Acre Heads Primary School

Online Safety Policy

Created by: Chloe Brown **Date:** September 2021

Last reviewed: October 2025

Next Review: September 2026

Online Safety Policy

Contents

1. Aims

This policy applies to all members of Acre Heads Primary (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of school.
The importance of safeguarding children from potentially harmful and inappropriate online material is recognised and understood, along with the fact that technology is a significant component in many safeguarding and wellbeing issues.

To address this and in light of the 4 categories of risk outlined below, we will adopt a whole school approach involving a number of measures and approaches with the aim of:

- Having robust processes (including filtering and monitoring systems) in place to ensure the online safety of pupils, staff, volunteers and governors
- Protecting and educating the whole school community in safe and responsible use of technology, including mobile and smart technology
- Setting clear guidelines for the use of mobile phones for the whole school community
- Establishing clear mechanisms to identify, intervene in and escalate any incidents or concerns, where appropriate

The approach to online safety is based on addressing the following 4 categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

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. This is pertinent to incidents of online bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but are linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and positive behaviour/ anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate Online Safety behaviour that take place in and out of school.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 Governors

The Governing Body will retain strategic oversight of the school's online safety approach and ensure that appropriate processes and procedures are established and maintained.

They will:

- Make sure that the school has appropriate filtering and monitoring systems in place and review their effectiveness
- Review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers about what needs to be done to support the school to meet these standards
- Make sure the DSL takes lead responsibility for understanding the filtering and monitoring systems in place as part of their role
- Make sure that all staff undergo safeguarding and child protection training, including online safety and that such training is regularly updated and is in line with advice from the safeguarding partners
- Make sure staff understand their expectations, roles and responsibilities around filtering and monitoring as part of safeguarding training
- Filtering and monitoring systems will be reviewed at least annually to ensure they remain effective and appropriate.
- Review the school's DfE's 'Plan Technology for Your School' self-assessment tool to evaluate the effectiveness of its filtering and monitoring provision.

The additional roles of the Online Safety Governor (Lucy Morris) will include:

- Meetings with the Online Safety Lead and/or DSL
- Attendance at Online Safety Group meetings
- Reporting to relevant Governors/Safeguarding Committee meetings
- Ensuring online safety is a running and interrelated theme which is implemented as a whole-school approach to safeguarding and related policies and/or procedures

A planned programme of formal online safety training will be made available to staff. Governors will

also be invited to attend this training. This will be regularly updated and reinforced.

All governors will:
● Ensure that they have read and understand this policy
● Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet ●Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
●Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 Headteacher

- The Headteacher is responsible for ensuring that all staff understand this policy, and that it is being implemented consistently throughout the school.
- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Designated Safeguarding Lead, Deputy Designated Safeguarding Lead, Child Protection Co-ordinator, Online Safety Lead or Behaviour Lead.
- The Headteacher and Designated Safeguarding Team are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (See flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse").
- The Headteacher is responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The Designated Safeguarding Leads will receive regular monitoring reports from the Online Safety Lead.

3.3 Online Safety Lead

- The Online Safety Lead:

  - leads the Online Safety Group and takes day to day responsibility for online safety issues in collaboration with the DSL, DDSL and CPC.
  - Has a leading role in establishing and reviewing the school online safety policies.
  - Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
  - Liaises with the school's Business Manager and Primary Tec.
  - Receives and monitors reports of online safety incidents through CPOMS.
  - Works with the relevant staff, including the DSL, DDSL and CPC to investigate, resolve and report e-safety issues.
  - Updates and delivers staff training alongside DSL on online safety.

3.4 Network Manager

Acre Heads Primary employs Primary Tec to manage their ICT services. Primary Tec is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check monthly and monitoring the school's ICT systems at all times.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

This list is not intended to be exhaustive.

3.5 Teaching and Support Staff

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive. A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly by the Online Safety Lead.

3.6 Designated Safeguarding Lead.

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place

- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services, if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively
- Complete the DfE's 'Plan Technology for Your School' self-assessment tool to evaluate the effectiveness of its filtering and monitoring provision.
- Conduct an annual online safety audit to assess staff training needs, pupil understanding, and the effectiveness of current policies and practices.

This list is not intended to be exhaustive.

3.7 Online Safety Representation

The headteacher, DSL, CPC, online safety lead, safeguarding governors, a representation group of parents on the GB and the child e-safety group provide a consultative group that has representation from the Acre Heads community, with responsibility for issues regarding online safety and the monitoring of the Online Safety Policy including the impact of initiatives.

- Mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression.
- Consulting stakeholders – including parents/carers and the students/pupils about the online safety provision.

3.8 Students / Pupils:

- Are responsible for using the school's digital technology systems in accordance with the Pupil Acceptable Use Agreement.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- 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/use of images and on online-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that Acre Heads' Online Safety Policy covers

their actions out of school, if related to their membership of the school.

3.9 Parents / Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Parents are expected to:

- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet.
- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.

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

- Digital and video images taken at school events
- Access to parents' sections of the website.
- Their children's personal devices.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Child net International
- Parent fact sheet - Child net International
- Healthy relationships – Disrespect Nobody

4. Education – Students/Pupils

Pupils will be taught about online safety as part of the curriculum:

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met

- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Education – Parents/Carers

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (VLE). This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings where appropriate.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher / DSL
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so. When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation

- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial Intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Acre Heads recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deep fakes', where AI is used to create images, audio or video hoaxes that look real.

We will treat any use of AI to bully pupils in line with our behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used.

Any AI-generated content used in school (e.g. lesson plans, feedback) will be clearly labelled and fact-checked to ensure accuracy and transparency.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

8. Using mobile devices in school

Pupils at Acre Heads are not permitted to use their own devices in school. Any mobile devices brought to school should be turned off and handed to a member of the Office or class teacher at the start of the day. These will be kept in a safe place and returned at the end of the school day. Any breach of the acceptable use agreement by a pupil may trigger actions in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g., asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software

● Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use. If staff have any concerns over the security of their device, they must seek advice from the School Business Manager and/or Primary Tec.

10. Use of digital and video images/ Data Protection

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. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students/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.
- Using the school's pupil's information, photographs of pupils will only be published on the school website/social media/local press when written permission from parents or carers has been obtained.
- 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 (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases 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 be taken on school equipment whenever possible. If it is necessary to use a personal device, images will not be stored on that device for more than 24 hours.
- Care should be taken when taking digital/video images that students/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
- Photographs published on the website/Seesaw, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students'/pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

● Student's/pupil's work can only be published with the permission of the student / pupil and parents or carers.

10.1 Data Protection

See separate Data Protection Policy.

11. Social media

11.1 When using social media, staff should ensure that:

● No reference should be made in social media to students/pupils, parents/carers or school staff, unless it's through the school's approved Social Media account and posted by the school.

● They do not engage in online discussion on personal matters relating to members of the school community.

● Personal opinions should not be attributed to the *school.*

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

11.2 When official school social media accounts are established there should be:

● A process for approval by senior leaders.

● Clear processes for the administration and monitoring of these accounts – involving at least two members of staff.

● A code of behaviour for users of the accounts.

● Systems for reporting and dealing with abuse and misuse.

● Understanding of how incidents may be dealt with under school disciplinary procedures.

11.3 Personal Use:

● Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy but at the discretion of the Headteacher or appropriate Senior Leader.

● Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

● Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

● The school permits reasonable and appropriate access to private social media sites.

11.4 Monitoring of Public social media

● As part of active social media engagement, the school pro-actively monitors the Internet for public postings about the school and reviews positive/negative comments and responds

appropriately.

● The school should effectively respond to social media comments made by others and take action if comments about pupils, teachers or the school are inappropriate.

The school's use of social media for professional purposes will be checked regularly by the Headteacher.

12. Issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police

12.1 Dealing with unsuitable/inappropriate activities

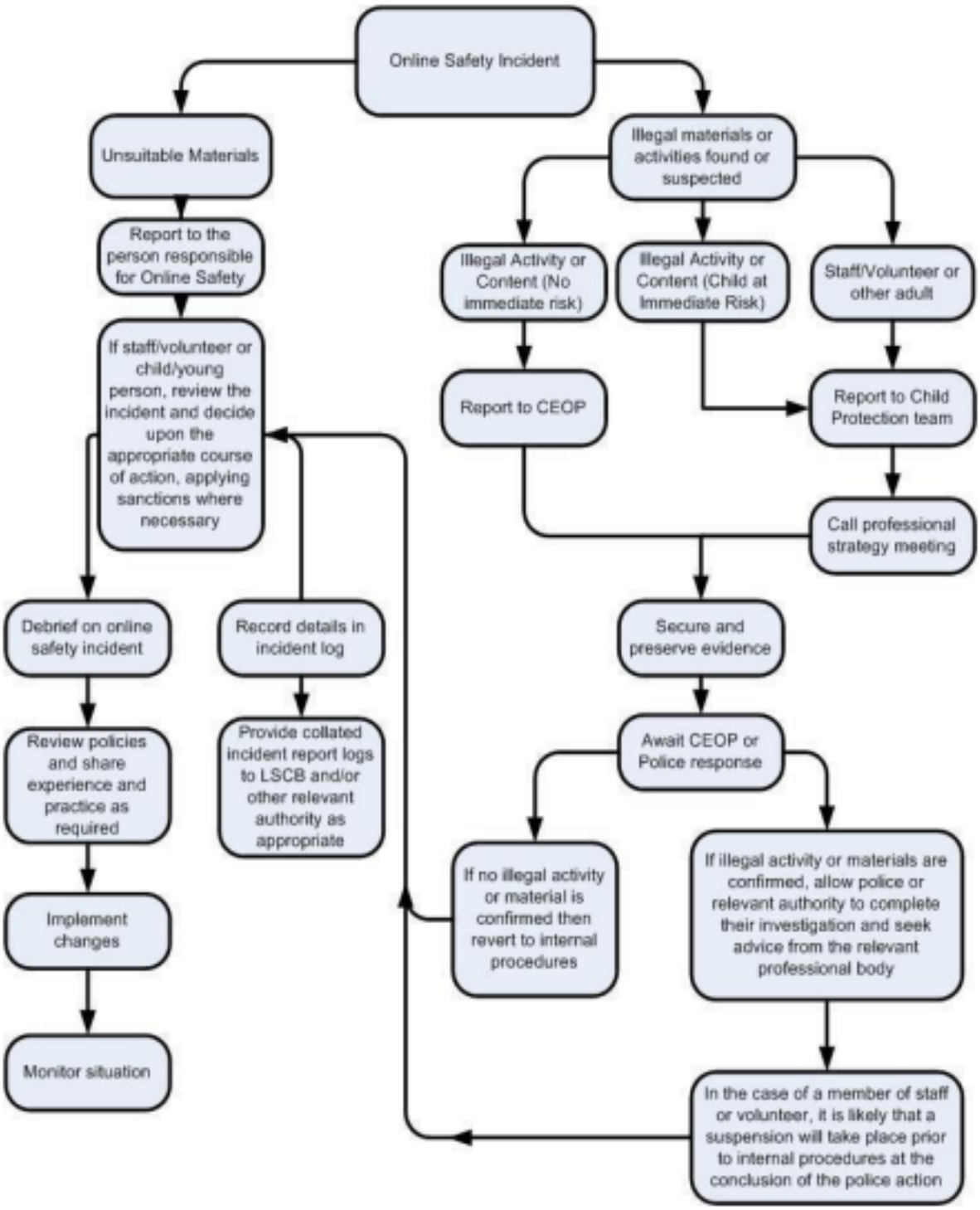
Some internet activity e.g., accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g., cyber bullying would be banned and could lead to criminal prosecution. There are however a range of activities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

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Applicable	Acceptable at certain times	Acceptable For Nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	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
	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	
	Promotion of extremism or terrorism				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					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 gambling					X	
On-line shopping / commerce					X	
File sharing					X	

12.2 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, refer to the right-hand side of the Flowchart below for responding to online safety incidents and report immediately to the police.



12.3 Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school 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, all steps in this procedure 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 should 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). Records of internet activity are kept and monitored using Securly and PrimaryTec.
- Record the URL of 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).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority Group or national / local organisation (as relevant).
    - Police involvement and/or action
- **If content being reviewed includes images of child abuse, then 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
    - Promotion of terrorism or extremism
    - Other criminal conduct, activity or materials
- **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 demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes

12.4 School Actions & Sanctions

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. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

	Actions / Sanctions								
Students / Pupils Incidents	Refer to classroom teacher	Refer to SLT/DSL	Refer to Head teacher	Refer to Police	Refer to technical support staff for action	Inform parents/carers	Removal of network /internet access rights	Warning	Further sanctions e.g., 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	X		X			
Unauthorised use of non-educational sites during lessons	X								
Unauthorised / inappropriate use of mobile phone / digital camera / another mobile device	X	X				X			
Unauthorised / inappropriate use of social media / messaging apps / personal email	X				X	X			
Unauthorised downloading or uploading of files	X				X				
Allowing others to access school network by sharing username and passwords	X	X	X						
Attempting to access or accessing the school network, using another student's / pupil's account	X	X	X		X	X			
Attempting to access or accessing the school network, using the account of a member of staff			X		X	X			
Corrupting or destroying the data of other users	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	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X		X				

Using proxy sites or other means to subvert the school's / academy's filtering system		X	X		X	X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident	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								

	Actions / Sanctions							
Staff Incidents	Refer to line manager	Refer to Head teacher	Refer to Local Authority/ HR	Refer to Police	Refer to technical support staff for action re-filtering / security etc.	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	X	X	X	X
Inappropriate personal use of the internet / social media / personal email		X	X		X	X	X	X
Unauthorised downloading or uploading of files		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	X	X
Careless use of personal data e.g., holding or transferring data in an insecure manner		X	X			X	X	X
Deliberate actions to breach data protection or network security rules		X	X			X	X	X

Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		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	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X	X		X	X	X	X
Actions which could compromise the staff member's professional standing		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
Using proxy sites or other means to subvert the school's / academy'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			
Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X	X	X	X
Breaching copyright or licensing regulations		X	X					
Continued infringements of the above, following previous warnings or sanctions		X	X				X	X

13. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually. Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable.

Appendix 1: Online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT

Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	