Online Safety Policy

2023- 2026

Background

Use of exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.
The improper or unsafe use of technology can present challenges to children, young people, volunteers and staff.

Some of the potential risks could 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 exploitation and abused 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 which may impact on the social and emotional development and learning of the young person.
- Blackmail involving threats to life, dignity and violence.
- Poor or inappropriate supervision of Internet access leading to the viewing of harmful or inappropriate.
- Risk of sexual exploitation

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).

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.

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 online 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 communications technologies for educational, personal and recreational use.

Development / Monitoring / Review

This online safety policy has been developed by a Strategic online safety working group made up of Headteachers, High School and Primary School ICT Leaders and Local Authority Staff and has been reviewed by a wide range of relevant stakeholders.

Schedule for Development / Monitoring / Review

This online safety policy was approved by the *Governing Body / Governors Sub Committee on:*	Autumn Term 2014
The implementation of this online safety policy will be monitored by the:	School's Senior Leadership Team & School's Designated Safeguarding Officer
Monitoring will take place at regular intervals:	
The *Governing Body / Governors Sub Committee* will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Three Year Rolling Programme
The online safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	Autumn Term 2020
Should serious online safety incidents take place, the following external persons / agencies should be informed:	LA Schools ICT Strategic Manager, LA Safeguarding Officer, Police Commissioner's Office

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of Internet activity (including sites visited)
- Surveys / questionnaires of:
- students / pupils (eg CEOP ThinkUknow survey)
- parents / carers
- staff

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The 2011 Education Act increased these powers with regards to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published behaviour policy.

The school will deal with such incidents within this policy and associated behaviour and antibullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that takes place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety of individuals and groups within the school:

Governors:
Governors are responsible for the approval of the online safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about online safety incidents and monitoring reports. The safeguarding Governor of the school's Governing Body will oversee this policy in conjunction with school staff and will conduct:
- regular meetings with the online safety Co-ordinator / safeguarding designated teacher
- regular monitoring of online safety incident logs
- reporting to relevant Governors committee / meeting

Headteacher & Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the online safety Co-ordinator / safeguarding designated teacher.
- The Headteacher / Senior Leaders are responsible for ensuring that the online safety Coordinator / safeguarding designated teacher and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Co-ordinator / safeguarding designated teacher.
- **The Headteacher and another members of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.** (see flow chart on dealing with online safety incidents and online safety incident included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / disciplinary procedures).

Online Safety Co-ordinator / Safeguarding Designated Teacher:

- leads the online safety committee
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff including how to be alert to the potential misuse of digital media and take responsibility for reporting it appropriately
- liaises with the Local Authority
- liaises with ICT technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments (see appendix).
- meets regularly with safeguarding Governor to discuss current issues, review incident logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

Network Manager/Technical Staff:

- 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/other relevant body online safety policies/guidance that may apply.

- Users may only access the networks and devices through a properly enforce password protection policy, in which staff passwords are changed regularly and pupils are taught about secure passwords.
- They keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- The use of the network/internet/virtual learning environment/remote access/email is regularly monitored so that any misuse/attempted misuse can be reported to the Headteacher/online safety coordinator for investigation/action/sanction.
- Software licence logs are accurate and up to date and that any software they upload has the requisite number of licences.
- Internet access is filtered for all users. The broadband/filtering provider filters illegal content by actively employing the Internet Watch Foundation CAIC list.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Ensuring the filtering system is always functioning effectively.

Teaching & Support staff:

Are responsible for ensuring that-

- they have an up to date awareness of online safety matters and of the current school online safety policy and school practices
- they have read, understood and digitally signed the school Staff Acceptable Use Agreement (AUA)
- they act as good role models in their use of digital technologies.
- they report any suspected misuse or problem to the Online Safety Co-ordinator / Senior Leader for investigation / action / sanction
- all digital communications (including Virtual Learning Environment's (VLE)) should be made on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and all digital activities.
- pupils understand and follow the school online safety and acceptable use policy
- they monitor the use of digital technologies, mobile devices, cameras etc in lesson and other school activities (where allowed) and implement current policies with regard to these devices
- They refer to the permissions database before allowing children to undertake online work or before publishing work/photos of children.
- 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.

