Our Lady of Perpetual Succour Catholic Primary School

Online Safety Policy

1. Scope of the Policy

This policy applies to all members of the school community (staff, pupils, volunteers, parents/carers, governors, visitors and community users) who have access to and are users of the school ICT systems, both in and out of school. The Education and Inspections Act 2006 empowers Headteachers, 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 Safety incidents covered by this policy, which may take place out of 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. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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 Safety behaviour that take place inside and outside of school.

2. Context

We live in a digital age where technology is playing an ever increasing part in our lives; it is changing the way that we do things both inside and outside of school and although we recognise the benefits of technology we must also be aware of the potential risks and ensure that all staff, pupils and parents/carers associated with the school are able to use technology in a safe and responsible manner.

Some of the potential dangers of using technology may include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet

- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.
- Distribution of personal data contrary to GDPR laws.

Many of these risks reflect situations in the offline world but it is important that as a school we have a planned and coordinated approach to using technology in a safe and responsible way.

3. Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

3.1 Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors e receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor, which is combined with the child protection officer. The role of the Online Safety Governor will include:

- meetings with the Online Safety Co-ordinator / Officer
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors / Board / Committee / meeting

3.2 Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, and as the Senior Designated Person (SDP) will take on the role of Online Safety Coordinator, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.
- As SDP, the Headteacher should be trained in Online Safety issues and be 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 / strangers
    - potential or actual incidents of grooming
    - cyber-bullying

- The Headteacher will liaise with the Local Authority and relevant bodies when and with school technical staff when necessary in cases of online safety incidents.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher will deal with incidents alongside the Online Safety Coordinator and decide on whether the investigation / action / sanctions are necessary.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Co-ordinator.

3.3 Online Safety Lead:

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- meets annually with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant Governors' meetings
- reports regularly to Senior Leadership Team
- The Online Safety Lead will deal with incidents alongside the Headteacher and decide on whether the investigation / action / sanctions are necessary.
- Holds regular meetings with the Digital Leaders

3.4 Network ICT Service Provider.

The school's intranet and connection to the internet is provided by 24/7 technology solutions. They provide internet access as well as a content filter, to ensure safe browsing, and antivirus/attack protection on all computers. It is the responsibility of the school, however, to ensure that 24/7 Technology carries out and updates its safety measures.

24/7 Technology will ensure:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack (See Appendix A)
- that the school meets required online safety technical requirements and any Local Authority/MAT/other relevant body online safety guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy.

- the filtering of illegal, harmful appropriate content is up to date and secure. (see Appendix A)
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network and internet is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher or Online Safety Lead / for investigation / action / sanction.
- that monitoring software / systems are implemented and updated as agreed in school policies

3.5 Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- ensure that GDPR is adhered to by following the Data Protection Policy
- they have read, understood and signed the Staff Acceptable Use Agreement
- they report any suspected misuse or problem to the Headteacher or Online Safety Lead for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use policies
- 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
- are aware of safeguarding issues, including extremism (Prevent duty), in line with Safeguarding Policy
- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- they have read and understood relevant parts of the Keeping Children Safe in Education document (2021).

3.6 Digital Leaders (Cyber Buddies)

The Digital Leaders provide a consultative group that has wide representation from pupils, and discuss issues regarding online safety and the monitoring the Online Safety

Policy, including the impact of initiatives. Digital Leaders will assist the Online Safety Lead with:

- The review and monitoring of the school Online Safety Policy / documents.
- Day to day in-class implementation of this policy, alongside class teachers.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- consulting stakeholders – including parents / carers and the pupils about the online safety provision

3.7 Pupils

- are responsible for using the school 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
- 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 / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the Online Safety Policy covers their actions out of school, if related to their membership of the school

3.8 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, school website and information about national / local online safety campaigns. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / Learning Platform
- following guidelines set out in the Data Protection policy regarding GDPR

3.9 Community Users

Community Users who access school systems or programmes as part of the wider school provision will be expected to sign a Visitor AUA before being provided with access to school systems.

