUP / Online Safety Rules age appropriate for pupils?	Yes – displayed in classes and computer suite.
Is the AUP / Online Safety rules displayed in all rooms with computers?	Yes with children's initials accepting the agreement / online safety promise.
Internet access is provided by an educational Internet service provider and complies with DfES requirements for safe and secure access?	Yes – provided by the LA Bolton SICT SLA.
Has an ICT security audit been initiated by SMT, possibly using external expertise?	Yes – provided by the LA Bolton SICT SLA.
Is personal data collected, stored and used according to the principles of Data Protection Act?	Yes – see school's GDPR policy.

Members of our school that have had inputted directly with this policy	
Head Teacher	√
Member of Senior Leadership Team	√
Online Safety / Computing lead	√
Designated Safeguarding lead	√
Linked Governor	√
Member of TA staff	√
School Council Representation	√

Roles and Responsibilities.

The following members of staff and the community take an active role in following and reviewing the school's online safety policy:

- Governors
- Head teacher
- Computing Subject leaders
- Technical Staff (SICT)
- Teachers and TAs
- Safeguarding leads
- Pupils
- Parents / Carers
- Community Users

Governors

The Governors are responsible for the approval of the Online Policy and for reviewing the effectiveness of the policy. This will be carried out by the School Effectiveness Committee. During the termly committee meetings, the governors will receive regular updates regarding the curriculum and any online concerns / incidents. Mr Kevin Lever, a member of the School Effectiveness Committee, is the school's Online Safety Governor. Mrs Linda Thomas, who is the Safeguarding Governor, is also a member of the School Effectiveness Committee.

The role of the Online Safety Governor includes:

- Termly updates with the computing leader
- Termly report of online incidents reported (CPOMS)
- reporting online safety information to other governors – this will be carried out through the sharing of the School Effectiveness Committee meeting minutes at the Full Governing Body Meetings

Head teacher and Senior Leaders:

The Head teacher has a duty of care for ensuring the safety (including Online) of members of the school community, though the day to day responsibility for Online Safety will be delegated to the Computing subject leader.

- The Head teacher and members of the Senior Leadership Team are aware of the procedures to be followed in the event of a serious online allegation being made against a member of staff. (See flow chart on dealing with Online incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR / other relevant body disciplinary procedures);
- The Head teacher and DHT are responsible for ensuring that the Computing subject leader receives suitable training to enable them to carry out their Online Safety roles and to train other members of staff;
- The Head teacher and DHT ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online monitoring role – see the school's strategic monitoring overviews;
- The Senior Leadership Team will receive regular monitoring reports from the Computing subject leaders – termly evaluations of the computing action plan and impact statement.
- The Designated Safeguarding Lead and Deputy Lead have up-to-date DSL training that includes online issues. They are aware of the potential for serious child protection / safeguarding issues to arise

from sharing of personal data; access to illegal / inappropriate materials; inappropriate on-line contact with adults / stranger; potential or actual incidents of grooming; and cyber-bullying

Computing / Online Safety subject leader:

- take day to day responsibility for Online issues and has a leading role in establishing and reviewing the school's online policies;
- ensure that all staff are aware of the procedures that need to be followed in the event of an online incident taking place;
- provide training and advice for staff;
- liaise with the Local Authority / relevant body;
- liaise with school technical staff;
- receive reports of online incidents and creates a log of incidents to inform future Online developments;
- regularly meets with Online Governor to discuss current issues, review incident logs;
- attend the School Effectiveness Committee meeting to update the governors;
- report regularly to Senior Leadership Team.

Network Manager / Technical staff:

The schools' onsite technician (SICT technician) is responsible for ensuring:

- the school's technical infrastructure is secure and is not open to misuse or malicious attack;
- the school meets required online technical requirements and any Local Authority or other relevant Online Policy / Guidance that may apply;
- users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed;
- the filtering policy (Bolton LA's SICT policy), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person - this is managed through Bolton's LA SICT SLA;
- they keep up to date with online technical information in order to effectively carry out their Online role and to inform and update others as relevant;
- the use of the school's network, internet, remote access and email is regularly monitored in order that any misuse or attempted misuse can be report to the Head teacher, DHT or Computing subject leaders for investigation and action. This monitoring is mainly carried out by the Local Authority and communication between SICT and the school's technician will inform school;
- the monitoring of software and systems are implemented and updated as agreed in school policies.

