Online Safety Policy

Online safety is an integral part of safeguarding. This policy sets out our approach to online safety to empower, protect and educate learners and staff in their use of technology. It establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

This policy is part of the School's Statutory Safeguarding Policy and has been written by the schools computing lead. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

Contents

1. Statement of Intent

This online safety policy is intended to demonstrate the partnership's commitment to:

- Ensuring the safety and wellbeing of children, young people and adults is paramount when using the internet, social media or mobile devices.
- Providing staff and volunteers with the overarching principles that guide our approach to online safety.
- Ensuring that we operate in line with our values and within the law in terms of how we use online devices.

This policy applies to all members of Hevingham and Marsham Primary School Partnership, including staff, pupils, governors, volunteers, parents, carers, visitors, and community users who have access to and are users of our digital technology systems.

2. Linked Policies

This policy statement should be read alongside our other policies and procedures, including:

- Anti-Bullying Policy (including Cyberbullying)
- Data Protection Policy
- Record Keeping Policy
- Freedom of Information Policy
- Home Learning Policy
- ICT code of conduct
- Mobile Phone policy
- Behaviour Policy
- RSE and Health Education Policy
- Safeguarding and Child Protection Policy
- Social Media Policy
- Special Educational Needs and Disability Policy
- Staff handbook which includes Staff Code of Conduct
- Staff Wellbeing Policy

The above list is not exhaustive but when undertaking development or planning of any kind the school will consider the implications for online safety.

3. Key Roles and Responsibilities

The school takes a whole-school approach to online safety and all stakeholders are responsible for ensuring that effective policies and procedures are maintained and upheld. It is expected that all staff and volunteers read and understand this policy and implement it consistently.

3.1 Governance

Our school governors play an important part in monitoring the online safety provision across the schools. They have a responsibility to keep up to date with online safety by receiving appropriate online safety training.

The governors are responsible for:

- Reviewing and approving this policy.
- Monitoring the effectiveness of the policy by reviewing data and reports from the Online Safety Lead and Safeguarding Lead.
- Having an oversight of safeguarding and online safety and ensure any weaknesses are addressed.
- Agreeing and adhering to the terms on acceptable use of the partnership's ICT systems and the internet.
- Developing individual knowledge and understanding to ask the right questions and professionally challenge and test what happens in both schools.

The Computing lead is responsible for:

- Monitoring this policy ensuring it meets the needs the school.
- Monitoring data and audit reports for the Online Safety Lead and Safeguarding Lead.
- Agreeing and adhering to the terms on acceptable use of the Partnership's ICT systems and the internet.
- Developing individual knowledge and understanding to ask the right questions and professionally challenge and test what happens in school.

3.2 Online Safety Lead

The role of Online Safety lead forms part of the safeguarding team. The Online Safety Lead will receive regular training on online safety and be aware of the potential for serious child protection and/or safeguarding issues that may arise from the online world. They will have overall oversight of the online safety strategy. Key responsibilities:

- Monitoring online safety in schools through yearly audits*
- Ensuring support mechanisms are in place for schools dealing with complex situations.

- Regularly updating governors on the progress made with online safety.
- Ensuring that there are robust protocols in place for both monitoring and reporting online safety issues.
- Ensuring all staff adhere to the policies and procedures around online safety. E.g. acceptable use policies.
- Responsible for actioning the annual review of the online safety policy.

*The computing lead will use the SWGFL 360 Safe audit as part of our yearly online safety audit. Details of this can be found here: https://swgfl.org.uk/products/360-degree-safe/
The purpose of these audits is to ensure the school continues to:

- Review and develop its online safety strategy.
- To find and action any areas of development within the school online safety program.
- To work towards achieving/renewing the Online Safety Mark

3.3 Head Teacher and SLT

The Head teacher and members of SLT take overall responsibility in ensuring that all staff and pupils understand and follow the policies and procedures of online safety. Key responsibilities:

- To liaise with the Online Safety DSL about the development of the partnership's online safety strategy.
- Support the Online Safety DSL in carrying out their role.
- Review the online safety curriculum with the Online Safety DSL.
- Share the online safety audit report and actions to the governing board.
- To know the procedures in the event of serious online safety allegations against a member of staff.
- Responsible for ensuring the Online Safety Lead is given time to receive suitable training to support them in their role.
- Ensure all staff understand this policy and that it is implemented consistently.
- Reviews the partnership's infrastructure/network with ICT Services to ensure it is safe and fit for purpose.