4. Policy Statements

4.1 Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. Whilst remaining age appropriate, the online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited.
- Online safety messages should be reinforced as part of the Computing Curriculum, and PSHE lessons with reference to the Education for a Connected World Document.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making, this in accordance with Prevent Duty.
- Pupils will be taught about the dangers of sharing inappropriate media, sexting and bullying.
- Pupils will be taught of the dangers of meeting people online, including grooming.
- Pupils will be taught how to report indecent or inappropriate material or communications, including the dangers of sexting, bullying, grooming harassment and exploitation.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices.

4.2 Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, Learning Platform
- Curriculum activities
- Reference to the relevant web sites / publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

4.3 Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Staff will teach online safety with through the Computing Curriculum and PSHE lessons – using Education for a Connected World.
- All new staff should 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 Online Safety Lead will provide advice / guidance / training to individuals as required.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Lead (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.
- The Online Safety Coordinator (or other nominated person) will provide advice/guidance/training to individuals as required.

4.4 Training – Governors/Directors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/MAT/National Governors Association/or other relevant organisation (e.g. SWGfL).
- Participation in school/academy training/information sessions for staff or parents

4.5 Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring 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. To ensure this, the school employ 24/7 technology to ensure the equipment and facilities are up to date and working. They ensure:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Internet access is filtered for all users (See Appendix A)

The school will ensure:

- There will be regular reviews and audits of the safety and security of school technical systems
- All users will be provided with a username and secure password by the class teacher, who will keep an up to date record of users and their usernames stored on the VLE. Users are responsible for the security of their username and password.
- This platform will be used to communicate, set and respond to work when children are learning remotely.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- All other GDPR procedures are followed (see Data Protection Policy).

4.6 Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet, which may include the school's learning platform and other cloud-based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited

to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, Data Protection Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme

- The school Acceptable Use Agreements for staff, pupils and parents/carers will give consideration to the use of mobile technologies

- The school allows:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*No[1]*	*Yes**Error! Bookmark not defined.*	*Yes/[3]*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet only					*Yes*	
No network access						

[1] In some exceptional circumstances, parents may bring a child's mobile device into school, switched off, and hand it to the office where it will be kept securely until the end of the school day. However, these are only in exceptional circumstances and some explanation should be given as to why the child needs the mobile device after school, whereby acceptance will be at the discretion of the Headteacher.

[2] Staff devices are allowed in school but may only be used, or visible within the designated area of the offices and staff room.

[3] Visitor's mobile devices will not be able to connect to the internet and should only be used or visible in the allocated area, or, when they are required for work related tasks. This is with the exception of parents attending school events and wishing to take pictures as outlined below.

4.7 The use of digital images and video

The development of digital imaging technologies has created significant benefits to learning, allowing school staff and pupils instant use of images they have recorded themselves or downloaded from the internet. School staff and pupils are made aware of the potential risks associated with storing, sharing and posting images on the internet and must follow the good practice detailed below.

- When using digital images, staff will inform and educate pupils about the risks associated with:
    - the taking, use, sharing, publication and distribution of images. In particular they will recognise
    - the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are permitted to take digital images and video 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 will be taken when capturing digital images and video that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not bring into school personal technology that allows for photography, recording video or audio.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Images and videos published on the school 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, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- 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 in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images. This is outlined in the Parent/Carer Acceptable Use Agreement.

4.8 Data Security and Protection

Data Protection in line with Data Protection Act 1998, and GDPR 2018 is covered by the Data Protection Policy, Information and Security Policy and the various Acceptable Use Agreements.

4.9 Prevent Duty

All staff have been trained, or will be trained as part of induction, in the Prevent scheme to combat extremism. This training covers online aspects of radicalisation.

