Our Lady of Perpetual Succour
Catholic Primary School

Online Safety Policy

We learn to love everyone as Jesus loves us

Scope of the Online Safety 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. It also applies to the use of personal digital technology on the school site (where allowed). 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 regarding 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 antibullying policies) and will, where known, inform parents/carers of incidents of inappropriate Online Safety behaviour that take place inside and outside of school.

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.
- Child Sexual Exploitation
- Child on Child abuse
- 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.

- **Policy development, monitoring and review**

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
- Pupils

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

Schedule for development, monitoring and 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:	January 2024

The school will monitor the impact of the policy using:

- logs of reported incidents
- monitoring logs of internet activity (including sites visited)

- internal monitoring data for network activity
- surveys/questionnaires of:
    - learners
    - parents and carers
    - Staff.

- **Policy and leadership**

- **Responsibilities**

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals**1** and groups within the school.

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 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 Coordinator

- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards
- regular monitoring of filtering / change control logs

- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- reporting to relevant Governors' meeting

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

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 Lead 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 Lead and decide on whether the investigation / action / sanctions are necessary.

- The Headteacher will ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents.

- The Headteacher will meet regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs.

- The Senior Leadership Team receives reports of online safety incidents and creates a log of incidents to inform future online safety developments and share this with the Online Safety Lead.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Coordinator.
- The Headteacher/Senior Leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and the IT service providers in all aspects of filtering and monitoring.

- The Senior Leadership Team will liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated.

Online Safety Lead

The Online Safety Lead will:

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents.
- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL)
- Provide training and advice for staff.
- reports regularly to Senior Leadership Team
- Promote an awareness of and commitment to online safety education / awareness raising across the school and beyond.
- The Online Safety Lead will deal with incidents alongside the Headteacher and decide on whether the investigation / action / sanctions are necessary.

Designated Safeguarding Lead (DSL)

The Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data [2]
- access to illegal/inappropriate materials.
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- Online bullying.

Curriculum Leads

Curriculum Leads will work with the Online Safety Lead to develop a planned and coordinated online safety education programme. This will be provided through:

- PHSE and SRE programmes
- A mapped cross-curricular programme
- assemblies and pastoral programmes
- Relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters and of the current school Online Safety Policy and practices.
- they understand that online safety is a core part of safeguarding.
- ensure that GDPR is adhered to by following the Data Protection Policy

[2] See 'Personal data policy' in the Appendix.

- 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 learners and 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.
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices.
- in lessons where internet use is pre-planned learners 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 a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc.
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.
- they have read and understood relevant parts of the Keeping Children Safe in Education document (2022).
- are aware of safeguarding issues, including extremism (Prevent duty), in line with Safeguarding Policy

Pupils

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement and Online Safety Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- should 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.

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.

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.

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.

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.

Professional Standards

There is an expectation that required professional standards will be applied to online safety as in other aspects of school life i.e., policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

Policy

- **Online Safety Policy**

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- describes how the school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction
- is published on the school website.

- **Acceptable use**

- The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

- **Acceptable use agreements**

- The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated/re-enforced through:
  - staff induction
  - digital signage
  - posters/notices around where technology is used
  - communication with parents/carers
  - built into education sessions
  - school website
  - peer support.

• User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Any illegal activity for example:** • Child sexual abuse imagery • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering					**X**
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information,					**X**

	databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			**X**	**X**	
	Promotion of any kind of discrimination				**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**	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			**X**	**X**	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				**X**	

Consideration should be given for the following activities when undertaken for **non-educational** or professional purposes:	**Staff and other adults**				**Learners**			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awareness
Online gaming	**X**				**X**			
Online shopping/commerce			**X**		**X**			
File sharing	**X**				**X**			
Social media	**X**				**X**			
Messaging/chat	**X**				**X**			
Entertainment streaming e.g. Netflix, Disney+			**X**		**X**			
Use of video broadcasting, e.g. YouTube, Twitch, TikTok			**X**		**X**			
Mobile phones may be brought to school		**X**			**X**			
Use of mobile phones for learning at school	**X**				**X**			
Use of mobile phones in social time at school		**X**			**X**			
Taking photos on mobile phones/cameras	**X**				**X**			

Use of other personal devices, e.g. tablets, gaming devices	**X**				**X**			
Use of personal e-mail in school, or on school network/wi-fi	**X**				**X**			
Use of school e-mail for personal e-mails	**X**				**X**			

When using communication technologies, the school considers the following as good practice:

- When communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school
- Any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- Staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- Users should immediately report to a nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- 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.

