Brentry Primary School

Online Safety Policy

Contents

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by a working group including:

- Head Teacher
- Computing Lead
- Staff
- Governor
- Parent

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:	*Senior Leadership Team & Governors*
Monitoring will take place at regular intervals:	*Annually in July*
The Governing Body 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:	*Annually at Term 6 FGB*
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:	*December 2025*
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*Hannah Jack, Computing Lead* *Geraint Clarke, Head Teacher* *Governors* *LA Safeguarding Team* *Police*

The school will monitor the impact of the policy using:

- Logs of reported incidents

- Monitoring logs of internet activity (including sites visited) / filtering which is reported by Bristol City Council.

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Head Teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the *school* but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. 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 out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals 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*. The role of the Online Safety *Governor* will include:

- regular meetings with the Computing Lead
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors meeting

Head Teacher:

- The *Head Teacher* has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the *Computing Lead.*
- The Head Teacher and 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 Head Teacher and Senior Leaders are responsible for ensuring that the Computing 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 Head Teacher & Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety-monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.*
- *The Senior Leadership Team will receive regular monitoring reports from the Computing Lead.*

Computing Lead:

- leads the Online Safety Group
- 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
- liaises with the Local Authority / relevant body
- liaises with school IT provider

- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with Online Safety *Governor* to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of *Governors*
- reports regularly to Senior Leadership Team

Managed ICT Provider:

Brentry Primary School external ICT provider (Soltech), is responsible for ensuring:

- that the *school's* technical infrastructure is secure and is not open to misuse or malicious attack
- that they meet required online safety technical requirements and any *Bristol City Council* Online Safety Policy that may apply.
- that users may only access the networks and devices through a properly enforced password protection
- the Bristol City Council filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- 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 / internet / remote access / email is monitored in order that any misuse / attempted misuse can be reported to the Head Teacher and Computing Lead to investigate / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school

Please see Appendix 1 for how Soltech adhere to the appropriate filtering for educational settings.

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

- they have read, understood and signed the Staff Acceptable Use Policy
- they report any suspected misuse or problem to the Head & Computing Lead for investigation / action / sanction
- all digital communications with students / 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 schools online safety expectations and follow the Computing Acceptable Use Charter
- they monitor the use of digital technologies used in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- 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

Designated Safeguarding Lead

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

Safeguarding Team

The Safeguarding Team provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body

Members of the Safeguarding Team will assist the Computing Lead with:

- the production / review / monitoring of the school Online Safety Policy / documents.
- adhering to Bristol City Council filtering policy and requests for filtering changes.

- monitoring the online safety curricular provision – ensuring relevance, breadth and progression
- reviewing incident logs
- reviewing feedback from stakeholders – including parents / carers and the students / pupils about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

Pupils

- are responsible for using the school digital technology systems in accordance with the Computing Acceptable Use Charter
- 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 school's Online Safety Policy covers their actions out of school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature. 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 and class pages
- their children's personal devices in the school (where this is allowed)

Community Users

Community Users who access school systems / website as part of the wider *school* provision will be expected to sign a Community User AUA before being provided with access to school systems.

Policy Statements

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. 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
- Key online safety messages should be reinforced as part of a planned programme of assemblies, digital literacy lessons and pastoral activities
- Pupils should be taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be helped to understand the need for the pupil Online Safety Charter 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 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.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that Soltech via Bristol City Council can temporarily remove those sites from the filtered list for the

period of study. Any request to do so, should be auditable, with clear reasons for the need. 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:

- Curriculum activities
- Letters, newsletters, web site
- Parents / Carers sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community

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:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly

- 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.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Computing Lead will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) 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 / INSET days.
- The Computing Lead will provide advice / guidance / training to individuals as required.

Training – Governors / Directors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee / 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 / National Governors Association / or other relevant organisation (e.g. SWGfL).
- Participation in school / academy training / information sessions for staff or

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. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems

- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users (at KS2 and above) will be provided with a username and secure password by Soltech who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must *also be available to the Head Teacher and Computing Lead.*
- Soltech are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by Bristol City Council. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- *The* school has provided differentiated user-level filtering allowing different filtering levels for– staff & pupils
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the Computing Lead. **Such items should be reported to Soltech IT Support via the helpdesk for checking and remediation work as necessary. Actual security breaches found by school staff should also be reported in accordance with the school's security guidelines. Security breaches found by IT Support will be reported to the Head Teacher and/or Computing Lead.**
- Appropriate security measures are in place via Bristol City Council filtering powere by NetSweeper to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

- Guests will only be given access to the school WIFI, there will be no access to the school server.
- An agreed policy is in place, Acceptable User Policy – Staff, that forbids staff from downloading executable files and installing programmes on school devices.
- All staff are given GDPR compliant memory sticks that can be used where necessary to take personal data off site if not using a school laptop.

