Roman Road Primary School

Online Safety Policy

Reviewed by Roman Road Primary School:	September 2022
Date next full review is due:	September 2023

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by the Computing Leader & agreed by the Head Teacher.

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Governing Body on:	*14th November 2018*
The implementation of this Online Safety policy will be monitored by the Computing Leader	*Mr A Allsop*
Monitoring will take place at regular intervals.	*Ongoing*
The Governing Body will receive a report on the implementation of the Online Safety Policy generated by the Computing Leader (which will include anonymous details of online safety incidents) at regular intervals:	*Annually*
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:	*September 2023*
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*LA Safeguarding Officer, LADO, Police*

The school will monitor the impact of the policy using:

- Logs of reported incidents;
- Monitoring logs of internet activity (including sites visited) / filtering;
- Internal monitoring data for network activity.

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers / Principals 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 online-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. The Governor responsible for Safeguarding will be informed of issues where there is need to.

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Computing Leader
- The Headteacher and (at least) another member of the Senior Leadership Team (Computing Leader) are 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 Computing Leader 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 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 Headteacher will receive regular monitoring reports from the Computing Leader which are used to inform the Governors when required.

Online Safety Officer – Computing Leader

- leads the Computing Group which encompasses Online Safety;
- 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 or relevant body;
- liaises with school technical staff (Omnicom);
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments;
- meets regularly with the Headteacher to discuss current issues, review incident logs and filtering / change control logs;
- reports regularly to Senior Leadership Team and Head Teacher;
- reports to the Governing body when required.

Network Manager – Currently Omnicom (Curriculum) and Gateshead Council (Administration)

The Computing Leader will inform the Contractor that we use to make sure:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack;
- that the school meets required online safety technical requirements and any Local Authority/ other relevant body Online Safety Policy / Guidance that may apply;
- that users may only access the networks and devices through a properly enforced password;
- the 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 / school website/ remote access / email is regularly monitored in order that any misuse or attempted misuse can be reported to the Head Teacher and Computing Leader for investigation / action / sanction;
- that monitoring software / systems are implemented and updated as agreed in school policies.

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 (AUP);
- they report any suspected misuse or problem to the Headteacher (DSL) / Computing Leader for investigation / action / sanction.
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems;
- online safety issues are embedded in all aspects of the curriculum and other activities;
- there are especially links with the Relationships and Sex Education curriculum;
- pupils understand and follow the Online Safety Policy and acceptable use policies;
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices;
- 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;
- use Google Classroom, when needed for home learning, in a professional manners and deal with any inappropriate comments (including cyberbullying) if it occurs.

Designated Safeguarding Lead / Designated Person

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 including child on child.

Computing Group

The Computing Group provides a consultative mechanism with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. Members of the Computing Group will assist the Computing Leader (Online Safety Lead) with:

- the production / review / monitoring of the school Online Safety Policy / documents;
- mapping and reviewing the online safety / digital literacy curricular provision – ensuring relevance, breadth and progression;
- assisting staff with the teaching of online safety;
- consulting stakeholders – including parents / carers and the pupils about the online safety provision;
- monitoring improvement actions.

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement;
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- will be expected to know and understand the rules on the use of mobile devices (including IPads), camcorders and digital cameras. They should also know and understand the rules on the taking / use of images and on cyberbullying;
- 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, if related to their membership of the school;
- understand that inappropriate keystrokes and usage will be identified through the monitoring software;
- log on to the laptop machines using a their username and password. This is not possible with Ipads, so a staff system of recording is in place.

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' 'sessions, newsletters, letters, Facebook page and the website. Parents and carers will also 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;
- the website and Facebook page.

Visitors

Users who access school computer systems (desktop and laptop machines) and/or website as part of the wider school provision will be assigned a traceable user name and referred to the AUP which they will sign to agree use of.