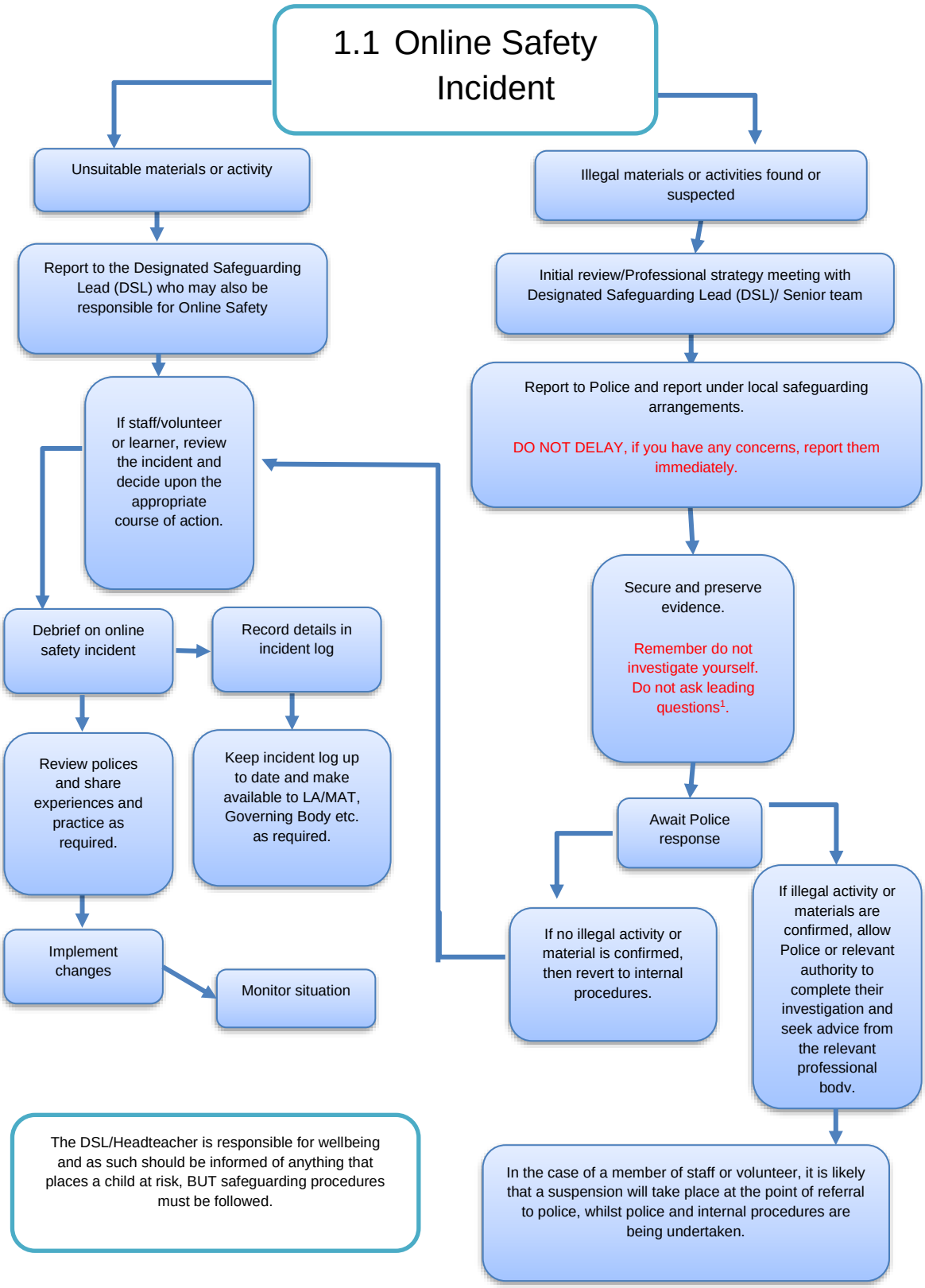
- # Reporting and responding

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all incidents will be logged in CPOMS
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm, the incident must be escalated through the agreed school safeguarding procedures.
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority / MAT
- where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
    - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
    - record 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
    - 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
        - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident

- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; etc.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions
- learning from the incident (or pattern of incidents) will be provided to:
    - staff, through regular briefings
    - learners, through assemblies/lessons
    - parents/carers, through newsletters, school social media, website
    - governors, through regular safeguarding updates
    - local authority/external agencies, as relevant

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.


1.1 Online Safety Incident
Unsuitable materials or activity
Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety
If staff/volunteer or learner, review the incident and decide upon the appropriate course of action.
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.
Implement changes
Monitor situation
Illegal materials or activities found or suspected
Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team
Report to Police 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 ask leading questions[1].
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 bodv.
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.
The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

- **School actions**

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

- # Responding to Learner Actions

Incidents	Refer to class teacher	Refer to Online Safety Lead	Refer to Headteacher	Refer to Police/Social Work	Refer to local authority technical support for advice/action	Inform parents/carers	Remove device/ network/internet access	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal		X	X	X					
Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords	X	X							
Corrupting or destroying the data of other users.	X	X	X						
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X			
Unauthorised downloading or uploading of files or use of file sharing.	X	X							
Using proxy sites or other means to subvert the school's filtering system.	X	X	X		X				

Accidentally accessing offensive or pornographic material and failing to report the incident.	X	X	X		X	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					
Unauthorised use of digital devices (including taking images)	X	X	X						
Unauthorised use of online services		X	X						
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		X	X			X			
Continued infringements of the above, following previous warnings or sanctions.		X	X			X			

- Responding to Staff Actions

Incidents	Refer to Online Safety Lead	Refer to Headteacher	Refer to local authority	Refer to Police	Refer to Technical Support Staff for action re filtering, etc.	Issue a 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				