Teaching and Support Staff

Are responsible for ensuring that:

- they follow the school's safeguarding policy in relation to online safety, including updates within the KCSiE document which includes safeguarding children both offline and online.
- they have an up-to-date awareness of online matters and the school's Online policy and practices;
- they have read, understood and signed the Staff Acceptable Use Policy (AUP);
- they report any suspected misuse or problem to the Headteacher, DHT or computing subject leaders for investigation and action;
- all digital communications with pupils, parents / carers should be on a professional level and only carried out using official school systems;
- Online issues are embedded in all aspects of the curriculum and other activities;
- pupils understand and follow the school's Online through the class Online Safety Promises;
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices;
- during lessons where internet use is pre-planned, pupils should be guided to sites that have been checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Pupils:

- are responsible for using the school digital technology in accordance with the Pupil Acceptable User Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking or use of images and on cyber-bullying.
- should understand the importance of adopting good online practice when using digital technologies inside and out of school and realise that the school's Online Policy covers their actions out of school.
- should understand the seriousness of inappropriate online behaviour (as outline in KCSiE 2025)

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to:

- use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national and/or local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in promoting good online practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parent / carers sections of the website
- their children's personal devices in the school (in Years 5 and 6)

Community Users

Community Users, such as Care Club, who access school systems, including the school's internet and website, will be expected to sign a Community User AUA before being provided with access to school systems. See appendix for this agreement.

The School's Aims for delivering Online Safety Education:

The education of online safety for our children is an essential part of the school's computing curriculum and aims to provide children with the knowledge and skills that will enable them to avoid online risks and build their resilience. Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. The Online safety curriculum (outlined within the computing curriculum and computing progression of skills) is broad, relevant and provide progression, with opportunities for creative activities.

Online safety will be taught in the following ways:

- Through planned online safety lessons as part of Computing lessons and across other curricular subjects where appropriate, such as PSHE (including extremism and radicalisation) and should be regularly revisited;
- Key Online safety messages will be shared with the children in class (through discussions / PSHE / Circle time) and through assemblies
- All children will be taught to be critically aware of the materials / content they access on-line
- Children will be taught and be guided to validate the accuracy of information and will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet – age appropriate.
- Through the understanding and agreement of class online safety promises, which are signed and displayed in classes or class computer areas.

Staff model and ensure online safety through their teaching practice, for example:

- Staff act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where Internet use is pre-planned, the children are guided to sites checked as suitable for their use and follow the school's procedure for dealing with any unsuitable material that is found in Internet searches. When children are allowed to freely search the Internet (i.e. in Years 4, 5 and 6), staff should be vigilant in monitoring the content of the websites visited.

The school also aims to promote online safety amongst parents / carers and the wider community. In order to provide information and awareness to parents and carers, a range of lines of communication in order to reach as many parents / carers as possible, for example:

- Parent Online Safety workshops
- Regular Online Safety updates on the school's Face Book page

- High profile events / campaigns e.g. Safer Internet Day
- Reference to the Online Safety Zone within the school's website
- Online safety publications, such as DITTO magazine.

In order to provide information and awareness to the wider community, regular Online Safety updates on the school's Face Book page are accessible for all Face Book users, as they are public, as is the school website which provides information for the wider community.

Training:

- All staff receive Online Safety training and understand their responsibilities, as outlined in this policy. Governors and the wider community are also invited to participate in the training that maybe relevant to them.
- The Computing Subject Leaders identify training needs through ongoing monitoring and arrange for the necessary training to be delivered; this includes formal and informal online safety training, which is updated and reinforced regularly.
- Key online safety messages are regularly shared which informs future teaching and policy amendment where appropriate.
- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Agreements.
- The Safeguarding Lead and Computing leaders receive regular online safety updates via LA network groups and through attendance at external training events.

Technical – infrastructure / equipment, filtering and monitoring

- The school has a managed ICT service provided by the Local Authority (LA). The school work in partnership with the LA to ensure that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. Servers, wireless systems and cabling are securely located and physical access is restricted. All technical users have clearly defined access rights to school technical systems and devices.
- All users across KS1 and KS2 have their own personal username and secure password. The computing subject leaders will keep an up to date record of users and their usernames and a copy will be given to class teachers – saved on the school network. The children are responsible for the security of their username and password. Children across EYFS have a group username and password which relates to their cohort.
- The 'administrator' passwords for the school ICT system, used by the LA technicians, must also be available to the Headteacher and DHT and kept in a secure place (e.g. school safe)