Mobile Technologies

Mobile technology devices may be school owned 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.

	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*	*Yes Y5 & Y6 ONLY*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*
Internet only	-	-	-	*No*	*Yes*	*Yes*
No network access	-	-	-	*No*	-	-

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer

term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

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

General Data Protection Regulation

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that personal data:

Brentry Primary School is fully committed to compliance with the requirements of the EU General Data Protection Regulation. The school will therefore aim to ensure that all employees, contractors, agents, consultants, or partners of the school who have access to any personal data held by or on behalf of the school, are fully aware of and abide by their duties and responsibilities under the Regulation as per the school's Data Protection Policy.

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.
- 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 and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

Communications

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:

Communication Technologies	Staff & other adults				Y5 & Y6 Pupils				
	Not Allowed	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		✓					✓		
Use of mobile phones in lessons			✓		✓				
Use of mobile phones in social time			✓		✓				
Taking photos on mobile phones / cameras		✓			✓				
Use of other mobile devices e.g. tablets, gaming devices		✓			✓				
Use of personal email addresses in school , or on school network			✓		✓				
Use of school email for personal emails	✓				✓				
Use of messaging apps			✓		✓				
Use of social media			✓		✓				
Use of AI		✓			✓				

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the 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.
- Any digital communication between staff and pupils or parents / carers (email, social media, chat, blogs, 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 social media must not be used for these communications.

- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

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

School staff should ensure that:

- No reference should be made in social media or messaging app to pupils, 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 or local authority
- Governors have a code of conduct which includes professional use of social media

- 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 there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- 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 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's use of social media for professional purposes will be checked regularly by the Head Teacher and Online Safety Group to ensure compliance with the school policies

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are

however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

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

User Actions		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					X
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

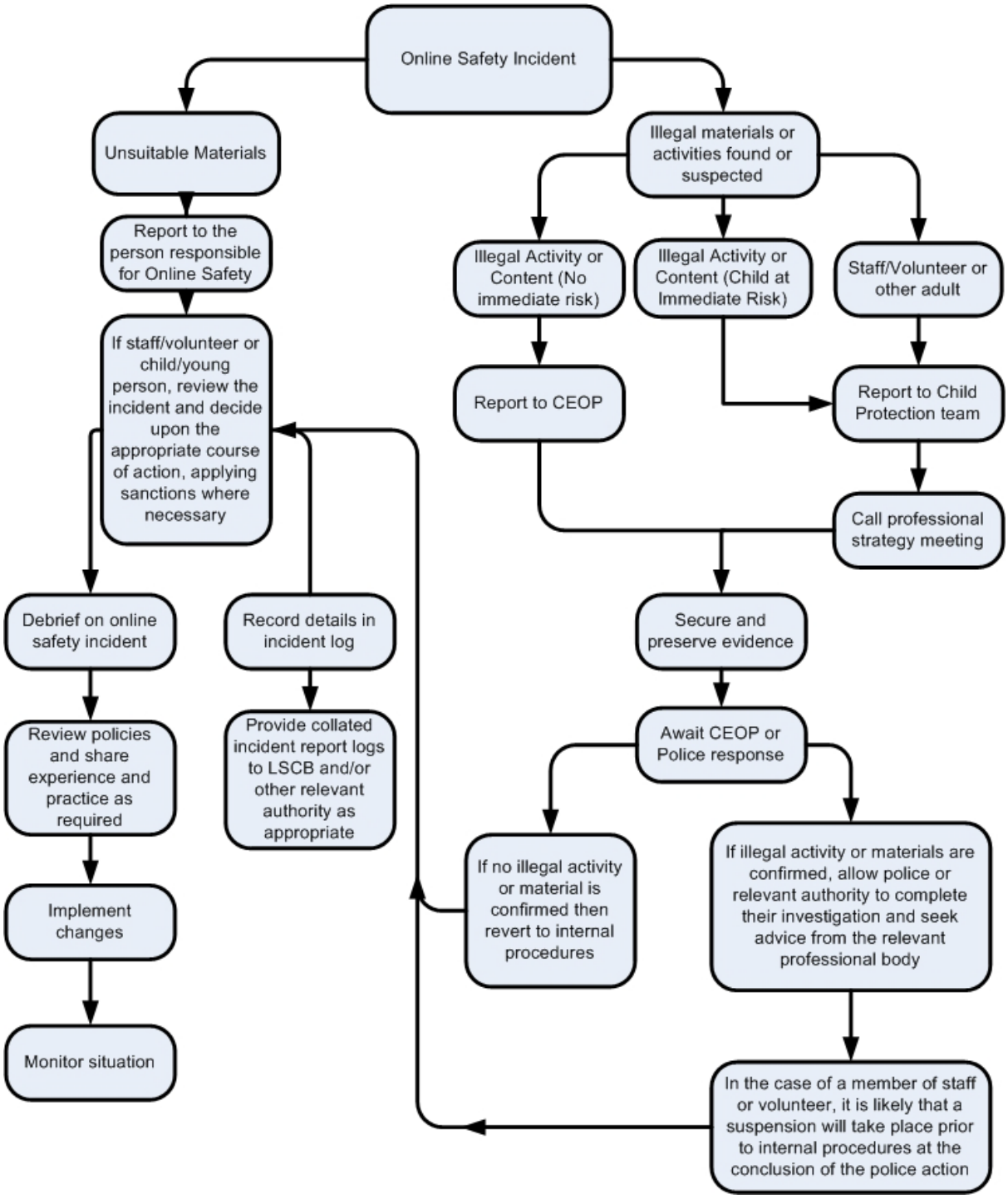
Using school systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy				X	
Infringing copyright					X
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files					X
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		X			
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping / commerce				X	
File sharing		X			
Use of social media		X			
Use of messaging apps		X			
Use of video broadcasting e.g. Youtube		X			