Deliberate actions to breach data protection or network security rules.	**X**	**X**						
Deliberately accessing or trying to access offensive or pornographic material		**X**	**X**	**X**	**X**			
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	**X**	**X**						
Using proxy sites or other means to subvert the school's filtering system.	**X**	**X**			**X**			
Unauthorised downloading or uploading of files or file sharing	**X**	**X**			**X**			
Breaching copyright or licensing regulations.	**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**						

Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature		X	X					
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers		X	X	X				
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail		X						
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner	X	X						
Actions which could compromise the staff member's professional standing		X	X					
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		X	X					
Failing to report incidents whether caused by deliberate or accidental actions		X	X					
Continued infringements of the above, following previous warnings or sanctions.								

- Online Safety Education Programme

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. 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 for all year groups is taught through Computing, PSHE and other bespoke lessons, following the Education for a Connected Work Framework CIS/DCMS and regularly taught in a range of contexts.
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- it incorporates relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- 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.
- Key online safety messages should be reinforced as part of a planned programme of lessons.
- 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
- learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school
- staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that learners 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.
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

• Staff/volunteers

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours
- this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- the Online Safety Lead will provide advice/guidance/training to individuals as required.

• Governors

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

- attendance at training provided by the local authority or other relevant organisation
- participation in school training / information sessions for staff or parents

A higher level of training will be made available to (at least) the Online Safety Governor to include

- Cyber-security training (at least at a basic level)
- Training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and review.

• 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

Technology

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.
- 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).

Filtering & Monitoring

The school filtering and monitoring provision is agreed by senior leaders, governors and 24/7 Technology Solutions and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and 24/7 technology solutions will have technical responsibility

The filtering and monitoring provision is reviewed (at least annually) by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of 24/7 technology solutions.