- The computing leaders and Headteacher are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider - this is managed by the LA. Requests to make filtering changes are passed onto the computing leaders, which are then checked by the Headteacher before asking the LA, via the school's technician.
- The school has enhanced / differentiated user-level filtering which is administered by the LA, via the school's technician.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Staff, children and other users (such as student teachers) understand their responsibilities to report online safety incidents. Teachers and other users (not children) know to report any potential risks / unsuitable material being used to the computing leaders or abuse that has been disclosed or suspected to the school's designated safeguarding lead, Mrs Thomas, or deputy lead in her absence, and understand that processes must be followed rigorously. Children know to report online safety incidents to their class teacher, who then passes it on. The school actively seeks support from other support agencies (e.g. local authority (SICT) and MASSS) in dealing with online safety issues. Reports are logged for future auditing / monitoring. Staff understand that some online safety incidents, such as PREVENT are reported directly to the police and know where to find the contact numbers for this. Staff know that all online safety safeguarding and behaviour issues need to be logged in CPOMs.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly by the LA school technicians. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests". Guests, such as trainee teachers, are given a unique login and password with limited access to network drives. Supply teachers and visitors (such as dental nurse using a school laptop) use a 'guest' login and password, which only provides access to the device, the Internet and one network drive that is specifically for guests and does not contain any personal or confidential information. It is the responsibility of the class TA to login onto the computer and lock it when not in class, e.g. at break times and lunchtimes.
- An agreed policy is in place regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on school devices that may be used out of school. This is outlined in the user agreements – see appendices 1, 2 and 3. Staff computers, laptops and mobile devices are to be used by members of staff for school use only.

The agreement also forbids staff from downloading executable files and installing programmes on school devices without permission from the Headteacher.

- An agreed policy is in place regarding data protection under the GDPR legislation and school policy. The use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices is allowed however must not contain personal data. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. All teachers have a remote access device to access pupil data or documents containing personal.

Bring Your Own Device (BYOD)

What does “bring your own device” mean?

For school use, ‘Bring your own device’ (often shortened to BYOD) is the term used to describe the connection of a personally-owned device (such as a laptop, smartphone or tablet) to a Wi-Fi network provided by school. The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. Each class have access to mobile devices, such as iPads and iPods and therefore there is not a need for staff to bring in their own devices, except for rare circumstances. In this instance, it must be agreed with the Headteacher beforehand and considerations will need to include levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. These considerations would be discussed with the LA’s technician in good time to ensure the necessary safety steps / provision has been put in place.

Should it be agreed for staff or visitors to bring in their own device, the following actions must be followed:

- All users are provided with and accept the Acceptable Use Agreement (A record of this will be kept)
- Mobile devices allowed into school must be used on the school’s secure network, i.e. use of 3G/4G networks is forbidden.
- The school adheres to the Data Protection Act principles
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school’s normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
- Pupils bringing mobile phones / mobile devices into school, must give them to the class teacher at the beginning of the day and the device will be returned at the end of the day. Pupils must not use their own mobile phones / mobile devices in school.
- School users must keep their passwords secure and not share with non-registered users.
- School does not take responsibility for lost, stolen, or damaged personal devices.

Violations of Acceptable Use Policy

Violations of this policy may have disciplinary repercussions, including: suspension of network, technology, or computer privileges, notification to employer, suspension from school and school-related activities, legal action and/or prosecution.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons. Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. The school will comply with the GDPR legislation and request parents / carers permission before taking and publishing images of their children.

The school will ensure the following measures are in place to ensure safe use of digital and video images:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases child protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission. In school, pupils must not share, publish or distribute images of others at all.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog and names must not be used in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or any marketing purposes.

Data Protection

Personal data will be recorded, processed, transferred and made available according to GDPR legislation, which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Use of Cloud Systems Permission

Microsoft Office 365 does not require this parental consent. School also uses iCloud in some instances (primarily for app storage), however photos taken on iPads and iPods are not backed up on the cloud – they are downloaded to the school system and deleted off the device.

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes, this policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Expectations for teachers' professional conduct are also set out in 'Teachers Standards 2012' and the Ofsted's Online framework 2012 reviews how a school protects and educates staff and pupils in their use of technology, including what measures would be expected to be in place to intervene and support should a particular issue arise.

The school outlines the following measures for all members of staff, governors and volunteers to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- It is not appropriate for representatives of the school to have pupils for which they have a duty of care who are under the age of 18 as 'friends' on such sites.
- Staff, governors and volunteers who have accounts on social networking sites must ensure the highest level of security is in place and that they do not either accept or make a friend request to any person under the age of 18 years to whom they have acted 'in a position of trust' (including ex-pupils), or someone who is over the age of 18 to whom they are still acting 'in a position of trust', i.e. sixth form pupils.
- No reference should be made in social media to pupils, parents / carers or school staff
- Staff, governors and volunteers should not engage in online discussion on personal matters relating to members of the school community personal opinions should not be attributed to the school or local authority

- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

When using social media, staff, governors and volunteers must ensure they adhere to the following expectations:

- behave online in a professional and appropriate manner
- be a 'responsible user' and stay safe whilst using technology
- ensure ICT systems that belong to school are protected from accidental or deliberate misuse
- always have the duty of care to pupils as their main priority
- ensure the school is not exposed to legal and governance risks

Should members of Staff, governors or volunteers become aware of unacceptable online / social media behaviour of other members of Staff, governors and volunteers, they must report it to the school's designated safeguarding lead, Mrs. Thomas, or deputy designated safeguarding lead.

