Woodland Primary School

‘Together We Thrive

E-safety Policy

Evidence of intentions and practice - for the information of
staff, governors, parents, LA, OFSTED and DfE

Prepared by: Miss K Sumpton	**Approved by:** Local Governing Body
Issue date: Spring 2024	**Review date:** Spring 2025

WOODLAND PRIMARY SCHOOL

E-safety Policy

1 Background/Rationale

1.1 New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

1.2 The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

1.3 The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the head teacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the children themselves.

1.4 The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

1.5 However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use that may influence the social and emotional development and learning of the young person.

1.6 Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. Behaviour, Anti-Bullying and Safeguarding policies).

1.7 As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' / pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

2 Schedule for Development/Monitoring/Review

This e-safety policy was approved by a Full Governing Body on:	Spring 2024
The implementation of this e-safety policy will be monitored by the:	E-Safety Lead / Senior Leadership Team/ Local Governing Body
Monitoring will take place at regular intervals:	Termly or when any incidents or developments have taken place.
The E-Safety Policy will be annually or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	Spring 2025
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	LA ICT Manager, Local Authority Designated Officer

2.1 The school will monitor the impact of the policy by:

- Logging incidents on CPOMS under E-Safety
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys/questionnaires of pupil, parents/carers and staff

2.2 The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The E-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communication technologies for educational, personal and recreational use.

3 Roles and Responsibilities

3.1 The following section outlines the roles and responsibilities for E-safety of individuals and groups within the school.

Governors

3.2 Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of it. This will be carried out by the Governing Body who receive regular information about E-safety incidents and monitoring reports.

3.3 A member of the Governing Body has taken on the role of E-Safety Governor as part of their wider role of Safeguarding Governor – Miss A. Wheal

3.4 The role of the E-Safety Governor will include:

- meetings with the E-Safety Lead
- monitoring of E-safety incident logs from CPOMS
- monitoring of filtering / change control logs
- reporting to relevant Governors committee / meeting

Head teacher and Senior Leaders

3.5 The Head teacher is responsible for ensuring the safety (including E-safety) of all members of the school community. The day-to-day responsibility for E-safety will be delegated to the E-Safety Lead.

3.6 The Head teacher / Senior Leadership Team are responsible for ensuring that the E-Safety Lead and other relevant staff receive suitable CPD to enable them to carry out their E-safety roles and to train other colleagues, where relevant

3.7 The Head teacher / Senior Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-safety monitoring role. This is to provide a safety net and support to those colleagues who take on important monitoring roles.

3.8 The Senior Leadership Team will receive monitoring reports from the E-Safety Lead.

3.9 The Head teacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious E-safety allegation being made against a member of staff.

Designated Safeguarding Lead (Miss H Kirk)
Deputy Designated Safeguarding Lead (Mrs M Dodson)

3.10 The Designated Safeguarding Lead and/or Deputy Designated Safeguarding Lead should be trained in E-safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

E-Safety Lead Miss K Sumpton

3.11 The E-safety lead:

- takes day to day responsibility for E-safety issues and has a leading role in establishing and reviewing the school E-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an E-safety incident taking place (see Acceptable Use Policy (AUP)
- provides training and advice for staff
- liaises with school Computing technical staff
- Is alerted to any E-Safety incidents logged on CPOMS
- meets with the E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports to Senior Leadership Team

Network Manager/Technical Staff (Mr. Mike Newton)

3.12 The Computing Technician in conjunction with the Head teacher, are responsible for ensuring:

- that the school's Computing infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the E-safety technical requirements outlined by the Local Authority E-Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- that they keep up to date with E-safety technical information in order to effectively carry out their E-safety role and to inform and update others as relevant
- that the use of the network/Virtual Learning Environment (VLE)/ remote access/email is regularly monitored for misuse or attempted misuse to be reported for investigation.
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

3.13 Teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of E-safety matters and of the current school E-safety policy and practices
- they have read, understood and signed the school Acceptable Use Policy
- they report any suspected misuse or problem to the E-Safety Lead / Head teacher for investigation
- digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school E-safety and Acceptable Use Policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor Computing activity in lessons, extra-curricular and extended school activities
- they are aware of E-safety issues related to the use of mobile phones, cameras and personal devices and that they monitor their use and implement current school 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

3.14 Pupils are responsible for using the school Computing systems in accordance with the Safer Internet Guidelines

3.15 They have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

3.16 They need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so (e.g. telling staff)

3.17 They will be expected to know and understand school policies on the use of mobile phones, digital cameras and personal devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.

3.18 They should understand the importance of adopting good E-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

4 Parents / Carers

4.1 Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. School has a responsibility to provide parents and carers with up to date information to safeguard their children at home. Information will be provided though leaflets available in reception and updates through the school Facebook page.

4.2 Parents and carers will be responsible for:

- Accessing the school website, school FB page and Tapestry in accordance with the Acceptable Use Policy.