5. Digital Communication

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

	Staff & other adults				**Students/Pupils**			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school[1]	X							X
Use of mobile phones in lessons				X				X
Use of mobile phones in social time[2]	X							X
Taking photos on school mobile phones/cameras	X							
Taking photos on personal mobile phones/cameras				X				X
Use of other mobile devices e.g. tablets, gaming devices				X				X
Use of personal email addresses in school, or on school network[2]		X						X
Use of school email for personal emails[3]		X						X
Use of messaging apps on personal devices								X
Use of messaging apps on school devices				X				X
Use of social media – school accounts[4]	X						X	
Use of social media – personal accounts[4]		X						X
Use of school blogs	X						X	

[1] – In some exceptional circumstances, parents may bring a child's mobile device into school, switched off, and hand it to the office where it will be kept securely until the end of the school day. However, these are only in exceptional circumstances and some explanation should be given as to why the child needs the mobile device after school, whereby acceptance will be at the discretion of the Headteacher.
[2] - Staff may use personal devices in the designated areas (staffroom and office corridor), or when no children are in the school, for personal reasons using the school network in accordance with the relevant acceptable use policies.
[3] – In some exceptional cases it is permitted for staff to use school email addresses for personal reasons in accordance with the relevant acceptable use policies.

[4] – Staff members are permitted to use the school social media accounts on school devices in accordance with the relevant policies. Pupils, under supervision may sometimes be allowed to post onto school social media. Staff may use personal social media only on personal devices using the school network in accordance with the relevant acceptable sue policies.

When using communication technologies, the school ensures the following good practice:

- The official school email service is regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff, pupils or parents/carers (email, chat, VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Pupils will be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material. Cyber buddies will be used to monitor misuse and report to the online safety lead
- Personal information will not be posted on the school website and only official email addresses should be used to identify members of staff.

6. Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- School staff should not add parent or pupil contacts on social media unless a close member of their family.
- 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 or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established, the school will ensure that:

- Accounts are approved by the Headteacher or Online Safety Lead
- Monitoring will be done regularly by the Headteacher and the Online Safety Lead
- Reports of Misuse and abuse will be dealt with by the Headteacher

Personal Use:

- Personal communications are those made via a personal social media accounts. 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
- 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

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school will not respond to comments on social media as it is used as a one-way communication tool for events etc.

7. Unsuitable/inappropriate activities

School ICT systems are only to be used for agreed, appropriate and suitable work related activities. Internet activity which is considered unsuitable or inappropriate will not

be allowed and if discovered will lead to disciplinary action. Internet activity that is illegal will be reported and could lead to criminal prosecution.

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place accidently, through careless or irresponsible or, very rarely, through deliberate misuse.

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 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 (Prevent Duty)				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	

