Online Safety Policy

2026-27

"Work hard, be kind"

Contents

1.0 Development/Monitoring/Review of this Policy 3

2.0 Teaching and Learning 5

3.0 Managing Internet Access 6

4.0 E-mail 6

5.0 Published content and the school website 7

6.0 Publishing pupils' images and work 7

7.0 Social networking and personal publishing 7

8.0 Managing filtering and monitoring 7

9.0 Managing video conferencing 8

10.0 Managing Emerging Technologies 8

11.0 Use of Generative AI (Artificial Intelligence) 7

12.0 Protecting Personal Data 8

13.0 Assessing risks 9

14.0 Handling Online Safety Complaints 9

15.0 Community Use of the Internet 9

16.0 Communicating the policy 9

17.0 Dealing with unsuitable/inappropriate activities 9

Responding to incidents of misuse 11

Illegal Incidents 11

Other Incidents 13

Appendix A 14

1.0 Development/Monitoring/Review of this Policy

- The Online Safety policy relates to other policies, including those for Computing, Anti-bullying, and Safeguarding children
- Our policy has been written after full consultation with school staff, parents/carers, governors, and young people
- It has been agreed by senior managers and approved by governors
- Because of the rapidly evolving online risks, our policy and its implementation will be reviewed annually, or sooner, should the need arise
- It is available to read or download on our school website, or as a printed copy from the school office
- The school has an Online Safety Lead
- Our lead is **Andrew Board**

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
- Surveys/questionnaires of:
    - pupils
    - parents/carers
    - staff

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, and community users) who have access to and use school digital technology systems, both inside and outside the school.

The Education and Inspections Act 2006 empowers the Headteacher, to such an extent that it is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers staff members 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 occur outside of the school but are 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.

Carnarvon Primary 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 outside of school.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk as identified in ‘Keeping Children Safe in Education’:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism, misinformation, disinformation (including fake news) and conspiracy theories
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as 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.

Roles and Responsibilities

Governors

Governors are responsible for approving the Online Safety policy and reviewing its effectiveness. They will carry this out by 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 Online Safety Co-ordinator
- regular monitoring of online safety incident logs provided by the DSL
- regular monitoring of filtering control logs
- reporting to relevant Governors.

Headteacher and Senior Leaders

- The Headteacher (Designated Safety Lead (DSL)) has a duty of care to ensure the safety of school community members
- The day-to-day responsibility for Online Safety will be delegated to the Online Safety Lead
- The Headteacher and (at least) another member of the Senior Leadership Team are aware of the procedures to be followed in case of a serious Online Safety allegation being made against a staff member
- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their Online Safety roles and to train other colleagues as relevant
- The Senior Leadership Team receive regular monitoring reports from the Online Safety Lead.
- The DSL logs behaviour and any safeguarding issues related to online safety using secure safeguarding software (CPOMS).

Online Safety Lead

- takes day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the school's online safety policies/documents
- ensures that all staff are aware of the procedures to follow in the event of an online safety incident
- provides training and advice for staff
- liaises with the 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 logs
- reports regularly to the Senior Leadership Team.

Technical staff

School technical staff are responsible for ensuring that:

- the school’s technical infrastructure is secure and is not open to misuse or malicious attack

- the school meets required Online Safety technical requirements and any Local Authority Online Safety policy/guidance that may apply
- users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated continuously
- the use of networks, the internet, and digital technologies is actively monitored so that any misuse or attempted misuse can be reported to the headteacher and senior leaders, as well as the online safety lead, for investigation and action
- 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 that technology is a significant component in many safeguarding and wellbeing issues, and children are potentially at risk of online abuse, either as victim, or perpetrator.
- they are fully aware 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 Teacher/Senior Leader/Online Safety Lead for investigation and action
- all digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems
- 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 and mobile devices in lessons and other school activities and implement current policies with regard to these devices
- where pupils are allowed to search the internet freely, staff should be vigilant in monitoring the content of the websites the young people visit.

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. Carnarvon Primary School takes every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, the Online Safety section of the school website (which contains many safety-related resources, and links to supporting websites and organisations), social media and information about national/local online safety campaigns/literature, also, via participation in high-profile events/campaigns, e.g., Safer Internet Day and Anti-bullying Week.

Parents and carers are encouraged to support the school in promoting good Online Safety practices and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website

2.0 Teaching and Learning

Why Internet and digital communications are important

- The purpose of any technology in school is to raise educational standards, promote achievement, support staff's professional work, and enhance the school's management functions
- The school has a duty to provide pupils with quality Internet access as part of their learning experience
- Internet use is part of the statutory curriculum and a necessary tool for staff

- Pupils will be educated on the safe, effective use of the Internet in research, including knowledge of location, retrieval, and evaluation skills
- They will be encouraged to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- Pupils will be shown how to publish and present information appropriately to a broader audience
- They will be taught what Internet use is acceptable and what is not and given clear objectives. These are also important transferable skills for their life out of school, including using mobile phones and other mobile devices
- They will be taught how to report unpleasant Internet content, including Cyberbullying or unwanted contact
- Issues such as Cyberbullying and Online Safety will be built into the PSHE curriculum to encourage self–efficacy and resilience. Teaching about online safety will be adapted for vulnerable children, victims of abuse and some children with SEND, where a more personalised or contextualised approach may often be more appropriate.

3.0 Managing Internet Access

Information security system

1. The school's IT technicians will regularly review the school's ICT system security. The school currently uses Sophos Anti-Virus protection, which provides automatic updates.
2. Virus protection will be updated regularly. This is an automatic process that is monitored on-site weekly.
3. The school's Internet provision is filtered using the company 'SmoothWall'

SmoothWall filtering updates in real time. This means that moments after a site is blocked, it will be inaccessible, while unblocked sites become usable practically as soon as they are needed.

Our IT technicians receive notifications about sites that are refused by SmoothWall.

The virus protection and filtering systems are both monitored continually by the school's IT Technicians.

4.0 E-mail

- Pupils and staff may only use approved e-mail accounts on the school system
- Pupils must immediately tell a member of staff if they receive offensive e-mail
- Staff-to-parent e-mail communication must only take place via a school e-mail address and will be monitored
- **All** incoming e-mails should be treated with caution, and attachments and links should not be opened unless the author is known
- Communication using e-mail will be organised to ensure it is for appropriate educational use
- The language and content of e-mails will be of an appropriate level expected of any written work and should ensure that the good name of the school is maintained
- The forwarding of chain letters and anonymous letters is banned
- E-mail messages on school business will be regarded as having been sent on headed notepaper and reflect a suitable tone and content
- E-mail and the Internet will not be used to order materials or undertake any activity which incurs a cost to the school unless specifically authorised by the school
- Email must not be used to sell items

- When sending confidential information, staff and governors should use their school email accounts and not personal ones.

5.0 Published content and the school website

- The contact details on the school's website should be the school address
- No staff or pupil's details will be published
- The headteacher will have overall editorial responsibility to ensure accurate and appropriate content.

6.0 Publishing pupils' images and work

- Photographs, including children, will be selected carefully and follow the school's policy
- Pupils' full names will be avoided on the website and learning platforms, including blogs and forums, especially if associated with a photograph
- Written permission will be obtained from parents and carers before any photographs are published on the school website or elsewhere
- Parents should be informed of the school image-taking policy and publishing policy.

7.0 Social networking and personal publishing

- The school will control access to social networking sites in school and educate pupils on their safe use through the Computing and PSHE curricula
- The school will encourage parents to support their children when setting up a social networking profile and offer help and guidance. This includes encouraging families to follow the terms and conditions specifying the appropriate age for using sites
- Via the Computing Curriculum Map, pupils will be advised never to give out personal details which may identify them or their location
- All staff should be aware of the potential risks of using social networking sites or personal publishing, either professionally with pupils or personally. They should be aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

8.0 Managing Filtering and Monitoring

In common with other media such as magazines, books and videos, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure such material is inaccessible. This is facilitated via the SmoothWall filtering and monitoring system. However, due to the international scale and linked nature of information available via the Internet and email, it is impossible to guarantee that particular types of material will never appear on a computer, and as such, the school cannot accept liability for the material accessed or any consequences thereof.

- The school will work with the LA to ensure that the systems that protect pupils are reviewed and improved as necessary
- Any unsuitable online material should be reported to the Online Safety Lead
- The IT technicians will regularly check to ensure that the filtering and monitoring methods are rigorous, effective, and reasonable
- Incidents, including accidental access to unacceptable websites will be reported to the Online Safety Lead. The school will make every attempt to ensure that pupils are always supervised when using the Internet and email, although we recognise that teaching self-regulation by pupils is the most effective strategy for long-term online safety
- All machines and devices available to pupils with Internet and email capability are frequently monitored

- A summary of filtering and monitoring arrangements along with a summary of monitoring reports will be presented to Governors annually.

9.0 Managing video conferencing

- Video conferencing will be appropriately supervised for the pupil's age
- Pupils will always ask permission from the supervising teacher before making or receiving a video conference call
- Video conferencing will use the best quality connection possible to ensure integrity of service and security.

10.0 Managing Emerging Technologies

- The school will examine emerging technologies for their educational benefit and carry out a risk assessment before use in school
- Mobile phones and associated cameras will not be used in lessons or formal school time, except as part of an educational activity
- If pupils bring in mobile phones, these must be handed in on arrival, and these will be stored in the school office until the end of the school day. Pupils are not permitted to use them during the school day at all, with only specific exceptions (e.g., medical monitoring, such as diabetes) to be agreed in advance with the Head Teacher
- Care will be taken with the use of hand-held technologies in school, which may not have the level of filtering required
- Staff will use a school phone connection where contact with pupils and their families is required, except in an emergency.

11.0 Use of Generative AI (Artificial Intelligence)

- We acknowledge that generative AI platforms (e.g., ChatGPT or Gemini for text creation or the use of Co-Pilot or Adobe Firefly to create images and videos) are becoming widespread. We are aware of and follow the DfE's guidance on this. In particular:
    - We will talk about the use of these tools, their practical use as well as their ethical pros and cons with pupils as part of our Computing curriculum, staff through our ongoing CPD and parents through the newsletter and awareness raising sessions.
    - We are aware that there will be use of these apps and exposure to AI creations on devices at home for some children – these experiences may be both positive/creative and also negative (inappropriate data use, misinformation, bullying, deepfakes, nudifying apps and inappropriate chatbots). We will discuss children's use of generative AI at home with them as part of their learning in Computing and PSHE.
    - By default, we block access to the Generative AI category for pupils using our Smoothwall filtering system. Access to specific platforms may be granted for teaching and learning purposes if appropriate, and on a case-by-case basis.

12.0 Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation, as mandated in the Data Protection Act 2018
- All staff must read and acknowledge the 'Staff Code of Conduct' before using any school digital resource.

13.0 Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material; however, it is not possible to guarantee that unsuitable material will never appear on a school computer
- The school will monitor ICT use to establish if the Online-Safety policy is appropriate and effective.

14.0 Handling Online Safety Complaints

- Complaints of misuse by staff will be referred to the headteacher
- Any complaints of a child protection nature must be dealt with in accordance to the school's child protection procedures
- Pupils and parents will be informed of the consequences and sanctions for pupils misusing the Internet and this will be in line with the school's behaviour policy.

15.0 Community Use of the Internet

- All use of the school Internet connection by the community and other organisations shall be in accordance with the Online Safety policy.

16.0 Communicating the policy

Pupils

- Appropriate elements of the Online Safety policy will be shared with pupils
- Online-Safety rules will be posted in all networked rooms
- Pupils will be informed that network and Internet use will be monitored
- Age-appropriate Computing and PSHE curricula will be used to ensure all pupils gain an awareness of online safety. These will be addressed on a regular basis and modified as newer risks are identified.

Staff

- All staff will be given a copy of the Online Safety policy, acknowledge that they have read and understood it and agree to work within the guidelines
- Staff should be aware that the system is monitored and that professional standards are expected
- Staff monitoring the system will be supervised by senior management and have a clear procedure for reporting
- All staff will be asked to sign the school's Acceptable Use Policy – please see Appendix A

Parents

- Parents will be made aware that the school policy is available on the school website
- All parents are asked to sign the parent/school agreement which covers permission to access the Internet, when they register their children.

17.0 Dealing with unsuitable/inappropriate 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	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)						X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)					X	