Additional guidance relating to social media can be found in the school's Social Networking Policy.

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying is also be banned and could lead to criminal prosecution. There are also a range of other online activities that may be legal but are inappropriate in school, either because of the age of the users or the nature of those activities.

The activities referred to in the following section have been identified as inappropriate in school and users defined below should not engage in these activities in school or outside school when using school equipment or systems.

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X

comments that contain or relate to:		Acceptable	Acceptable at	Acceptable for	Unacceptable	Unacceptable
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)		X				
On-line gaming (non educational)			X			
On-line gambling					X	
On-line shopping / commerce			X			
File sharing			X			
Use of social media			X			
Use of messaging apps			X			
Use of video broadcasting e.g. YouTube			X			

Responding to incidents of misuse:

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, follow the procedure outlined in the Online Safety Incident Reporting flowchart (right hand side of the flowchart) – Appendix 4 - report immediately to the police.

Other Incidents

It is expected that all members of the school community will be responsible users of digital technologies and will understand and follow school's policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, the following steps should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, appropriate action will be required and could include the following:

- Internal response or discipline procedures
- Involvement by Local Authority
- Police involvement and/or action

If content being reviewed includes images of child abuse, the monitoring should be halted and referred to the police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act

- criminally racist material
- other criminal conduct, activity or materials.

In addition, it is important to isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school (and possibly the police) and will demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Inappropriate behaviour

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. Should staff become aware of inappropriate use, they should take appropriate action as outlined below. **A log must also be made on CPOMS.** Incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as stated within the school's Behaviour Policy and Code of Conduct Policy.

Pupils

Actions / Sanctions

Incidents:	Refer to class teacher	Refer to Computing leaders	Refer to Head teacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons	X				X			X	
Unauthorised use of mobile phone / digital camera / other mobile device	X					X			X
Unauthorised use of social media / messaging apps / personal email	X	X			X	X			X
Unauthorised downloading or uploading of files	X	X	X		X	X			X

Allowing others to access the school network by sharing username and passwords	X	X				X			X
	Refer to class teacher	Refer to Computing leaders	Refer to Head teacher	Refer to Police	Refer to technical support staff for action re filtering /	Inform parents / carers	Removal of network / internet access rights	Warning	Sanction e.g. detention / exclusion
Attempting to access or accessing the school network, using another student's / pupil's account	X	X				X			X
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X			X			X
Corrupting or destroying the data of other users	X	X	X			X			X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X			X
Continued infringements of the above, following previous warnings or sanctions	X	X	X			X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X			X	X		X
Using proxy sites or other means to subvert the school's filtering system	X	X	X		X	X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X	X		X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X		X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X	X		X	X		X

Staff

Actions / Sanctions

Incidents:	Refer to line manager	Refer to Head teacher	Refer to Local Authority Designated Officer & HR	Refer to Police	Refer to Technical Support Staff for action	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Inappropriate personal use of the internet / social media / personal email	X	X				X		
Unauthorised downloading or uploading of files	X	X			X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X			X	X		
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X			X			X
Deliberate actions to breach data protection or network security rules	X	X			X			X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X			X			X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X						X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	X	X						X
Actions which could compromise the staff member's professional standing	X	X						X

	Refer to line manager	Refer to Head teacher	Refer to Local Authority Designated	Refer to Police	Refer to Technical Support Staff for	Warning	Suspension	Disciplinary action
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X				X		
Using proxy sites or other means to subvert the school's filtering system	X	X			X			X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X			X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X				X
Breaching copyright or licensing regulations	X	X		X				X
Continued infringements of the above, following previous warnings or sanctions	X	X		X				X

The KCSiE 2025 guidelines, updated on September 1, 2025, for schools in England, expand the online safety risks list to include **misinformation, disinformation (including fake news), and conspiracy theories**. The guidelines also reference new Department for Education (DfE) resources on **generative Artificial Intelligence (AI), filtering and monitoring**, and a self-assessment tool to help schools manage online risks effectively.

Key Changes to Online Safety in KCSiE 2025

- **Expanded list of harmful content:**

The updated guidance explicitly names misinformation, disinformation (including "fake news"), and conspiracy theories as risks that schools must address under their online safety duties.

- **New resources:**

The DfE has provided links to new guidance and tools for schools, including a self-assessment tool for filtering and monitoring systems and information on cybersecurity standards (Provided by Bolton SICT).

- **Focus on generative AI:**

The new guidelines include updated advice on how schools should approach the challenges and opportunities presented by generative AI (see AI Policy).