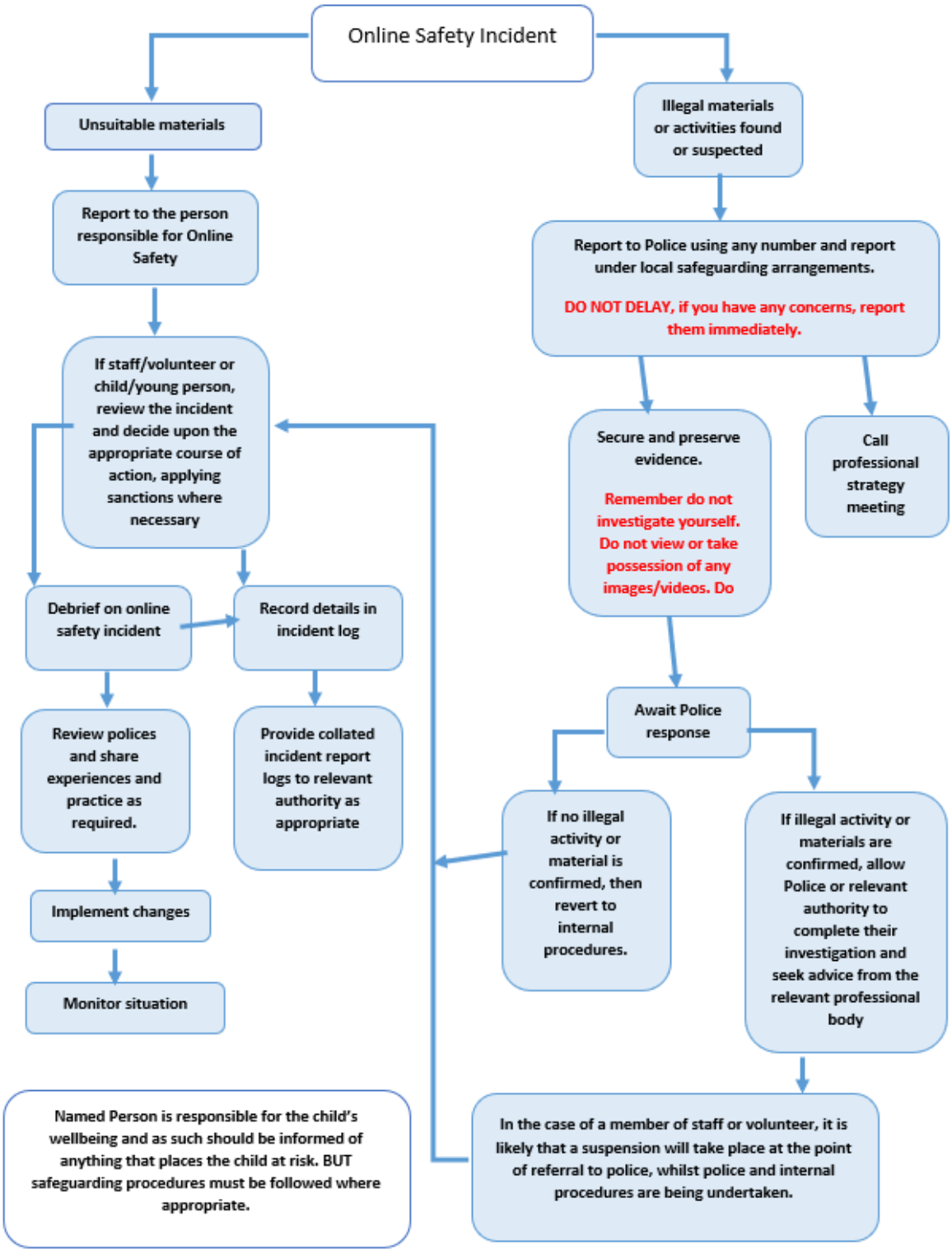
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line 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			

8. Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

8.1 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 and appendix) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

8.2 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).
- 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 – 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, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority 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.

8.3 School actions and 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 class teacher/tutor	Refer to Online Safety Lead	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access rights	Warning	Further sanction
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								
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	X		X			X			
Unauthorised/inappropriate use of social media/ messaging apps/personal email	X	X	X		X	X			
Unauthorised downloading or uploading of files	X	X	X		X	X			
Allowing others to access school/academy network by sharing username and passwords	X	X	X						
Attempting to access or accessing the school/academy network, using another	X	X							