Checks on the filtering and monitoring system are carried out by 24/7 technology solutions with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or new technology is introduced

Filtering

- the school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE.

- illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective
- there is a clear process in place to deal with, and log, requests/approvals for filtering changes
- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.

Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services through 24/7 Technology.
- An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with safeguarding policy and practice
- Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.
- breaches are flagged immediately to 24/7 Technology and are communicated with the Headteacher.

Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements

- responsibility for technical security resides with SLT who may delegate activities to identified roles.
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT service provider and will be reviewed, at least annually, by the SLT/Online Safety Group
- password policy and procedures are implemented. (consistent with guidance from the National Cyber Security Centre)
- the security of their username and password and must not allow other users to access the systems using their log on details.
- all users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone.

- the administrator passwords for school systems are kept securely by 24/7
- there is a risk-based approach to the allocation of learner usernames and passwords.
- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- appropriate security measures are in to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software.
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- 24/7 is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
- use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them
- staff members are not permitted to install software on a school-owned devices without the consent of the SLT/IT service provider
- removable media is not permitted unless approved by the SLT/IT service provider
- systems are in place to control and protect personal data and data is encrypted at rest and in transit
- mobile device security and management procedures are in place
- guest users are provided with appropriate access to school systems based on an identified risk profile.

• 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 individual use	School owned for multiple users	Authorised device[3]	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	No[1]	Yes[2]	Yes[3]
Full network access	Yes	Yes	Yes	No	No	No
Internet only				No	No	No
No network access				Yes	Yes	Yes

[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.

[3] Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

- Social media

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 learners through:

- ensuring that personal information is not published
- clear reporting guidance, including responsibilities, procedures and sanctions
- risk assessment, including legal risk
- guidance for learners, parents/carers

School staff should ensure that:

- no reference should be made in social media to learners, parents/carers or school staff
- 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
- they act as positive role models in their use of social media

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

- a process for approval by senior leaders
- clear processes for the administration, moderation, 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.

- Personal use
  - personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, 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
  - the school permits reasonable and appropriate access to personal social media sites during school hours using personal equipment

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.

• Digital and video images

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
- staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes
- 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/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners 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, storage, distribution and publication of those images
- care should be taken when sharing digital/video images that learners are appropriately dressed
- learners must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy . This is outlined in the Parent/Carer Acceptable Use Agreement.
- learners' 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 learners are taken for use in school or published on the school website/social media.
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy
- images will be securely stored in line with the school retention policy
- learners' work can only be published with the permission of the learner and parents/carers.

- # Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school:

- has a Data Protection Policy.
- implements the data protection principles and can demonstrate that it does so
- has paid the appropriate fee to the Information Commissioner's Office (ICO)
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest.
- has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed
- has an 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule" supports this
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- provides staff, parents, volunteers, teenagers, and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice
- has procedures in place to deal with the individual rights of the data subject,
- carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier
- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors
- understands how to share data lawfully and safely with other relevant data controllers.
- has clear and understood policies and routines for the deletion and disposal of data
- reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- has a Freedom of Information Policy which sets out how it will deal with FOI requests

- provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff

When personal data is stored on any mobile device or removable media the:

- data will be encrypted, and password protected.
- device will be password protected.
- device will be protected by up-to-date endpoint (anti-virus) software
- data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Staff must ensure that they

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- only use encrypted data storage for personal data
- will not transfer any school personal data to personal devices, using only online access when working from home.
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

Appendices

A - Webfiltering Provision

B - Learner Acceptable Use Agreement Template – KS2

C - Learner Acceptable Use Agreement Template – for younger learners (Foundation/KS1)

D - Parent/Carer Acceptable Use Agreement Template

E- Staff/Governor/Community Users Acceptable Use Policy Agreement Template

F - Responding to incidents of misuse – flow chart

G – Useful Links

H- Glossary of Terms

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		The list is part of the Diladele B.V

assessed list of unlawful terrorist content, produced on behalf of the Home Office'		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		All schools have the option of managing their own Block and Permit policies.