- **A whole-school approach:**

The document emphasizes the need for schools and colleges to take a whole-school approach to online safety, involving all staff, governors, volunteers, and parents in keeping children safe online.

Appendix 1: Pupils Acceptable Use Policy Agreement



EYFS Technology Agreement

 My Learning Using technology @school 	My conduct as a Digital Citizen • I will be respectful when I use a school device (PCs, laptops, tablets/ipads) for my learning and tell a teacher if something is not working properly. • I will ask a teacher before using a device and ask for help if I can't work the device. • I will only use activities that a teacher has told me to use. • I will ask a teacher if I am not sure what to do or think I have done something wrong. • I can talk about my digital footprint and will try to use what I have learned about Online Safety in school. • I know that there are rules that I need to follow to help me keep safe and healthy online at school when using technology. • I will only use the internet when the teacher says I can. • I will tell my teacher if I see something or somebody has made me feel sad, uncomfortable, embarrassed, or upset on the screen. 
 Using technology @home	My online world content • I know that there are rules that I need to follow to help me keep safe and healthy online at home when using technology. • I will tell a trusted adult if I see something or somebody has made me feel sad, uncomfortable, embarrassed, or upset on the screen.

I understand that I need to be respectful when I use a school device.

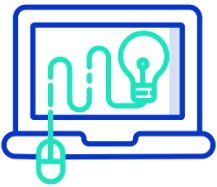
Year 1 and Year 2 Technology Agreement

 My Learning Using technology @school 	My conduct as a Digital Citizen • I will be respectful when I use a school device (PCs, laptops, tablets/ ipads) for my learning and tell a teacher if I am struggling or something is not working properly. • I know I need to follow our online safety rules to help me keep safe and healthy online at school when using technology. • I will only use activities that my teacher has told or allowed me to use. • I will be kind online, so I do not upset my friends. • I can talk about my digital footprint and will use what I have learned about Online Safety in school to search safety. • I will tell my teacher if I see something or somebody has made me feel sad, uncomfortable, embarrassed, or upset on the screen.
 Using technology @home	My online world content • I understand that certain sites and games have age restrictions to keep me safe. • I understand that by accessing such sites and games, I may be putting myself at risk of cyberbullying. • I will tell a trusted adult if I see content or somebody has made me feel sad, uncomfortable, embarrassed, or upset on the screen. My online world contact • Where I have my own username and password, I will keep it safe and secret. • I will not share personal information about myself when on-line (names, addresses, telephone numbers, age, gender, school details) • I will tell a trusted adult if I see something or somebody has made me feel sad, uncomfortable, embarrassed, or upset on the screen.

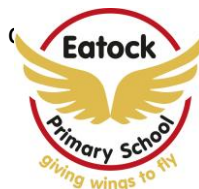
- I understand that this agreement will help me to stay safe and I agree to follow these rules.
- I also understand that I must behave respectfully and kind online to everyone wh



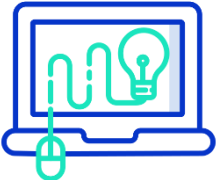
Year 3 and Year 4 Technology Agreement

 My Learning	- I will be respectful when I use a school device (PCs, laptops, tablets/ ipads) for my learning and tell a teacher if something is not working properly or I am struggling. My School Accounts - I will keep my usernames and passwords safe and secure - I will not share them. - I will not use anyone else's username and password. - I will only use apps, programs, or websites that my teacher has told me to use. - I will save only schoolwork on the school network.
 Using technology @school	My conduct as a Digital Citizen - I know that I can talk to my teachers about my digital footprint and if I see content or somebody has made me feel sad, uncomfortable, embarrassed, or upset on the screen, I can tell them. - I will respect other people's work and property and will not access, copy, delete any other user's files. - I know that I should check the content on websites as not everything is real or true.
 Using technology @home 	My online world content - I understand that certain sites and games have age restrictions to keep me safe. - I understand that by accessing such sites and games, I may be putting myself at risk of accessing inappropriate content and cyberbullying. - I will tell a trusted adult if I see content or somebody has made me feel sad, uncomfortable, embarrassed, or upset on the screen. My online world contact - I will be aware that new friends made online may not be who they say there. - I will be aware of what information cannot be shared between my friends. - I will be polite and responsible when I communicate with others online. - I will not use inappropriate language and I understand that others may have different opinions than me. My online world conduct - I understand that spending too much time online is not always good for me. - I understand that content I share online can still be there even after I have deleted it. - I will tell a trusted adult if I see content or somebody has made me feel sad, uncomfortable, embarrassed, or upset on the screen. - With the help of a trusted adult I will report any inappropriate content, messages or anything that makes me feel uncomfortable online, using the app/social media reporting tool or other online support agencies e.g. CEOP, Childline, Barnardos.

- I understand that this agreement will help me to stay safe and I agree to follow these rules.
- I also understand that I must behave respectfully and kind online to everyone when I



Year 5 and Year 6 Technology Agreement

 My Learning	• I will be respectful when I use a school device (PCs, laptops, tablets/ipads) for my learning and tell a teacher if something is not working properly or I am struggling. My School Accounts • I will keep my usernames and passwords safe and secure - I will not share them. • I will not use anyone else's username and password. • I will only use apps, programs, or websites that my teacher has told me to use. • I will log off or shut down a computer when I have finished using it.
 Using technology @school	My conduct as a Digital Citizen • I know that I can talk to my teachers about my digital footprint and can report any unpleasant or inappropriate content, messages or anything that makes me feel uncomfortable when I see it online to a trusted adult. • I know that some websites may present 'opinions' as 'facts'; whilst the popularity of an opinion or the personalities of those promoting it does not necessarily make it true, fair or perhaps even legal. • I will respect other people's work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission. • I will not take or distribute images of anyone without their permission.
 Using technology @home 	My online world content • I understand that certain sites and games have age restrictions to keep me safe. • I understand that by accessing such sites and games, I may be putting myself at risk of accessing inappropriate content and cyberbullying. • I will tell a trusted adult if I see content or somebody has made me feel sad, uncomfortable, embarrassed, or upset on the screen. My online world contact • I will be aware that new friends made online may not be who they say there. • I will be aware of what information cannot be shared between my friends. • I will be aware of regularly checking privacy on apps to keep me safe. • If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me. My online world conduct • I understand that spending too much time online is not always good for me. • I will be polite and responsible when I communicate with others online. • I will not use inappropriate language and I understand that others may have different opinions than me. • I understand that content I share online can still be there even after I have deleted it. My online world commerce • I understand that there are some sites that have a high risk of me accessing content such as online gambling, inappropriate advertising, phishing and or financial scams. • With the help of a trusted adult I will report any inappropriate content, messages or anything that makes me feel uncomfortable online, using the app/social media reporting tool or other online support agencies e.g. CEOP, Childline, Barnardos.

- I understand that this agreement will help me to stay safe and I agree to follow these rules.

- I also understand that I must behave respectfully and kind online to everyone when online.

Notes for School

Good Practice

At the beginning of a term, to review as part of a lesson when using technology.

To have a A3 class agreement on display so it can be referred during lessons where technology is being used.

This paragraph can be included when sending online safety updates home.

Parents / Carers:

Please encourage your child/children to adopt safe use of the internet and their devices at home.

Throughout the year your child/children will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

The school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and IT systems. The school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

If you have any concerns over your child/children's online safety experience do not hesitate to contact school for advice.

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The Internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe Internet access at all times.

This Acceptable Use Policy is intended to ensure:

- staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers have good access to ICT to enhance their work, to enhance learning opportunities for pupils' learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the pupils in my care in the safe use of ICT and embed online safety in my work.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, iPods, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school. Refer to actions and sanctions of inappropriate use within the Online Safety Policy.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- 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 not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident that I become aware of to the appropriate person. Refer to actions and sanctions of inappropriate use within the Online Safety Policy.
- I will be professional in my communications and actions when using school ICT systems.

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- 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 ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. Refer to the School's Online Safety Policy.
- I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website, Facebook) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies, i.e. for educational purposes to share / celebrate learning with parents /carers with their permission or to enhance learning with the permission of the headteacher.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. I will protect personal email addresses / mobile phones / social networking sites for such communications.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I will not support or promote extremist organisations, messages or individuals.
- I will not give a voice or opportunity to extremist visitors with extremist views.
- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.

To ensure safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc.) 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. Refer to BYOD section of the School's Online Safety Policy.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies, including the school's GDPR policy.
- I will not try to upload, download or access any materials that are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.

- I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up Internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless permission has been given from the Headteacher.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School's Personal Data Policy (GDPR). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the Internet in my professional capacity or for school sanctioned personal use:

- 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 understand that I am responsible for my actions in and out of the school:

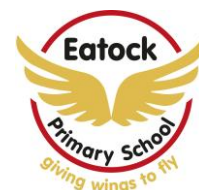
- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. See Actions / sanctions of inappropriate use section within the School's Online Safety Policy.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date



Appendix 3: Acceptable Use Agreement for Community Users

This Acceptable Use Agreement is intended to ensure:

- community users of school digital technologies will be responsible users and will stay safe while using these systems and devices
- school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- users are protected from potential risk in their use of these systems and devices

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school.

- I understand that my use of school systems and devices and digital communications will be monitored.
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work without permission from the Headteacher.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission from the Headteacher to do so.
- I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.