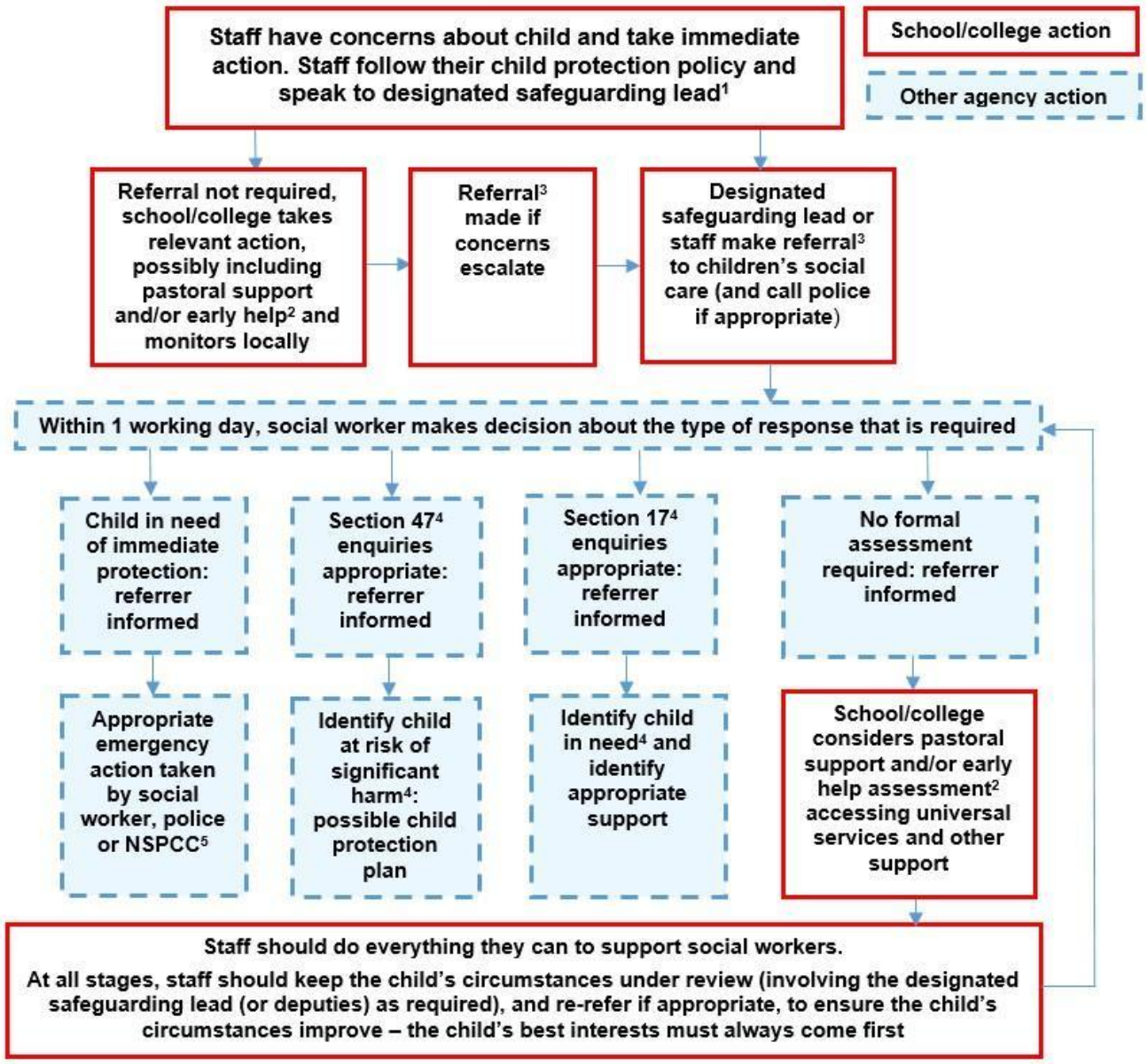
student's/pupil's account									
Attempting to access or accessing the school/academy network, using the account of a member of staff	X	X	X						
Corrupting or destroying the data of other users	X	X	X						
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X			
Continued infringements of the above, following previous warnings or sanctions			X			X			X
Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school			X						
Using proxy sites or other means to subvert the school's/academy's filtering system	X	X	X		X				
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X			
Deliberately accessing or trying to access offensive or pornographic material		X	X	X		X			
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X	X						

	Actions/Sanctions							
Staff Incidents	Refer to Online Safety lead	Refer to Headteacher	Refer to Local Authority/HR	Refer to Police	Refer to Technical Support Staff for action re filtering	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						
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						
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X						
Deliberate actions to breach data protection or network security rules	X	X						
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X						
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X					
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils		X	X	X				
Actions which could compromise the staff member's professional standing		X	X					

Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school/academy		X	X					
Using proxy sites or other means to subvert the school's/academy's filtering system	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			
Breaching copyright or licensing regulations	X	X						
Continued infringements of the above, following previous warnings or sanctions		X	X					