3.4 School Online Safety Lead

The Online Safety DSL will be responsibility:

- For online safety issues in school.
- Liaise with external agencies where necessary.
- Provide regular reports on online safety in school to the SLT.
- Keep up to date with current legislation, developments, and resources.
- Provide training and advice for all staff across school.

- Lead role in personalising policies/documents.
- Provide updates on progress of online safety.
- Ensure pupil voice is considered as part of online safety development/strategy (this will be supported by the Computing Lead).

3.5 School IT Technicians (ICT Solutions)

School IT technicians are the first line of defense against online safety, and they play a huge role in ensuring that pupils and staff are kept safe. Key responsibilities are to:

- Ensure that school networks are secure and safe to use.
- Regularly monitor school networks and internet.
- Implement and update monitoring software/systems are as requested.
- Ensure that only authorised users can access the network and these users adhere to password rules.
- Ensure that they keep up to date with relevant online safety updates.
- Ensure that filtering policies are applied to the correct users.
- Ensure that any filtering request changes are liaised and agreed with the Head teacher before actioning.
- Ensure that any online safety incidents are sent to class teachers and SLT for actioning.

3.6 Teaching and Support Staff

Teachers and support staff are the day-to-day contact for pupils and therefore responsible for promoting safe online safety behaviour. Key responsibilities are to:

- Ensure they attend any relevant training that is issued by the Head teacher/Online Safety DSL.
- Ensure that they adhere to the policies and procedures relating to online safety. E.g., acceptable use policy and staff handbook.
- Support pupils understanding and ensure they follow online safety procedures and policies.
- Ensure that where there is pre-planned internet use, pupils are guided to sites that are suitable.
- Report any online safety concerns to the Online Safety DSL.
- Ensure policies around mobile phones are enforced with all pupils.
- Ensure digital communications with pupils/parents/carers on carried out using official school systems and that conversations always remain professional.
- Ensure they deliver the online safety curriculum to all pupils.
- Ensure online safety issues are embedded into all aspects of the curriculum.

3.7 Pupils

Pupils are responsible for:

- Ensuring that they use the digital technology systems in accordance with the pupil acceptable use policy.
- Understanding the importance of reporting abuse, misuse or access to inappropriate material.
- Adhering to the school mobile phone policies and are aware of the consequences if they don't follow this.
- Understanding the need for good online safety behaviour both in and out of school.
- Providing valuable feedback about online safety through surveys and discussions.

3.8 Parents/Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The partnership will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, social media, 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.
- Online learning platforms (Google Classroom) by following the Home Learning Policy.
- Their children's personal devices in school (where this is allowed).

3.9 Community Users

Community users who have access to the school systems or programs as part of the wider school provision will be expected to sign a Community User Acceptable Use Policy/Agreement before being provided with access to school systems. This will be done as they enter the building following our signing in procedures.

4 Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The Online Safety Designated Safeguarding Lead has overall responsibility for the partnership's approach to online safety, with support from the school's SLT, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online.

The importance of online safety is integrated across all school operations in the following ways:

- Staff receive regular training.
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation.
- Online safety is integrated into learning throughout the curriculum.
- Assemblies/sessions are conducted termly (as a minimum) on the topic of remaining safe online.

5 Online safety in the curriculum

We want our pupils to take responsibility and act in a responsible way.

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 Partnership'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 all subjects where relevant. The online safety curriculum used is SWGfL Project Evolve (https://projectevolve.co.uk) and is broad, relevant and provides progression, with opportunities for creative activities.

Online safety will be provided in the following ways:

- The school uses a planned online safety curriculum (SWGfL Project Evolve) which is delivered through dedicated online safety lessons, as well as being reinforced through all parts of daily school life.
- Key online safety messages are reinforced as part of a planned programme of themed Online-Safety focused weeks, including Internet Safety Day and Wellbeing Week.
- Pupils are 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 are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils will 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. Schools are required to ensure all devices have monitoring software on them that detects and alerts the school of any potential exposure to extremism, this will be discussed with ICT solutions.
- Pupil's will be helped to understand the need for the pupil ICT Code of Conduct Agreement **(Appendix 1)** and encouraged to adopt safe and responsible use both within and outside school.

- Staff will act as good role models in their use of digital technologies, the internet, and mobile devices.
- In lessons where internet use is pre-planned, staff will do their best to ensure that students/pupils are 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.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can make a request to 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 and be agreed by the partnership’s Head teacher before actioned by the IT technicians.