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 / digital literacy 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 is incorporated within the Computing Scheme. This links to the targets in the RSE scheme
  (Various elements must be continually re-inforced such as child on child abuse – sexting, cyberbullying / not knowing who you are communicating with/ age limits for social media/ inappropriate games/ dangers of viruses of different types etc)
- Key online safety messages will be reinforced as part of assemblies and pastoral activities;
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information;
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making;
- Pupils should be helped to understand the need for the pupil 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 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 triggering alerts. Agreement to use such sites could be given after discussion with the Computing Leader. This will be recorded and signed as agreed.
- Pupils must realise that the use of Google Classroom for home learning (when needed) must be used in sensible way as if it was a school lesson. Children must not engage in formal of behaviour which will upset others eg. cyberbullying.

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 online 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;
- Use of school social media site - Facebook;
- Parent sessions;
- High profile campaigns e.g. Safer Internet Day;
- Reference to the relevant web sites.

Education & Training – Staff / Volunteers

Staff and volunteers must adhere to the Acceptable Use Policy (AUP) which outlines the ways staff must use the technology.

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:

- Formal training will be made available to staff regularly. Some online elements will be contained in the annual Safeguarding updates. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out.
- All new staff will receive guidance, 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 Leader will receive regular updates 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 (Online Safety Leader) (or other nominated person) will provide advice / guidance / training to individuals as required.

Training – Governors

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

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

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 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 discussions with the ICT providing company (Omnicom) about school technical systems;
- Servers, wireless systems and cabling are securely located and physical access restricted;
- All users will have clearly defined access rights to school technical systems and devices;
- All users will be provided with a username and password by Computing Leader 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 Computing systems, used by the Network Manager (or other person) must also be available to the Headteacher;

- Omnicom is 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 (eg. child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored;
- Internet filtering / monitoring ensures that children are safe from terrorist and extremist material when accessing the internet;
- The Computing Leader regularly monitors and records the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Policy and Pupil's Acceptable Use Policy which they sign to agree with;
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed. (report to Computing Leader for technical incidents or follow GDPR policies for data breach)
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software;
- The Acceptable Use Policy is in place regarding the extent of personal use that users (staff) are allowed on school devices that may be used out of school;
- Staff/pupils are forbidden from downloading executable files and installing programmes on school devices;
- The Acceptable Use Policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technologies

Mobile technology devices are school owned and provided to the staff under the guidance of the Computing Lead. These might include: IPad, 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 (Google Classroom) 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. Rules about mobile technologies are 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, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies are part of the school's Online Safety education programme.

Unless it is in exceptional circumstances all users within school will not be allowed to connect personal devices other than memory sticks to the school network without permission from the Headteacher.

Personal memory sticks such as those containing resources are allowed but must not hold personal data and must be virus checked.

The school Acceptable Use Policy (AUP) for staff and pupils will give consideration to the use of mobile technologies

School Owned Equipment

The AUP also determines how mobile technologies that are owned by the school can be used and when/if they are allowed off site.

Each member of teaching staff has an encrypted memory stick which must be used for personal and confidential data.

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 or the dangers of sending their own image to other people including as a result of sexting;
- Children can opt out of having their photo take;
- 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 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 *pupils* in the digital / video images;
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should be taken on school equipment. (See AUP for further details);
- 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.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current GDPR data protection legislation. The school has various GDPR policies which together with the Acceptable Use Policy cover the requirements.

Users must:

- 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, 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.

	Staff				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Locked in office on entry	Not allowed
Mobile phones may be brought to the school	x						x	
Use of mobile phones in lessons				x				x
Use of mobile phones in social time		x						x
Taking photos on mobile phones / cameras				x				x
Use of other mobile devices e.g. tablets, gaming devices		x						x
Use of personal email addresses in school , or on school network		x						x
Use of school email for personal emails				x				x
Use of messaging apps	**							x
Use of social media	**							x
Use of blogs	Only School Related							Only School Related ones

*<u>** Staff can use their own phone out of class in areas where there are no children present such as the staffroom.</u>*

*<u>*** Children with diabetes need to use a mobile device to monitor their pump. This is done under staff supervision.</u>*