9. Incidents Where there are Concerns about a Child.

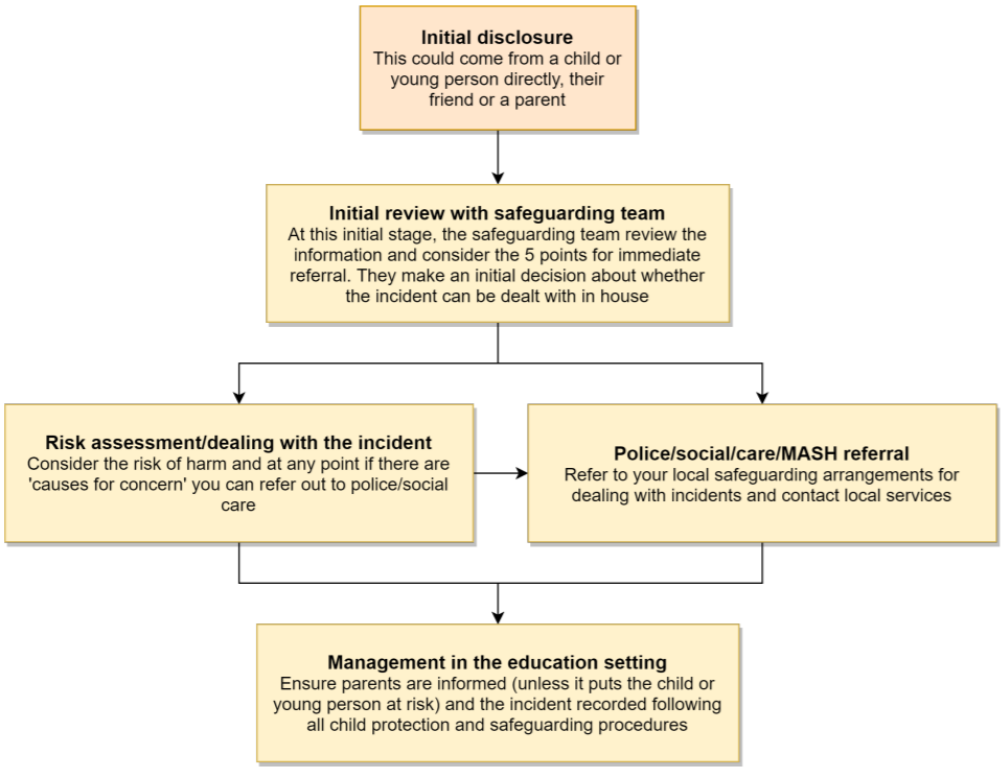
The following flow chart is taken from page 22 of Keeping Children Safe in Education 2021 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.



9.1 Sexting – sharing nudes and semi-nudes

All schools (regardless of phase) should refer to the updated UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: advice for education settings to avoid unnecessary criminalisation of children. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse. There is a one-page overview called Sharing nudes and semi-nudes: how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken.

Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.The school DSL will in turn use the full guidance document, Sharing nudes and semi-nudes (Appendix B) – advice for educational settings to decide next steps and whether other agencies need to be involved.



***Consider the 5 points for immediate referral at initial review:**

1. The incident involves an adult
2. There is reason to believe that a child or young person has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent (for example, owing to special educational needs)
3. What you know about the images or videos suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The images involves sexual acts and any pupil in the images or videos is under 13
5. You have reason to believe a child or young person is at immediate risk of harm owing to the sharing of nudes and semi-nudes, for example, they are presenting as suicidal or self-harming

It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

9.2 Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence, as highlighted in Keeping Children Safe in Education and that pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

9.3 Bullying

Online bullying should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter. See Bullying Policy for more information.

9.4 Sexual Violence and Harassment

DfE guidance on sexual violence and harassment is referenced in Keeping Children Safe in Education and also a document in its own right which staff have read.
Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

10.`Development/Monitoring/Review of this Policy

This online safety policy has been developed by a working group/ made up of:

- Headteacher and senior leaders
- Online Safety Coordinator
- Online Safety Lead
- Staff – including teachers, support staff, technical staff
- Governors
- Parents and carers
- Pupils

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development/Monitoring/Review

This online safety policy was approved by the Governing Body on:	
The implementation of this online safety policy will be monitored by the:	Online Safety Coordinator Headteacher Senior Leadership Team Governors
Monitoring will take place at regular intervals:	Once per Year
The Governing Body Committee will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Once per Year
The online safety 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 safety or incidents that have taken place. The next anticipated review date will be:	November 2021

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity from filtering flags
- Internal monitoring data for network activity
- Surveys/questionnaires of
    - students/pupils
    - parents/carers
    - staff

Appendix A

WEBFILTERING PROVISION

What is the web filtering service?
The web filtering service provided to the school provides a filter for staff and learners, which prevents them from accessing potentially harmful and explicit content online. The service, which is not noted by the end user, intercepts all internet traffic from the schools network provided as part of the Broadband Provision.
All filtering can be configured using various policies; these policies can be set globally across all computers or at individual level depending on the requirements of staff, time of day, time of week, or website specific e.g. Facebook.