the filter themselves to permit or deny access to specific content		
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 –		We implement a standard block page, and schools can

the ability to report inappropriate content for access or blocking		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 - Learner Acceptable Use Agreement Template – for KS2

Pupil Acceptable Use Agreement – KS2

- ✓ I will only use ICT in school for school purposes.
- ✓ I will not tell other people my ICT passwords.
- ✓ I will only open/delete my own files.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my parent, teacher or Cyber Buddy immediately.
- ✓ I will not give out my own or anyone else's details such as: name, phone number or home address or post pictures, without their permission. I will not arrange to meet someone contacted over the internet.
- ✓ I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- ✓ I understand that the school will check my files and will keep track of the Internet sites I visit and that my parent/ carer contacted if a member of school staff is concerned about my e-Safety.
- ✓ I will always tell an adult or my Cyber Buddy straight away if I am upset or worried about something that has happened online. I will save any messages that have upset me so I can show them to who I tell as they will be able to help.
- ✓ I will not bring to school any communication technology, including phones, tablets, or internet-connected watches.
- ✓ Where work is protected by copyright, I will not try to download copies (including music and videos).
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ✓ I understand that any online behaviour outside of school might affect the school or other members of the school and will adhere to this agreement.

Pupil Acceptable Use Agreement - Agreement

Dear Parent/ Carer

Technology, including the internet, email and mobile technologies, etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any connected technology.

Please read and discuss these Online Safety rules with your child and return the slip at the bottom of this page. The rules can be kept at home so that you can refer to them when your child is using technology. If you have any concerns or would like some explanation please contact the head teacher at school.

✂---

Pupil Signature

We have discussed this and …………………………………….........(child name) agrees to follow the Online Safety rules and to support the safe use of technology at Our Lady's School.

Parent/ Carer Signature …….…………………..………………………….

Child Signature …….…………………..………………………….

Class …………………………………. Date ………………………………

Appendix C - Pupil Acceptable Use Agreement Template – for younger learners (Foundation/KS1)

Pupil Acceptable Use Agreement – EYFS/KS1

This is how we stay safe when we use computers:

- ✓ I will ask a teacher or suitable adult if I want to use the computers / tablets
- ✓ I will only use activities that a teacher or suitable adult has told or allowed me to use
- ✓ I will take care of the computer and other equipment
- ✓ I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- ✓ I will tell a teacher or suitable adult if I see something that upsets me on the screen
- ✓ I know that if I break the rules I might not be allowed to use a computer / tablet.

Signed (child):

Signed (parent):

Appendix D - Parent/Carer Acceptable Use Agreement Template

Parent/Carer Acceptable Use Agreement – online Safety Rules

- ✓ I will monitor my child's use of the Internet outside school using any technology for example consoles, mobile phones, laptops and by adhering to our Acceptable Use Policy.
- ✓ I will discuss online safety issues with my children, supporting the school in its online safety approaches and reinforcing appropriate behaviour at home.
- ✓ I will liaise with school if they suspect or have identified that my child is conducting risky behaviour online.
- ✓ I will not allow my child to lie about their age and access social networking sites e.g. Facebook which are designed for older children and adults.
- ✓ I will not discuss school or personal matters about other children online: e.g Facebook posts/Tweets about incidents involving other children/teachers/parents.
- ✓ I will not publish any pictures or videos of school events or those taken in school if they contain children other than my own.
- ✓ I will not contact any staff member through social media, and use the school office email should I need to.
- ✓ I will make sure that all online contact with other children and adults is responsible, polite and sensible.
- ✓ I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- ✓ I understand that failure to adhere to these rules **may** result in referral to outside agencies.
- ✓ I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Parent Acceptable Use Agreement - Agreement

Dear Parent/ Carer

ICT including the internet, email and mobile technologies, etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

As parents and carers it is our responsibility to ensure we keep our children and the wider school community safe whilst using technology.

✂----------

Parent Signature

I/We have read and understood and agree to follow the Parent Online Safety rules and to support the safe use of ICT for my Child.