6 Parent awareness and working with the wider community

We understand that many parents and carers only have 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 children’s online behaviour. 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 provide information and awareness to parents and carers through:

- Curriculum activities, themed online safety awareness weeks. High profile events/campaigns e.g Safer Internet Day and Wellbeing Week.
- Letters, school newsletters, school web site
- Online Safety newsletter

All parents sign an ICT Code of Conduct Agreement on behalf of their children when they join the school and then re-sign annually (September). (**Appendix 1)**

7 Training

7.1 All staff

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 is 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 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 Online Safety Lead will receive regular updates through attendance at external training events when available.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff meetings/training sessions.

7.2 Online Safety Lead DSL

It is essential that the Online Safety Lead DSL receives additional training to support them in their role. This training will be done by:

- Attending advanced online safety training DSL training.
- Participating in online safety expert groups (e.g. SWGfL 360 Safe Assessor Programme).
- Attending expert external training sessions through various providers.
- Keeping up to date with latest legislation and policy changes.

7.3 Governors

Governors will take part in online safety training/awareness sessions, with particular importance for those who are involved in technology/online safety/health and safety/safeguarding.

8 Online safety concerns

8.1 Cyberbullying

Cyberbullying can include the following:

- Threatening, intimidating, or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Threatening or bullying emails, possibly sent using a pseudonym or someone else’s name
- Menacing or upsetting responses to someone in a chatroom
- Unpleasant messages sent via instant messaging apps (e.g. WhatsApp)

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

8.2 Peer on peer abuse

Pupils may use the internet and technology as a vehicle for sexual abuse and harassment. The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person’s clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery

The school will respond to all concerns regarding online peer-on-peer sexual abuse and DSLs will investigate the matter in line with our Safeguarding Policy.

8.3 Grooming

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.
Staff will be aware that grooming often takes place online where the perpetrator will often hide their identity through pretending to be someone they are. Pupils are less likely to report grooming behaviour because:

- The pupil believes they are talking to another child
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer’s attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the pupil feel ‘special’, particularly if the person they are talking to is older.
- The pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

8.4 Child sexual exploitation (CSE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CSE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL **immediately**, who will manage the situation in line with the Safeguarding Policy.

8.5 Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda.

Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

8.6 Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime.

Where there are any concerns about a pupil's use of technology and their intentions about using their skill and affinity towards it, the DSL will get advise on the best way to divert them to a more positive use of their skills and interests.

9 Responding to online incidents

9.1 Responding to pupil incidents

Where a pupil misuses the partnership's IT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident.

The partnership's DSLs will determine the seriousness of all incidents and report all illegal activities/incidents to the appropriate organisation, these include:

- Police

- CEOP (child exploitation and online protection)

9.2 Responding to staff incidents

Where a staff member misuses the school’s IT systems or internet or uses a personal device in a way that their actions constitute in misconduct, then the matter will be dealt with in accordance with the staff disciplinary procedure. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police. A flow chart in dealing with illegal activity (**appendix 2)** supports the school in taking the correct action.

10 Personal devices

10.1 Pupils

Pupils in upper KS2 may bring mobile devices into school. Parents/Carers will need to complete an agreement that their child can bring a mobile phone into school. Pupils must hand their mobile device into the office (directly or via the class teacher) where it will be kept securely. Pupils are not allowed to use their mobile phone during the school day, this includes:

- Lessons
- Playtime/Lunchtime
- Clubs before or after school

Any breach of the mobile device agreement may trigger disciplinary action in line with the partnership’s behaviour policy and could result in confiscation of their device.

10.2 Staff

Staff members must not use a personal device (e.g., phones and tablets) throughout the school day, unless this is in their own break/lunch time. Staff are not permitted to take or store images of pupils on their mobile device. Personal information about staff, pupils, or the school is not to be stored on any personal device.

For more information on use of mobile phones, please refer to the mobile phone policy.

11 Technical Systems

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that internet filtering is actively monitored for misuse.

12 Remote learning

All remote learning is delivered in line with the partnership's Home Learning Policy.

The partnership will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use.

During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software and filtering, on devices not owned by the school.

12. Policy review

This policy will be reviewed by the Computing Lead annually and updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation. A formal review will be completed every two years for Governor approval.