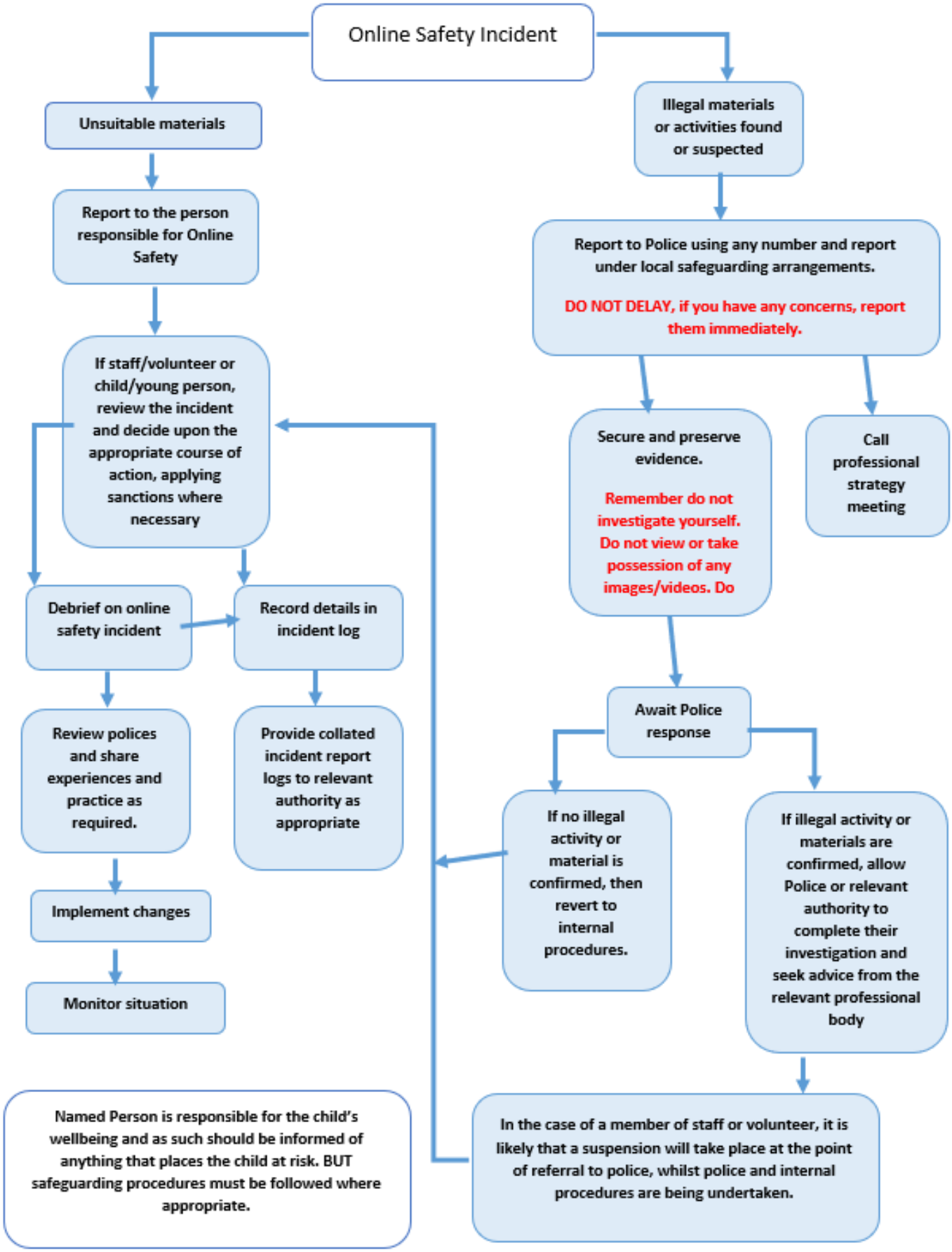
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
Using school systems to run a private business				X	
Infringing copyright				X	

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

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 carelessness, irresponsibility 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 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 disciplinary procedures
    - Involvement by Local Authority and/or national/local organisation (as relevant)
    - Police involvement and/or action.
- If the content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of ‘grooming’ behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - offences under the Computer Misuse Act (see User Actions chart above)
    - 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.

Appendix A

Acceptable Use Policy – Digital Technologies

Digital technologies, such as email, the Internet, and mobile devices, are an expected part of our working life in school. This policy is designed to ensure all staff are aware of their professional responsibilities when using any form of digital resources. All staff are expected to sign to say that they will adhere to its contents at all times, as follows:

- I appreciate that Information technology includes a wide range of systems and devices, including mobile phones, tablets, digital cameras, email, and social networking and may include personal digital devices when used for school business
- I understand that it is a criminal offence to use a school digital device for a purpose not permitted by its owner
- I will comply with the Computing system security and not disclose any passwords provided to me by the school or other related authorities
- I understand that I am responsible for all activities carried out under my user name
- I will only use the school email, internet, intranet, or any related technologies for professional purposes
- I will ensure that personal data is kept secure and used appropriately, whether in school, taken out of school or used remotely when authorised by the headteacher or governing body
- I will not install any hardware or software without permission, with the exception of educational apps
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- I will respect copyright and intellectual property rights
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with the consent of the parent, carer or staff member. Images will not be distributed outside the school network/learning platform without permission
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute
- I will ensure that all electronic communications with parents, pupils and staff are compatible with my professional role and that messages cannot be misunderstood or misinterpreted
- I will support the school's online safety policy and help pupils to be safe
- I will report any incidents of concern regarding children's safety to the Online Safety Lead, and any incidents of cyberbullying to the headteacher
- I understand that sanctions for disregarding any of the above will be in line with the school's disciplinary procedures, and serious infringements may be referred to the police.

I agree to follow the code of conduct and support the safe use of digital resources throughout the school.

Full Name: _____

Job Title:_____

Signature:_____ Date:_____