I/We agree that if I/we take pictures or video at, or of, school events which include images of children other than my/our own, I/we will not distribute, post or share these on any social media platform.

Parent/ Carer Signature …….…….

Print Name.....

Child Name (s) .....

Class(es) …… Date ……

- # Appendix E – Use of Digital Images Agreement

- **Use of Digital Video Images**

The use of digital or video images plays an important part in learning activities. Learners and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and on social media.

The school will comply with the Data Protection Act and request parent's/carer's permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

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/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents/carers to agree.

Images are stored in on individual devices and backed up into the cloud storage. Sometimes we will publish images on Twitter or the school's website. All members of staff with access to the cloud storage will be able to access the pictures. If you would like an image removed please contact the school office.

Parent Signature

Parent/Carers Name:

Pupil Name:

I agree to the school taking digital/video images of my child/children (please tick). ☐

I agree to these images/videos being published on the school website and/or school social media: ☐

Signed:

Date:

Appendix F - Staff, Governor and Community Users Acceptable Use Policy Agreement Template

School Policy

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

This acceptable use policy is intended to ensure:

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

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

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

- I will be professional in my communications and actions when using school systems:
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not communicate or add any parent or pupil on social media unless they are a close family member or personal friend.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will not use personal email addresses on the school's ICT systems
- I will not use the school network with personal devices.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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

- I understand that this acceptable use policy applies not only to my work and use of school's digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/Trustees and/or the Local Authority and in the event of illegal activities the involvement of the police.

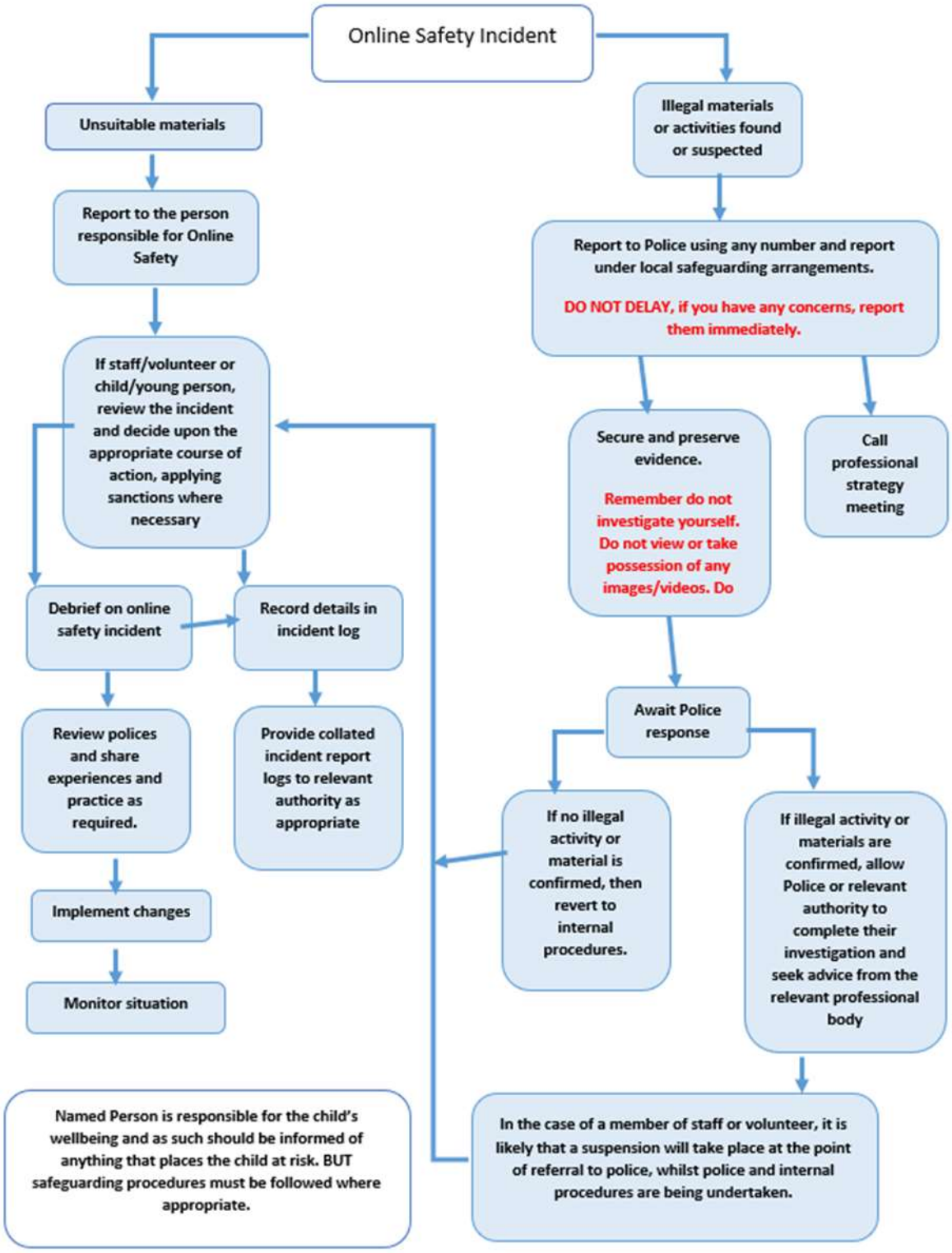
I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: .....