Appendix 1: ICT codes of conduct KS1 & KS2

Pupil ICT Code of Conduct:
agreement for EYFS/KS1 pupils

Name of pupil:

When using the computers, iPads and accessing the internet in school, I will:

- turn computers on and off using the correct procedure.
- carry computers carefully, with the lid down, and never more than one at a time
- log on and off in the correct way, using my own username
- only use it for school work.
- only use them when a teacher is there.
- only go on sites that have been given to me by the teacher.
- never open anything that I am unsure about without asking a teacher.
- tell a teacher immediately if I see anything I am unhappy with
- not access social networking sites.
- not use chat rooms
- never share any personal information with other people except my parents/carers
- not bring a mobile phone or any other electronic device into school.

I know that the school may check my computer files and may monitor the Internet sites I visit
I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers
I shall learn how to stay safe on the internet
Signed (pupil): **Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet and will make sure my child understands these.

Signed (parent/carer): **Date:**

Pupil ICT Code of Conduct:
agreement for KS2 pupils

Name of pupil:

When using the computers, iPads and accessing the internet in school, I will:

- turn computers on and off using the correct procedure.
- carry computers carefully, with the lid down, and never more than one at a time.
- never share my personal passwords or usernames with others or log in to the school's network using someone else's details.
- only use it for school work or homework.
- only use them when a teacher is there or given me permission to be on my own.
- never open anything that I am unsure about without asking a teacher.
- tell a teacher immediately if I see anything I am unhappy with, or I receive messages I do not like.
- not access any inappropriate websites.
- not access social networking sites.
- not use chat rooms.
- never give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer.
- never open any attachments in emails, or follow any links in emails, without first checking with a teacher.
- use only kind and appropriate language when communicating online, including in emails.
- never arrange to meet anyone offline.

If I bring a personal mobile phone or other personal electronic device into school:

- not use it during the school day, in any lesson times, clubs or other activities organised by the school.
- hand my mobile phone into the office before school and collect it afterwards.
- use it responsibly.

I know that the school may check my computer files and may monitor the internet sites I visit
I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers
I shall learn how to stay safe on the internet

Signed (pupil): **Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet and will make sure my child understands these.

Signed (parent/carer): **Date:**

Appendix 2: Staff, Governor and Visitor ICT Code of Conduct

Hevingham and Marsham Primary School Partnership and Hevingham Under 5's Staff, Governor and Visitor ICT Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This code of conduct is provided to ensure that all users are aware of their responsibilities when using any form of ICT provided by or directed by Norfolk County Council. All such users will be issued with this code of conduct. Any concerns or clarification should be discussed with Hevingham and Marsham Primary School Partnership.

All staff, Governors and visitors:

- understand that ICT includes a wide range of systems, including mobile phones, smart watches, digital cameras, laptops and tablets
- understand that it is a disciplinary offence to use the school ICT system and equipment for any purpose not permitted by its owner.
- will not disclose any passwords provided to them by the school or other related authorities.
- understand that they are responsible for all activity carried out under their username
- understand that their permitted use of the Internet and other related technologies is monitored and logged and will be made available, on request, to their Line Manager or Headteacher in line with any disciplinary procedures. This relates to all school owned devices, including laptops provided by the school.
- will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for uses permitted by the Head or Governing Board.
- will ensure that all their school generated electronic communications are appropriate and compatible with their role.
- will ensure that all data is kept secure and is used appropriately as authorized by the Head teacher or Governing Body. If in doubt, they will seek clarification. This includes taking data off site.
- using personal devices must only be used in the context of school business with explicit permission of the Headteacher.
- using school equipment will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- will only use the approved email system(s) for any school business

Images will only be taken, stored and used for purposes in line with school policy. They will not be distributed outside the school network/learning platform without the consent of the parent/carer and the permission of the Head teacher.

- All staff, Governors and visitors will comply with copyright and intellectual property rights.

- All staff, Governors and visitors will report any incidents of concern regarding staff use of technology and/or children’s safety to the Senior Designated Professional or Head teacher in line with the school’s Safeguarding Policy.

I acknowledge that I have received a copy of the ICT Code of Conduct.

Full name:…………………………………………………………………..(printed)

Job title:…………………………………………………………………………..…

Signature:…………………………………………………**Date:**……………………

Appendix 3: Parent/Carer ICT Code of Conduct

Hevingham and Marsham Primary School Partnership
Parent/Carer ICT Code of Conduct

Parent / carer name: ……………………………………………

Pupil(s) name(s): ……………………………………………………..

Pupil's Year Group(s): ……………………………………

As the parent or carer of the above pupil(s), I grant permission for my child to have access to use the Internet, Google Drive, school email and other ICT facilities at school.