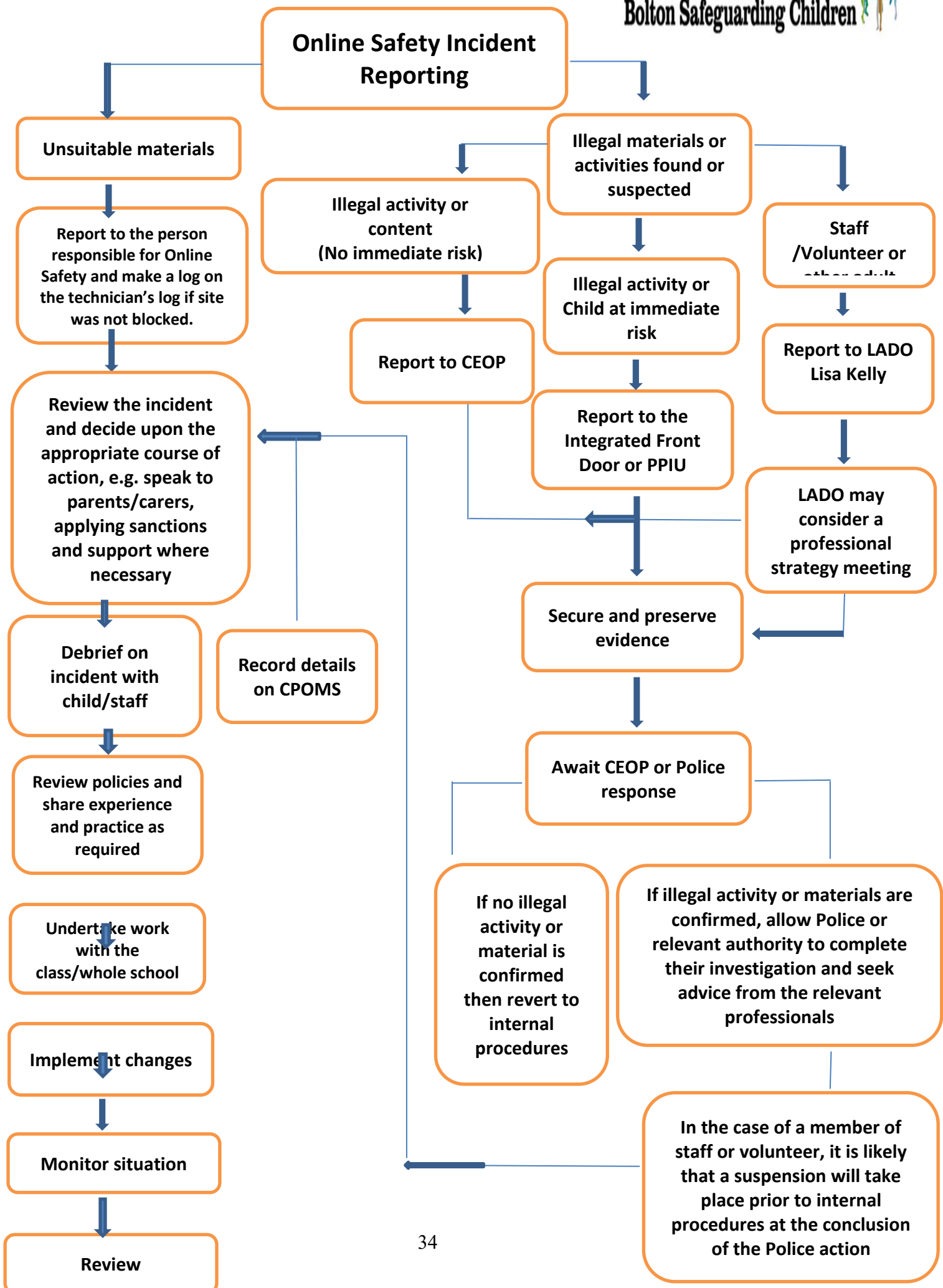
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work. Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Policy, the school has the right to remove my access to school systems / devices

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Print Name

Date

Signature



Appendix 5: Support for Bolton Schools

SET – Safeguarding in Education Team:

- Jo Nicholson– Safeguarding in Education Officer – 07917072223
- Natalie France – Safeguarding Education Social Worker – 07725809490

LADO: Lisa Kelly- 07824541233

Integrated Front Door – 01204 331500

Police protection investigation unit – 0161 856 7949

Community Police - 101

EXIT Team – Exitteam@bolton.gov.uk

Bolton Safeguarding Children’s Partnership: Shona Green – 01204 337964

If there is an ICT network issues contact your school ICT provider.