Schools can require greater control if required in line with individual school policies.
In the event of a site being discovered that is deemed inappropriate by the school, this should be logged immediately via your point of contact at 24/7 Technology or consultant so that we can take the appropriate action.

How does web filtering work?
Web filtering blocks access to potentially harmful material found online from staff and learners by categorizing online content e.g. gaming, gambling, pornography, social media etc.

Statement from our provider
“Our categorization is based on an automated engine called ICAP which uses language dictionaries in any language as well as sites being scanned in a number of ways:

- URLs which are requested by the user but have not been rated will be automatically scanned for any illicit language as well as colour tone in images before being displayed to the end user
- Users can request we scan specific sites either in bulk or on a site by site basis
- In general the ratings are done by the automated rating system. The system does not rate malicious content such as viruses and exploits as in some cases the sites have legitimate content. The ICAP server also obtains third party feeds from governments and other organisations of sites containing extremist or sexual violence.
- Any requests to change the rating of a site will be dealt personally by a member of staff and the site will be fully vetted before re-rating to ensure the highest level of security.
- All data is displayed in a hierarchical system that displays, IP, domain and website details of what was visited, it may only block a certain portion of the website due to illicit language and the rest of the website be free to browse

Does the service provide appropriate filtering and monitoring?
Schools in England (and Wales) are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering" [1] . Furthermore, the Department for Education published the revised statutory guidance 'Keeping Children Safe in Education'[2] in May 2016 (and active from 5th September 2016) for schools and colleges in England. Amongst the revisions, schools are obligated to "ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system" however, schools will need to "be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

Illegal Online Content
Filtering providers should ensure that access to illegal content is blocked, specifically that the filtering providers:

Aspect	Rating	Explanation
Are IWF Members		Diladele B.V are IWF members
And block access to illegal child abuse images (by actively implementing the IWF CAIC list)		The IWF CAIC list is part of Diladele B.V Web Filtering Service. Category – Child Abuse: websites that have been verified by the Internet Watch Foundation to contain or distribute images of non-adult children that are depicted in a state of abuse.
Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		The list is part of the Diladele B.V web filtering system.

Inappropriate Online Content
Recognizing that no filter can guarantee to be 100% effective, providers should both confirm, and describe how, their system manages the following content

Content	Rating	Explanation
Discrimination		**Category - Discrimination** Sites that promote the identification of racial groups, the denigration or subjection of groups, or the superiority of any group.

		Sites in this category are blocked by default for schools
Drugs/Substance Abuse		**Category - Drug Abuse** Websites that feature information on illegal drug activities including: drug promotion, reparation, cultivation, trafficking, distribution, solicitation, etc. ***Sites in this category are blocked by default for schools***
Extremism		**Category - Extremist Groups** Sites that feature radical militia groups or movements with aggressive anti-government convictions or beliefs **Sites in this category are blocked by default for schools**
Malware/Hacking		**Category - Malicious Websites** Sites that host software that is covertly downloaded to a user's machine to collect information and monitor user activity, and sites that are infected with destructive or malicious software, specifically designed to damage, disrupt, attack or manipulate computer systems without the user's consent, such as virus or trojan horse. **Category - Hacking** Websites that depict illicit activities surrounding the unauthorized modification or access to programs, computers, equipment and websites. ***Sites in these categories are blocked by default for schools***
Pornography		**Category - Pornography** Mature content websites

		(18+ years and over) which present or display sexual acts with the intent to sexually arouse and excite. **Category - Nudity and Risque** Mature content websites (18+ years and over) that depict the human body in full or partial nudity without the intent to sexually arouse ***Sites in these categories are blocked by default for schools***
Piracy & Copyright		**Category - Peer-to-Peer File Sharing** Websites that allow users to share files and data storage between each other. ***Sites in this category are blocked by default for schools***
Self Harm		**Category - Explicit Violence** This category includes sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc **Sites in this category are blocked by default for schools**
Violence		**Category - Explicit Violence** This category includes sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc **Sites in this category are blocked by default for schools**

This list should not be considered an exhaustive list. Please outline how the system manages this content and many other aspects.