5 Community Users

5.1 Community users (such as other HET staff) who access school or the website can use school systems under supervision of a school employee for CPD purposes or as part of a working group.

6 Policy Statements

Education –pupils

6.1 Whilst regulation and technical solutions are important, there is a balance with educating pupils to take a responsible approach to E-Safety. This is an essential part of school's E-Safety provision. Children are taught how to recognise risks or potential risks and how to report any issues to a member of staff.

6.2 E-Safety education will be provided in the following ways:

- A planned E-safety programme should be provided as part of Computing / PHSE / other lessons and should be regularly revisited – this will cover both the use of Computing and new technologies in school and outside school
- An E-Safety programme is provided as part of the computing curriculum (stand-alone lessons and revisited throughout sessions) and PSHE lessons. Key messages are reiterated whenever technology is in use.
- Key E-safety messages are reinforced as part of a planned programme of assemblies
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of Computing, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of Computing systems and internet are posted in all classrooms and around school
- Staff act as good role models in their use of Computing, the internet and mobile devices

Education – parents / carers

6.3 Many parents and carers have limited understanding of E-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. 'There is a generational digital divide'. (Byron Report).

6.4 School will provide parents with information and guidance to support E-Safety at home through updates on the school website, on the Facebook page and leaflets available in school. As school become aware of any potential risks, parents will be informed.

Education - Extended Schools

6.5 Messages to the public around E- safety should are also targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Education & Training – Staff

6.6 All staff receive E-safety training and understand their responsibilities, as outlined in this policy. Regular updates are given in Staff meetings and Teaching Assistant Meetings to reiterate key messages.

6.7 A planned programme of formal E-safety training will be made available to staff. An audit of the E-safety training needs of all staff will be carried out regularly.

6.8 All new staff should receive E-safety training as part of their induction programme, ensuring that they fully understand the school E-safety policy and Acceptable Use Policies

Training – Governors

6.9 Governors should take part in E-safety training with particular importance for those who are members of any sub-committee / group involved in Computing / E-safety / health and safety /Safeguarding.

6.10 The school is responsible for ensuring that the infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

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

- School Computing systems are managed in ways that ensure that the school meets the E-safety technical requirements outlined in the Acceptable Use Policy and any relevant Local Authority E-Safety Policy and guidance
- Regular reviews and audits of the safety and security of school Computing systems take place.
- Servers, wireless systems and cabling must be securely located and physical access restricted. All users will have clearly defined access rights to school Computing systems.
- All users are provided with a username and password.
- The 'master / administrator' passwords for the school ICT Computing system, used by the Network Manager (or other person) must also be available to the Head teacher or other nominated senior leader and kept in a secure place (e.g. school safe)

7 Curriculum

7.1 E-safety should be a focus in all areas of the curriculum and staff should reinforce E-safety messages in the use of Computing across the curriculum.

7.2 In lessons where internet use is pre-planned, it is best practice that 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.

7.3 Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

7.4 It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff must request access in advance by contacting the school IT technician (Alan Clarke) or by directly contacting the safewall providers (East Riding)

7.5 Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

7.6 Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

8 Use of digital and video images - Photographic, Video

8.1 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 and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

8.2 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.

8.3 Staff 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. Staff all have access to a list of children whose photograph cannot be shared. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.

8.4 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.

8.5 Pupils must not take, use, share, publish or distribute images of others without their permission

8.6 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.

8.7 Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

8.8 Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. All parents sign a GDPR compliance form at the start of the year stating whether or not their child can be photographed.

8.9 Pupil's work can only be published with the permission of the pupil and parents or carers. This is covered in the GDPR compliance form.

9 Data Protection

9.1 Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 - the UK's implementation of the General Data Protection Regulation (GDPR), which states that:

Everyone responsible for using personal data has to follow strict rules called 'data protection principles.' They must make sure the information is:

- 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

9.2 Staff must ensure that they:

- At all times, take care to ensure the safekeeping 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, USB 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

10 Communications

10.1 A wide range of rapidly developing communications technologies has the potential to enhance learning. School currently considers the benefit of using these technologies for education outweighs their risks/disadvantages.

- No children are allowed to bring mobile phones into school. In the few cases, exceptions are made in consultation with parents and the head teacher; the phone will be switched off, locked in the main office and collected at the end of the day.
- If a child brings a phone to school, it will be switched off and locked in the main office and must be collected by an adult at the end of the school day.
- Staff must not use their mobile phone in the classroom and must not be used to take photographs.
- Use of chatrooms, instant messaging or social media sites is not allowed by pupils

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

- Official school email service is regarded as safe and secure.
- Users need to be aware that email communications can be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc.) must be professional in tone and content.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

11 Unsuitable / inappropriate activities

11.1 The activities outlined below are inappropriate and are not permitted using school equipment or systems inside or outside of school: The usage restricted by school is as follows:

- Users shall not visit sites, download, make, post or pass on material relating to child sexual abuse, pornography or adult material that breaches the Obscene Publications Act.
- Users shall not promote any kind of discrimination, hatred or illegal acts
- Users will not use school systems to run a private business
- Users will not reveal or publish confidential information
- Users will not participate in gambling, online gaming, shopping or video broadcasting (YouTube)

Responding to incidents of misuse

11.2 All members of the school community are responsible users of Computing, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. The SWGfL flowchart below shows the responses that will be made to any apparent or actual incidents of misuse.