Signed: .....

Date: .....

Appendix G - Responding to incidents of misuse – flow chart



Appendix H - Useful Links

UK Safer Internet Centre
Safer Internet Centre – https://www.saferinternet.org.uk/
South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Revenge Porn Helpline - https://revengepornhelpline.org.uk/
Internet Watch Foundation - https://www.iwf.org.uk/
Report Harmful Content - https://reportharmfulcontent.com/
Harmful Sexual Support Service

CEOP
CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Others
LGfL – Online Safety Resources
Kent – Online Safety Resources page
INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/
UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety

Tools for Schools / other organisations
Online Safety BOOST – https://boost.swgfl.org.uk/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/
360Data – online data protection self-review tool: www.360data.org.uk
SWGfL Test filtering - http://testfiltering.com/
UKCIS Digital Resilience Framework - https://www.gov.uk/government/publications/digital-resilience-framework

Bullying/Online-bullying/Sexting/Sexual Harassment
Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/
SELMA – Hacking Hate - https://selma.swgfl.co.uk
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388
DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
Childnet – Cyberbullying guidance and practical PSHE toolkit: http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit
Childnet – Project deSHAME – Online Sexual Harrassment
UKSIC – Sexting Resources
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm
Ditch the Label – Online Bullying Charity

Diana Award – Anti-Bullying Campaign

Social Networking

Digizen – Social Networking
UKSIC - Safety Features on Social Networks
Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum

SWGfL Evolve - https://projectevolve.co.uk
UKCCIS – Education for a connected world framework
Department for Education: Teaching Online Safety in Schools

Teach Today – www.teachtoday.eu/
Insafe - Education Resources

Professional Standards/Staff Training

DfE – Keeping Children Safe in Education
DfE - Safer Working Practice for Adults who Work with Children and Young People
Childnet – School Pack for Online Safety Awareness
UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure/Technical Support/Cyber-security

UKSIC – Appropriate Filtering and Monitoring
SWGfL Safety & Security Resources
Somerset - Questions for Technical Support
SWGfL - Cyber Security in Schools.
NCA – Guide to the Computer Misuse Act
NEN – Advice and Guidance Notes

Working with parents and carers

SWGfL – Online Safety Guidance for Parents & Carers
Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops/education
Internet Matters

Prevent

Prevent Duty Guidance
Prevent for schools – teaching resources
Childnet – Trust Me

Research

Ofcom –Media Literacy Research

Appendix I - Glossary of Terms

AUP/AUA	Acceptable Use Policy/Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of National Crime Agency, UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ICO	Information Commissioners Office
ICT	Information and Communications Technology
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MAT	Multi Academy Trust
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.
UKCIS	UK Council for Internet Safety
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol