AMBERLEY PRIMARY SCHOOL

Online Safety Policy

Agreed: September 2026

Review date: September 2027

Online Safety (Digital Safety)
Amberley Primary School

Date of publication: September 2023 Review date: September 2024

Schedule for Development / Monitoring / Review

This online safety policy was approved by the Governing Body on:	September 2025
The implementation of this online safety policy will be monitored by:	The Head teacher, Computing Coordinators and the School Governing Body.
Monitoring will take place 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 2026
Should serious online safety incidents take place, the following external persons / agencies should be informed:	MASH, CEOP, The Police.

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 tothe searching for and of electronic devices and the deletion of data (see appendix for template policy). 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.

The school identifies that the breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

Content: being exposed to illegal, inappropriate or harmful content. For example, pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact: being subjected to harmful online interaction with other users. For example, child on child pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit children for sexual, criminal, financial or other purposes.

Conduct: personal online behaviour that increases the likelihood of, or causes, harm. For example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

We recognise that technology, and the risks and harms related to it, evolve and change rapidly. The school will carry out an annual review of our approaches to online safety, supported by an annual risk assessment which considers and reflects the risks our children face.

The headteacher and DSL will be informed of online safety concerns. The named governor for safeguarding will report on online safety practice and incidents, including outcomes, on a regular basis to the wider governing board.

We use a wide range of technology. This includes computers, laptops, tablets and other digital devices, the internet, our learning platform, intranet and email systems.

All school owned devices and systems will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.

We recognise the specific risks that can be posed by mobile and smart technology, including mobile/smart phones, cameras and wearable technology. In accordance with the current KCSIE documents, the school has appropriate mobile and smart technology, image use, online and acceptable use policies in place, which are shared and understood by all members of the community.

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 Computing Link Governor. The role of the Computing Link Governor will include:

- regular meetings with the Computing Co-ordinator(s)
- regular monitoring of online safety incident logs

- regular monitoring of filtering and monitoring logs
- reporting to relevant Governors committee

Headteacher/DSL:

- 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 Co-ordinator.
- The Headteacher (Designated Safeguarding Lead) and Deputy Safeguarding Lead 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 Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher will oversee filtering and monitoring reports sent by North Tyneside. The Headteacher will complete monitoring log, including any actions taken.
- The Headteacher will receive regular monitoring updates from the Computing Co-ordinator.

The DSL has overall responsibility for online safety within the school but will liaise with other members of staff, for example IT technicians, curriculum leads etc. as necessary.

The DSL is trained in online safety issues and is aware of the potential for serious child protection / safeguarding issues to arise from:

- Sharing of personal data.
- Access to illegal / inappropriate materials.
- Inappropriate online contact with adults / strangers potential or actual incidents of grooming.
- Cyber-bullying.

The DSL will respond to online safety concerns reported in line with our child protection and other associated policies, including our anti-bullying, social media and behaviour policies.

Internal sanctions and/or support will be implemented as appropriate.

- Where necessary, concerns will be escalated and reported to relevant partner agencies in line with local policies and procedures. A list of linked policies can be found at the end of this policy.

Computing/ Online safety Coordinators:

- 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 relevant bodies e.g. NTLP, CEOP, CAS, Local Authority.
- Liaises with school technical staff.
- 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.

- Reports regularly to the Headteacher.

Technical staff:

The Computing Subject Leader and Computing Technician is responsible for ensuring:

- 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 protection policy, in which passwords are regularly changed.
- Filtering is applied and updated on a regular basis, through North Tyneside SLA.
- 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.
- Produce filtering reports and send to the Headteacher, on a weekly basis.

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 / Agreement.
- They report any suspected misuse or problem to the Headteacher for investigation, action or 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.
- Staff ensure that pupils understand and follow the online safety and acceptable use policies.
- Staff ensure that 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.

Pupils:

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile devices. 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, if related to their membership of the 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 online student accounts e.g. TTRS.
- Their children's personal devices in the school (where this is allowed).

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. In line with Filtering and Monitoring standards, children must be allowed to become digital citizens and learn to manage risks. 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 is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. The online safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and is provided in the following ways:

- A planned online safety curriculum is provided as part of Computing / PHSE / other lessons and is regularly revisited.
- Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access online 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 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 being blocked. In such a situation, staff can request that the Technical Staff 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 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, social media pages
- Parents / Carers evenings / sessions.
- High profile events / campaigns eg Safer Internet Day.
- Reference to the relevant web sites / publications eg:
  www.digitiallyconfident.org
  www.saferinternet.org.uk
  www.childnet.com/parents-and-carers
  www.thinkyouknow.co.uk
  www.nationalonlinesafety.com

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:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety. 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.
- Supporting community groups eg Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their online safety provision.

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.
- The Computing Coordinator will receive regular updates through attendance at external training events (eg from Northern Learning Grid / 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 meetings.
- The Computing Coordinator will provide advice / guidance / training to individuals as required.
- We will ensure that all staff receive online safety training as part of induction and that ongoing online safety training and update for all staff will be integrated, aligned and considered as part of our overarching safeguarding approach.

Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any THE C&P committee. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (eg Northern Grid/ Digitally Confident).
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

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 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.
- John Wardle 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. Inadequate licensing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered through North Tyneside Council SLAs, using Smoothwall. North Tyneside team act upon information by the Internet Watch Foundation and update filtering accordingly.
- There is a clear process in place to deal with requests for blocking/unblocking websites.
- School technical staff regularly monitors 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 relevant person (John Wardle), as agreed.
- 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.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An agreed 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. (see School Personal Data Policy Template in the appendix for further detail)

Appropriate Filtering and Monitoring

The leadership and relevant staff are:

- Aware of all internet monitoring and filtering systems
- Manage them effectively
- Know how to escalate concerns when they are identified

We will do all we reasonably can to limit children's exposure to online risks through school provided IT systems and will ensure that appropriate filtering and monitoring systems are in place. ***The schools systems are filtered and monitored through North Tyneside council by Smoothwall.***

If children or staff discover unsuitable sites or material, they are required to: *turn off monitor/screen, report the concern immediately to a member of staff, report the URL of the site in the Filtering and Monitoring file.*

All users will be informed that use of our systems can be monitored, and that monitoring will be in line with data protection, human rights, and privacy legislation.

Filtering breaches or concerns identified through our monitoring approaches will be recorded and reported to the DSL who will respond as appropriate.

Any access to material believed to be illegal will be reported immediately to the appropriate agencies, such as the Internet Watch Foundation and the police.

When implementing appropriate filtering and monitoring, we will ensure that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

We acknowledge that whilst filtering and monitoring is an important part of our online safety responsibilities, it is only one part of our approach to online safety.

Children will use appropriate search tools, apps and online resources as identified following an informed risk assessment.

Children's device use will be closely physically monitored by staff. Children will not have any supervised access to devices.

Children will be directed to use age appropriate online resources and tools by staff.

Information Security and Access Management

School is responsible for ensuring an appropriate level of security protection procedures are in place, in order to safeguard our systems as well as staff and learners.

We will review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies.

Remote Learning

We will ensure any remote sharing of information, communication and use of online learning tools and systems will be in line with privacy and data protection requirements.

All communication with children and parents/carers will take place using school provided or approved communication channels; for example, school provided email accounts and phone numbers and agreed systems e.g. Seesaw

Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the DSL.

Staff and children will engage with remote teaching and learning in line with existing behaviour principles as set out in our behaviour for learning policy.

Staff and children will be encouraged to report issues experienced at home and concerns will be responded to in line with our child protection and other relevant policies.

When delivering remote learning, staff will follow our remote learning policy.

Parents/carers will be made aware of what their children are being asked to do online, including the sites they will be asked to access. We will continue to be clear who from the school *(if anyone)* their child is going to be interacting with online.

Parents/carers will be encouraged to ensure children are appropriately supervised online and that appropriate parent controls are implemented at home.

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.
- 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 only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- 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, unless express parental permission has been sought beforehand.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (covered as part of an agreement signed by parents or carers at the start of the year).
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to GDPR, which states that personal data must be:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary

- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy.
- It is registered as a Data Controller for the purposes of the General Data Protection Act (DPA, 2018).
- Risk assessments are carried out.
- It has clear and understood arrangements for the security, storage and transfer of personal data.
- Data subjects have rights of access and there are clear procedures for this to be obtained.
- There are clear and understood policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from information risk incidents.
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

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 (below) once it has been transferred or its use is complete.

Data Stored on iPads:

Periodically, at the start of each term, all photos and data will be removed from the iPad's used by children. This will be done remotely by the IT technician in the first week of the term.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. 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. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- 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, chat, 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, cyber bully, 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 limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions, Risk assessment, including legal risk School staff should ensure that:
- No reference should be made in social media to pupils, parents / carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information. The school's use of social media for professional purposes will be checked regularly by the online safety coordinator.

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).

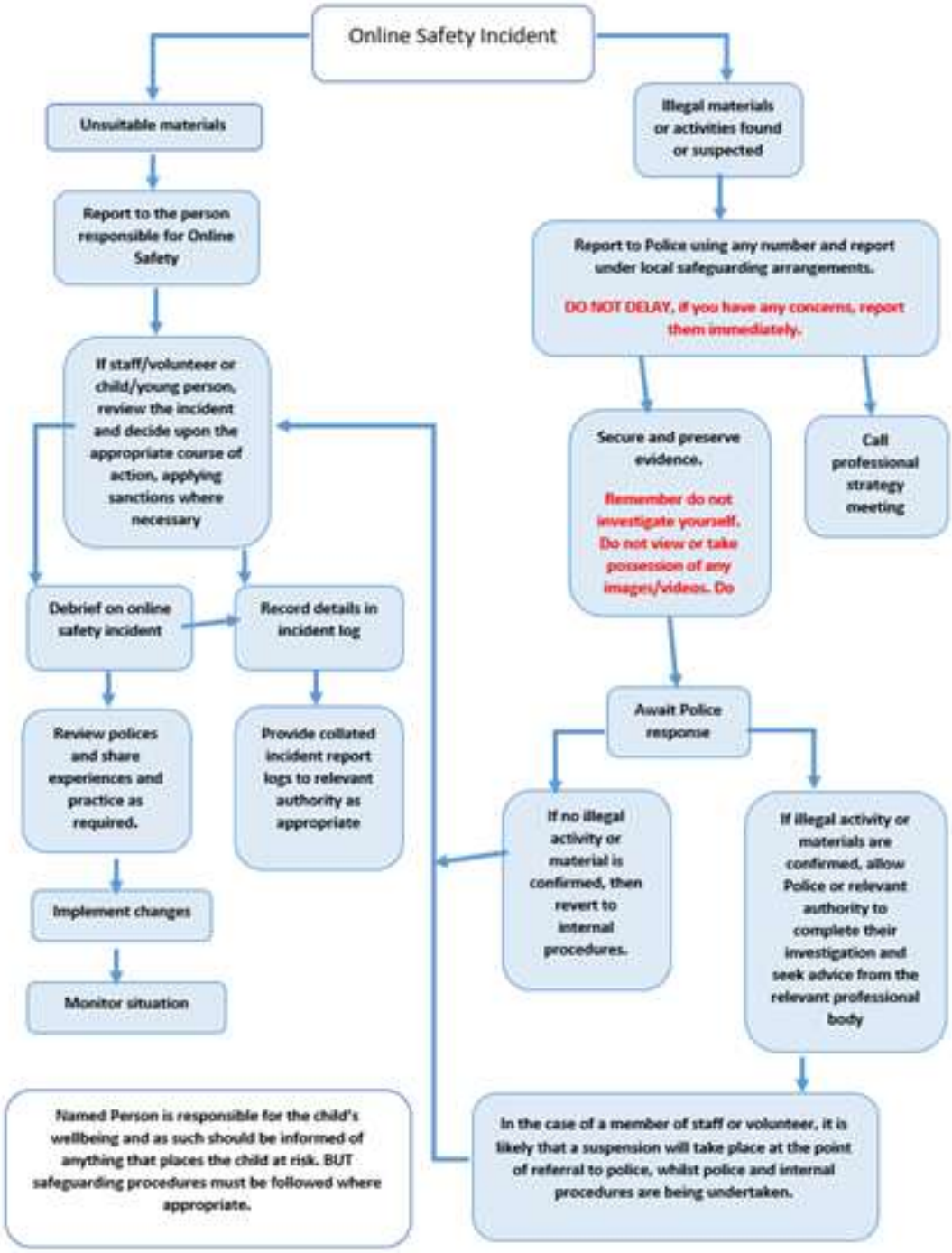
Website Filtering Hits

School are alerted by Smoothwall if anything has flagged up on the filtering and monitoring system. This data will then be analysed and any concerns followed up on by the Computing leads and Headteacher. Any concerns and action taken will be written into the Filtering and Monitoring file and signed off by the Headteacher and Deputy Headteacher. The schools Computing timetable and device numbering system will allow pinpointing of which classes/individuals may be attempting to access restricted content.

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

A9 Responding to incidents of misuse – flow chart



Other Incidents

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

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.

- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

- Internal response or discipline procedures
- Involvement by Local Authority or national / local organisation (as relevant).
- Police involvement and/or action

If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of “grooming” behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act • criminally racist material
- 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 child protection 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.