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

- The official school email service may be regarded as safe and secure. Users should be aware that the monitoring system (Smoothwall) will pick 'captures' of words or phrases the system considers may of be a concern. This will provide a screenshot of the e-mail. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school equipment systems (e.g. by remote access);
- Users must immediately report to the Computing Leader, 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. If the communication is child protection or safeguarding based, the DSL must be informed.
- Any digital communication between staff and parents / carers must be professional in tone and content. These communications may only take place on official (monitored) school systems (Microsoft 365 e-mail). Personal email addresses, text messaging or social media must not be used for these communications apart from the School's Facebook account and Text Messaging Service;
- The pupils will not be allowed personal e-mail addressees;
- Pupils will 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 data won't 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 have a duty of care to provide a safe learning environment for pupils and staff. The School, and Local Authority could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, 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 when required;
- Clear reporting guidance, including responsibilities, procedures and sanctions;
- Risk assessment, including legal risk.

School staff must should ensure that:

- No reference should be made in social media by name to pupils, parents / carers or school staff unless specific permission from the parent/carer/staff member has been gained;
- 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.

School Facebook Account:

- Approved by a senior member of staff;
- Three members of staff run the account (currently School Facebook);
- The moderators of the site must take down any inflammatory comments as soon as they have been seen then report them to the Headteacher;
- The Account must only be used for information purposes making sure the detail is appropriate;
- Security settings are checked and are appropriate;
- Parents/Carers must give permission for the account to show pictures of their children.

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.

The school system blocks access to Social Media sites apart from a selected Administration machine which is used for updating the school Facebook page.

THE SCHOOL HAS A SEPARATE SOCIAL MEDIA POLICY.

Dealing with unsuitable / inappropriate activities

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

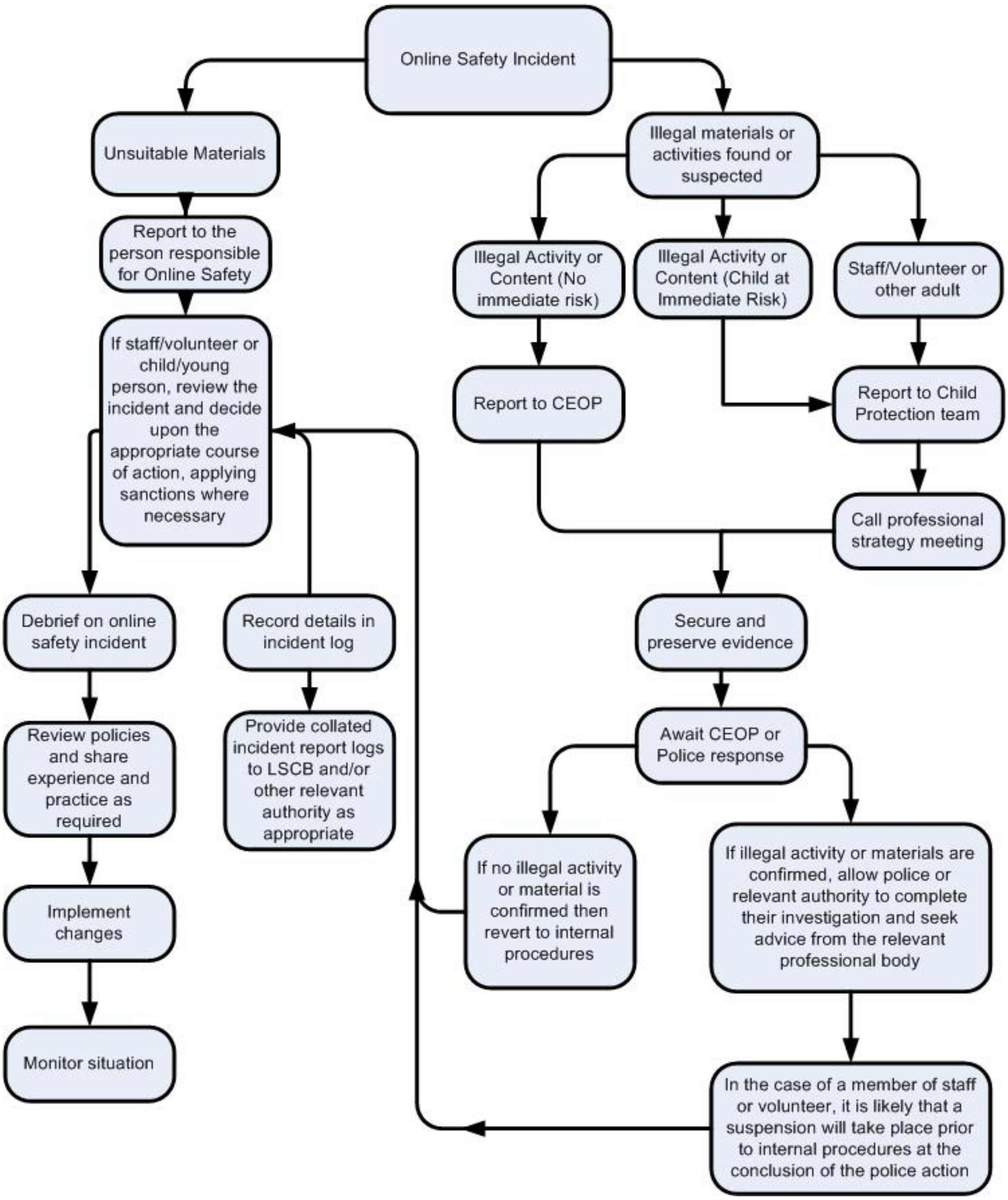
	Promotion of any kind of discrimination				X	X
	threatening behaviour, including promotion of physical violence or mental harm					X
	Promotion of extremism or terrorism					X
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright						X
Revealing or publicising confidential or proprietary information (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.



Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Other Incidents

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

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Any machine involved should be isolated and not be further used. If necessary it maybe taken off site by the police should the need arise.
- the sites and content visited should be recorded by two people (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. If the issue is brought to the attention of the Computing Lead by the Smoothwall system, it may record and store screenshots of the content which can be used in further investigations. (For issues regarding child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures;
    - Involvement by Local Authority or national / local organisation (as relevant);
    - Police involvement and/or action.

The log should be retained securely for evidence and reference purposes.

- 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 including by another child eg. sexting;
    - adult material which potentially breaches the Obscene Publications Act;
    - criminally racist material;
    - promotion of terrorism or extremism;
    - other criminal conduct, activity or materials including newly criminalised acts such as upskirting.
- *Isolate the computer in question as best you can. An Ipad can be put on flight mode. If this can't be done, then the machine should be put off. Any other action may hinder a later police investigation.*
- *Staff must not view the images or forward them on.*

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.

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

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

Actions / Sanctions

Staff Incidents	Refer to Computing Leader	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

Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Inappropriate personal use of the internet / social media / personal email		x	x		x		x	x
Unauthorised downloading or uploading of files	x	x				x	x	
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	x	x				x		
Careless use of personal data e.g. holding or transferring data in an insecure manner	x	x	x			x		
Deliberate actions to breach data protection or network security rules	x	x	x			x	x	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x	x	x		x		x
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x	x			x	x	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils			x					
Actions which could compromise the staff member's professional standing			x					
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			x					
Using proxy sites or other means to subvert the school's filtering system	x	x			x	x		
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x	x		x			
Deliberately accessing or trying to access offensive or pornographic material			x					
Breaching copyright or licensing regulations (Additionally, check with Gateshead Data Protection Officer for advice.)		x						
Continued infringements of the above, following previous warnings or sanctions			x					x

Acknowledgements

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School Online Safety Policy Template and of the 360 degree safe Online Safety Self Review Tool:

- Members of the SWGfL Online Safety Group
- Avon and Somerset Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- NEN / Regional Broadband Grids

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in April 2018. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material.