I know that my son or daughter has signed a form to confirm that they will keep to the school's rules for responsible ICT use, outlined in the ICT Code of Conduct. I also understand that my son/daughter will be informed if the rules have to be changed during the year. I know that the latest copy is available at http://www.hevinghamprimary.co.uk and that further advice about safe use of the Internet can be found at https://www.thinkuknow.co.uk/parents/

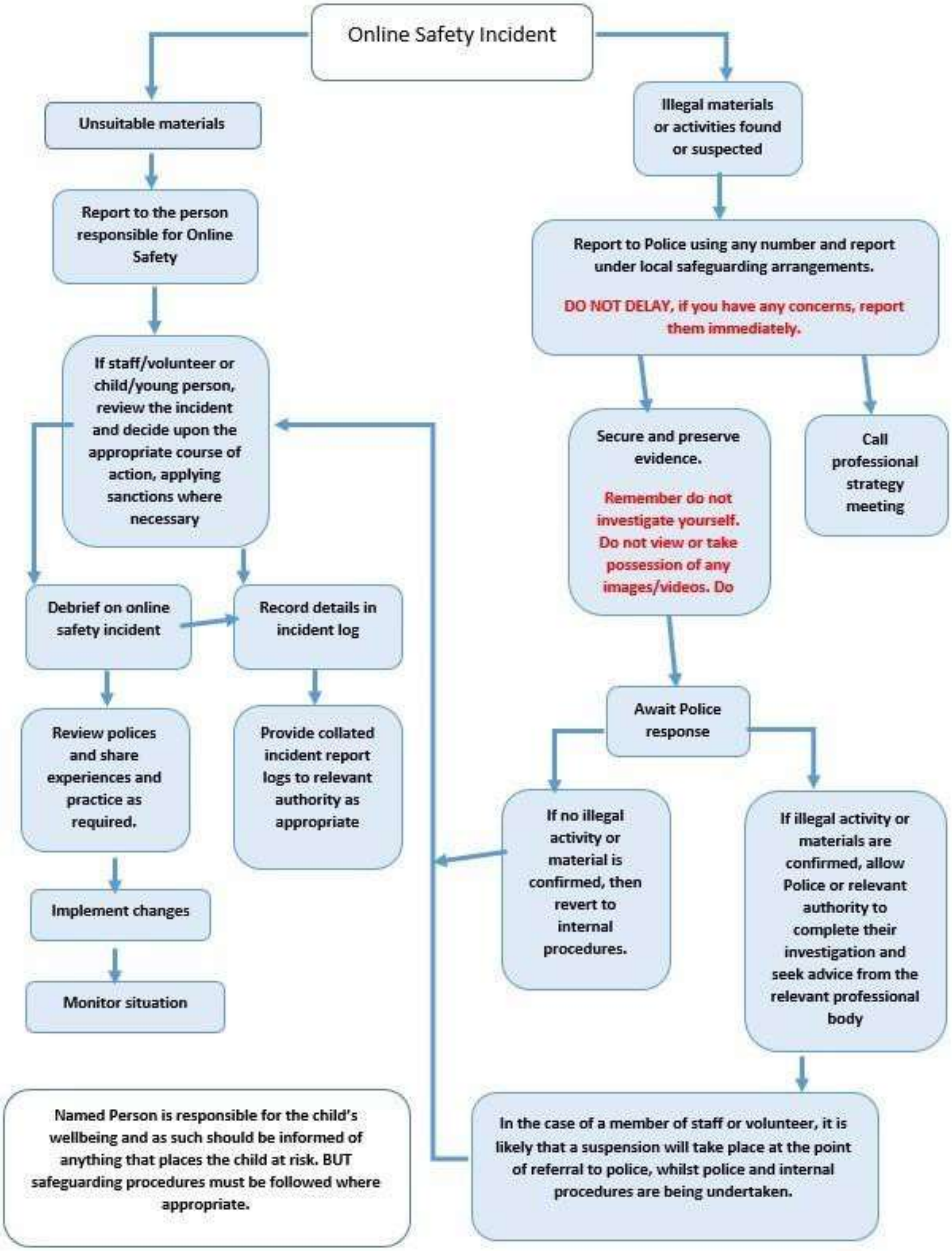
I accept that ultimately, the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service, safe access to email, employing appropriate teaching practice and teaching online safety skills to pupils.

I understand that the school can check my child's computer files and the websites they visit. I also know that the school may contact me if there are concerns about my son/daughter's online safety or online behaviour.

I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's online safety.

Parent/carer signature: …………………………………………… **Date:** ………………….

Appendix 4: Staff online safety incident flow-chart



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

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.

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.