Responding to incidents of misuse

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).

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.



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 / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- 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 / Academy Group or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - racist or discriminating 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.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

	Actions / Sanctions									
Pupils Incidents	CPOMS	Refer to class teacher	Refer to KS Lead	Refer to Head Teacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X		X		X	X			
Unauthorised use of non-educational sites during lessons		X					X	X	X	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	
Unauthorised downloading or uploading of files	X	X							X	
Attempting to access or accessing the school network, using another pupil's account		X					X		X	
Attempting to access or accessing the school network, using the account of a member of staff		X		X			X		X	X
Corrupting or destroying the data of other users		X							X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X		X			X			X
Continued infringements of the above, following previous warnings or sanctions				X			X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school				X			X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident		X				X			X	
Deliberately accessing or trying to access offensive or pornographic material	X			X		X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act									X	

Actions / Sanctions

	Refer to line manager	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
		X	X	X	X	X	X	X
	X					X		
	X					X		
		X				X		
		X				X		X
		X				X		X
		X				X		X
		X	X			X		X
	X					X		
	X					X		
		X				X		
		X			X	X		
		X	X		X	X		X
	X					X		
		X				X		X

APPENDIX 1

Appropriate Filtering for Education settings

UK Safer Internet Centre

June 2020

Filtering Provider Checklist Reponses

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". Furthermore, the Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England 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."

Included within the Scottish Government national action plan on internet safety, schools in Scotland are expected to "have policies in place relating to the use of IT and to use filtering as a means of restricting access to harmful content."

By completing all fields and returning to UK Safer Internet Centre (enquiries@saferinternet.org.uk), the aim of this document is to help filtering providers to illustrate to education settings (including Early years, schools and FE) how their particular technology system(s) meets the national defined 'appropriate filtering standards. Fully completed forms will be hosted on the UK Safer Internet Centre website alongside the definitions

It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision.

Company / Organisation	Soltech IT
Address	Unit 1 Westway Farm, Wick Road, Bishop Sutton, BRISTOL BS39 5XP
Contact details	Sales@soltechit.co.uk
Filtering System	Shield Internet
Date of assessment	12/10/2020

System Rating response

Where a supplier is able to confirm that their service fully meets the issue identified in a specific checklist the appropriate self-certification colour for that question is GREEN.	YES
Where a supplier is not able to confirm that their service fully meets the issue identified in a specific checklist question the appropriate self-certification colour for that question is AMBER.	

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		Zvelo since 2011
• and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)		Yes, as standard
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Yes, as standard

Inappropriate Online Content

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

Content	Explanatory notes – Content that:	Rating	Explanation
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.		As standard, our education profile includes blocking a category named 'Extreme' which includes violence, hate speech and discrimination on the grounds of race, religion, age or sex.
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		As standard, our education profile includes blocking a category named 'Dugs' which includes alcohol, illegal drugs, marijuana, tobacco. Combined with an additional category called 'Addiction', websites displaying or promoting illegal use of drugs or substances are blocked.
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		As standard, our education profile includes blocking a category named 'Extreme' which blocks websites promoting terrorism, terrorist ideologies, violence or intolerance.
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		As standard, our education profile includes blocking categories named 'Malware', 'Anonymisers' and 'Criminal Activities' which blocks sites promoting the compromising of systems including anonymous browsing and other filter bypass

			tools as well as sites hosting malicious content
Pornography	displays sexual acts or explicit images		As standard, our education profile includes blocking a category named 'Pornography/Nudity' and 'Mature' which includes blocking 'Sex and Erotic sites', 'Lingerie', 'Suggestive and Pinup'. All of which ensures websites displaying sexual acts or explicit images are blocked.
Piracy and copyright theft	includes illegal provision of copyrighted material		As standard, our education profile includes blocking a category named 'Piracy and Copyright Theft' which includes illegal provision of copyrighted material
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		As standard, our education profile includes blocking a category named 'Criminal Activities' which blocks websites promoting or displaying deliberate self-harm including suicide and eating disorders
Violence	Displays or promotes the use of physical force intended to hurt or kill		As standard, our education profile includes blocking a category named 'Extreme' and 'Weapons' which includes sites that displays or promotes the use of physical force intended to hurt or kill

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

Soltech IT's education filtering uses advanced categorisation that is automatically updated and continually reassessed into the 140+ categories available.

Regarding the duration and extent of logfile (Internet history) data retention, providers should outline their retention policy.

As standard, log files and associated data is available to access on request. This information can be downloaded and provided to the client. As standard the duration is set to one year and can be increased or reduced in accordance to the clients policy.

Providers should be clear how their system does not over block access so it does not lead to unreasonable restrictions

Soltech IT's filtering system incorporates the categorisation by Zvelo who have be in the industry since 1984 and a member of the IWF since 2011. This intelligent level of filtering results in effective blocking of unwanted websites in line with the client's policy.

Soltech IT can tailor the filtering to each school, for instance a secondary school may allow YouTube whilst a primary may want this blocked. Filtering can also be adjusted in accordance to the role of a person within the school.

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		Filtering is linked to active directory which allows the adjustment of filtering to be easily managed and maintained by either groups or per user basis. Grouping is also linked to the filtering so each year group can have a different level of filtering if required.
• Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, specifically VPN, proxy services and DNS over HTTPS.		The category 'Anonymizer' is blocked as standard which prevents access to sites used to circumvent filtering. Firewall rules are also in place to block VPN and proxy services.
• Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content		Filtering customisation is discussed at the prior to installation and periodically reviewed and updated if necessary, in line with the schools request.
• Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		Soltech IT provides the school with an internet provisioning document that highlights the categorises blocked/granted.
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		Soltech IT filtering is managed by a central team who deploy any necessary / appropriate updates to the schools filtering.
• Identification - the filtering system should have the ability to identify users		Soltech IT filtering links in with Active Directory and

		therefore identifies usage on a per user and IP bases.
• Mobile and App content – mobile and app content is often delivered in entirely different mechanisms from that delivered through a traditional web browser. To what extent does the filter system block inappropriate content via mobile and app technologies (beyond typical web browser delivered content)		Soltech IT filtering supports application awareness which allows Soltech IT to inspect traffic from mobile apps and apply filtering rules appropriately.
• Multiple language support – the ability for the system to manage relevant languages		Soltech IT filtering system support multiple languages
• Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices		Soltech IT filtering system does not require any software to be installed on any device, with the exception of HTTPS filtering which requires a SSL certificate.
• Reporting mechanism – the ability to report inappropriate content for access or blocking		The school would contact Soltech IT for recategorization.
• Reports – the system offers clear historical information on the websites visited by your users		Soltech IT filtering includes real-time monitoring and historical reporting. Real-time alerts is also available that are emailed to a designated contact at the school.

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*".[1]

Please note below opportunities to support schools (and other settings) in this regard

Soltech IT has been providing advice and solutions to the education sector since 2009 during which time have worked with schools to ensure appropriate safeguarding measures surrounding IT are recommended. From initial audit of systems and ongoing account management, Soltech IT provide ongoing advice and recommendations regarding the safe and effective use of IT in schools.

[1] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

Provider Self-Certification Declaration

In order that schools can be confident regarding the accuracy of the self-certification statements, the supplier confirms:

- that their self-certification responses have been fully and accurately completed by a person or persons who are competent in the relevant fields
- that they will update their self-certification responses promptly when changes to the service or its terms and conditions would result in their existing compliance statement no longer being accurate or complete
- that they will provide any additional information or clarification sought as part of the self-certification process
- that if at any time, the UK Safer Internet Centre is of the view that any element or elements of a provider's self-certification responses require independent verification, they will agree to that independent verification, supply all necessary clarification requested, meet the associated verification costs, or withdraw their self-certification submission.

Name	Stuart Clark
Position	Director
Date	12/10/2020
Signature