11.3 If any apparent or actual misuse appears to involve illegal activity e.g.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- hate material
- other criminal conduct, activity or materials

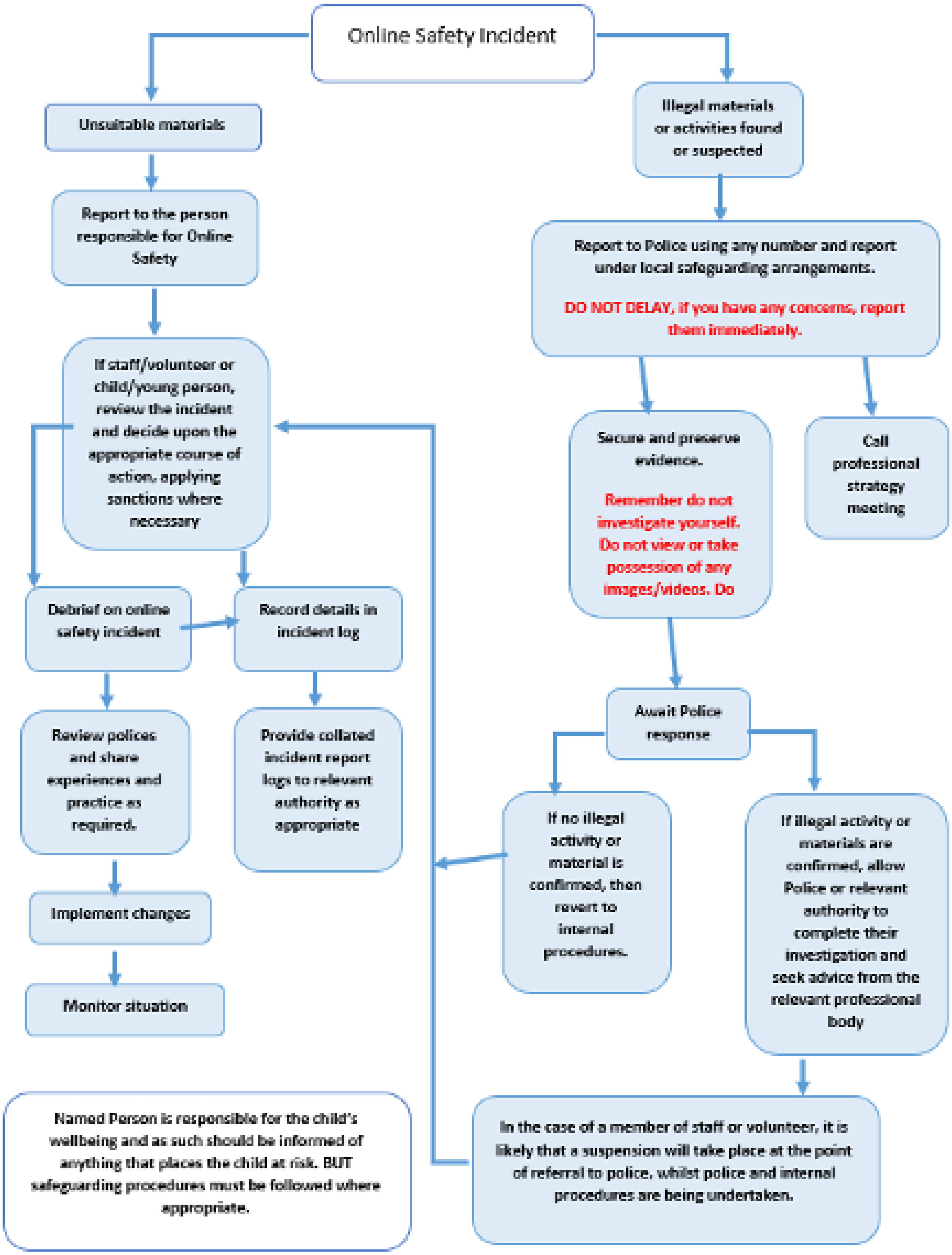
the headteacher must be informed immediately and the Police notified.

11.4 If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

11.5 School will deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows. If a member of staff suspects misuse has occurred the headteacher must be informed immediately.

11.6 If pupils are found misusing the equipment in ways outlined above the headteacher must be informed immediately who will then inform police (for illegal misuse) and the parents of the children. Actions and Sanctions will then be decided by the headteacher.

SWGfL Flowchart of response



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.