If your provider is Bolton School ICT Unit – contact 01024 332034 or contact@sict.bolton.gov.uk

Appendix 6: Legislation

The legislative framework of which this Online Policy and guidance has been produced is listed for reference to. 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 legal advice is sought in the advent of an online safety issue 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 person 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.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

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

The new 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. 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 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 of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

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 Head teachers, 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 Head teachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see [template policy in these appendices](#) and for DfE guidance)

<http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation>

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:

<http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/b0075738/reducing-bureaucracy/requirements/changestoschoolinformationregulations>

Appendix 7: Useful resources, additional guidance and contacts

UK Safer Internet Centre

[Safer Internet Centre -](#)

[South West Grid for Learning](#)

[Childnet](#)

[Professionals Online Safety Helpline](#)

[Internet Watch Foundation](#)

CEOP

Public enquiries

Telephone: 0870 000 3344

For general enquiries or to verify a person as an NCA officer:

Email: communication@nca.x.gsi.gov.uk

Telephone: 0370 496 7622 (available 24/7)

<http://ceop.police.uk/>

[ThinkUKnow](#)

Others:

INSAFE - <http://www.saferinternet.org/ww/en/pub/insafe/index.htm>

UK Council for Child Internet Safety (UKCCIS) www.education.gov.uk/ukccis

Netsmartz <http://www.netsmartz.org/index.aspx>

Cyberbullying

[DfE – Preventing & Tackling Bullying – Advice to school leaders, staff and Governing Bodies](#)

Anti-Bullying Network - <http://www.antibullying.net/cyberbullying1.htm>

Cyberbullying.org - <http://www.cyberbullying.org/>

Social Networking

Digizen – [Social Networking](#)

[SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people](#)

[Connectsafely Parents Guide to Facebook](#)

[Facebook Guide for Educators](#)

<https://www.disrespectnobody.co.uk/sexting/what-is-sexting/>

Mobile Devices / BYOD

Cloudlearn Report [Effective practice for schools moving to end locking and blocking](#)

NEN - [Guidance Note - BYOD](#)

Data Protection

Information Commissioners Office:

[Your rights to your information – Resources for Schools - ICO](#)

[ICO pages for young people](#)

[Guide to Data Protection Act - Information Commissioners Office](#)

[Guide to the Freedom of Information Act - Information Commissioners Office](#)

[ICO guidance on the Freedom of Information Model Publication Scheme](#)

[ICO Freedom of Information Model Publication Scheme Template for schools \(England\)](#)

[ICO - Guidance we gave to schools - September 2012 \(England\)](#)

[ICO Guidance on Bring Your Own Device](#)

[ICO Guidance on Cloud Hosted Services](#)

[Information Commissioners Office good practice note on taking photos in schools](#)

[ICO Guidance Data Protection Practical Guide to IT Security](#)

[ICO – Think Privacy Toolkit](#)

[ICO – Personal Information Online – Code of Practice](#)

[ICO – Access Aware Toolkit](#)

[ICO Subject Access Code of Practice](#)

Bolton Information Management Unit - Tasadiq.Naveed@bolton.gov.uk

<http://mossextranet.bolton.gov.uk/website/pages/DataProtectionandFreedomofInformation.aspx>

Professional Standards / Staff Training

DfE - <http://www.rrrecruitment.com/wp-content/uploads/2016/04/Guidance-for-Safer-Working-Practice-October-2015.pdf>

Kent - [Safer Practice with Technology](#)

[Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs](#)

[Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs](#)

[UK Safer Internet Centre Professionals Online Safety Helpline](#)

Working with parents and carers

[SWGfL / Common Sense Media Digital Literacy & Citizenship Curriculum](#)

[Connect Safely - a Parents Guide to Facebook](#)

[Vodafone Digital Parents Magazine](#)

[Childnet Webpages for Parents & Carers](#)

[DirectGov - Internet Safety for parents](#)

[Get Safe Online - resources for parents](#)

[Teach Today - resources for parents workshops / education](#)

[The Digital Universe of Your Children - animated videos for parents \(Insafe\)](#)

[Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide](#)

[Insafe - A guide for parents - education and the new media](#)

[The Cybersmile Foundation \(cyberbullying\) - advice for parents](#)

Research

[EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011](#)

[Futurelab - "Digital participation - its not chalk and talk any more!"](#)

Appendix 8: Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document
BSCB	Bolton Safeguarding Children’s Board
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPC	Child Protection Committee
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
EA	Education Authority
ES	Education Scotland
HWB	Health and Wellbeing
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers’ Association
IWF	Internet Watch Foundation
LA	Local Authority
LADO	Local Authority Designated Officer
LAN	Local Area Network
MASSS	Multi-agency Screening and Safeguarding Service
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
PPIU	Police Public Protection Investigation Unit
SET	Safeguarding in Education Team
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational Online programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Access Point

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in July 2016. However, BSCS cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal / professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.