The policies which we use for schools have been carefully tailored to enable access to the majority of appropriate websites. On the occasion where a school is unable to access a specific website, the school is able to either unblock the website themselves if they have requested this level of access or contact our service desk to request the site be unblocked.

Filtering System Features
How does the filtering system meet the following principles:

Principle	Rating	Explanation
Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role		Policies can be adjusted to account for different, requirements, use groups, times of day etc.
Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content		All schools have the option of managing their own Block and Permit policies.
Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		The general categories can be found here Diladele B.V Categories
Identification - the filtering system should have the ability to identify users		Users are identified via IP address.
Mobile and App content – isn't limited to filtering web traffic and includes the blocking of inappropriate content via mobile and app technologies		The Diladele B.V service is a proxy service managed by group policy that can be enabled on mobile app and other technologies
Multiple language support – the ability for the system to manage relevant languages		The filter has multi-lingual support
Reporting mechanism – the ability to report inappropriate content for access or blocking		We implement a standard block page, and schools can either unblock or report the issue to us via our service desk for the site to be unblocked. Where inappropriate access has occurred, again the school can block this site if they have requested that level of access, or contact our service desk for the site to

		be blocked
Reports – the system offers clear historical information on the websites visited by your users		The system offers a broad range of reports which schools can request. Historical data is stored for a set period of time and reports ran against this data.

Filtering systems are only ever a tool in helping to safeguard children when online and schools have an obligation to *"consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum".*

Appendix B

Sharing nudes and semi-nudes: how to respond to an incident

An overview for all staff working in education settings in England

UK Council for Internet Safety

This document provides a brief overview for frontline staff of how to respond to incidents where nudes and semi-nudes have been shared.

All such incidents should be immediately reported to the Designated Safeguarding Lead (DSL) or equivalent and managed in line with your setting's child protection policies.

The appropriate safeguarding lead person should be familiar with the full 2020 guidance from the UK Council for Internet Safety (UKCIS), ***Sharing nudes and semi-nudes: advice for education settings working with children and young people*** and should **not** refer to this document instead of the full guidance.

What do we mean by sharing nudes and semi-nudes?

In the latest advice for schools and colleges (UKCIS, 2020), this is defined as the sending or posting of nude or semi-nude images, videos or live streams online by young people under the age of 18. This could be via social media, gaming platforms, chat apps or forums. It could also involve sharing between devices via services like Apple's AirDrop which works offline. Alternative terms used by children and young people may include 'dick pics' or 'pics'.

The motivations for taking and sharing nude and semi-nude images, videos and live streams are not always sexually or criminally motivated.

This advice does not apply to adults sharing nudes or semi-nudes of under 18-year olds. This is a form of child sexual abuse and must be referred to the police as a matter of urgency.

What to do if an incident comes to your attention

Report it to your Designated Safeguarding Lead (DSL) or equivalent immediately. **Your setting's child protection policy should outline codes of practice to be followed.**

- **Never** view, copy, print, share, store or save the imagery yourself**,** or ask a child to share or download – **this is illegal**.[1]
- If you have already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report this to the DSL (or equivalent) and seek support.
- **Do not** delete the imagery or ask the young person to delete it.
- **Do not** ask the child/children or young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL (or equivalent).
- **Do not** share information about the incident with other members of staff, the young person(s) it involves or their, or other, parents and/or carers.
- **Do not** say or do anything to blame or shame any young people involved.
- **Do** explain to them that you need to report it and reassure them that they will receive support and help from the DSL (or equivalent).

For further information

Download the full guidance, *Sharing nudes and semi-nudes: advice for education settings working with children and young people* (UKCIS, 2020) at www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people.

[1] In exceptional circumstances, it may be necessary for the DSL (or equivalent) only to view the image in order to safeguard the child or young person. That decision should be based on the professional judgement of the DSL (or equivalent).