Designated Safeguarding Officer:

should be trained in online safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials

- inappropriate online contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Agreement, which they will be expected to sign before being given access to school systems.
- need to understand the importance of safe use of digital media and how to report abuse, misuse or access to inappropriate materials and know how to do so.
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the Internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website / VLE and information about national / local online safety campaigns / literature.*

Parents and carers will be encouraged to support the *school* in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / VLE and on-line pupil records
- their children's personal devices in the school
- digital media and how to report abuse, misuse or access to inappropriate materials

Visiting Adults & Pupils

Users who access school ICT systems / website / VLE via login as part of the Extended School provision will be expected to sign an AUA before being provided with access to school systems.

Policy Statements

Education - Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students / pupils* to take a responsible approach. The education of *students / pupils* in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the Internet and mobile devices
- in lessons where Internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Where pupils are allowed to freely search the Internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in Internet searches being blocked. In such a situation, staff can request that the Local Authority (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Students should be supported to understand and report unsafe or harmful digital misuse.

Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often

children and young people come across potentially harmful and inappropriate material on the Internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, VLE
- Parents / Carers evenings / presentation evenings
- Reference to the relevant web sites / publications eg www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online Safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community
- Supporting community groups eg Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their online safety provision when requested

Education & Training – 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 will be made available to staff. An audit of the online safety training needs of all staff will be carried out regularly. It is expected that some staff will identify online safety as a training need within the performance management process.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Policies
- The Online Safety Coordinator / Designated Safeugarding Officer will receive regular updates through attendance at Consortium/ LA / other information / training sessions and by reviewing guidance documents released by BECTA / Consortium / LA and others.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Coordinator / Designated Safeugarding Officer will provide advice / guidance / training as required to individuals as required.

Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in ICT / online safety / health and safety / child protection. This may be offered in a number of ways:

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

Cyberbullying

Cyber bullying has become an increasing concern for schools, parents and children alike. Cyber bullying has traditionally been defined as harassment and victimisation using interactive technology. It is important that we understand the complex nature of cyber bullying to be able to prevent incidents and respond effectively to incidents when they arise. For example, one comment made online becomes bullying when it is repeatedly forwarded or commented on by others, which in turn is seen by multiple people over a sustained period of time. It can often be difficult to gain closure when subject to a cyber bullying incident when the comment or photo can resurface at anytime.

Cyber bullying differs from traditional forms of bullying and can have a significant detrimental impact upon individuals who are targeted by such behaviour. The 24/7 nature of cyber bullying can make it difficult for a target to escape the attacks directed at them. In some cases an individual may not know they are being bullied if they have not seen the content posted about them, but it is important to understand that the intentions of the perpetrator is still to bully the individual in question by posting humiliating and hurtful content.

We promote the positive use of Interactive Technology and Social Media, where pupils are provided with opportunities to discover the benefits social media has to their learning and social development. We understand that it can sometimes be easy to forget that we are talking to real people with real emotions when using social media; as such we encourage and promote responsible use and respectful communications with others online.

All incidents of inappropriate use of social media are taken seriously and we encourage all members of the school community to report any incidents of inappropriate use of social media and interactive technology.

Inappropriate use of social media includes, but not restricted too:

- harassment and intimidation of others,
- sending hateful messages,
- posting inappropriate and unwanted pictures online and;
- creating content which has the potential to hurt, embarrass and humiliate others.
- Sexting
- Online exploitation including sexual abuse

We respond to inappropriate use and bullying online in accordance with the procedures and guidance outlined in our anti-bullying and behaviour policy. Support is provided to all parties involved in incidents of bullying online and parents will be notified following a report of bullying online. Where appropriate we will contact external agencies to obtain further advice, information and provide additional support to individuals if necessary. Restorative approaches will be implemented to resolve any issues of inappropriate use of social media. We understand that in some circumstances there will be a requirement to involve the police. We will liaise with our Police School Liaison Officer for advice on the appropriate route and action to take in these circumstances.

Responding to Incidents of Misuse

It is hoped that all members of the school community will be responsible users of ICT, 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, e.g. searching for unsuitable/inappropriate material on the Internet that may cause harm to the person searching or anyone else who may view the material.

Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.

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

The flow chart on the next page should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

Mobile/Personal Devices Policy

Mobile technology devices may be school/college owned/provided or personally owned and might include smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's/college's wireless network. The device then has access to the wider internet which may include the school/college learning platform and other cloud-based services such as e-mail and data storage.

A range of mobile devices are used by the school to deliver the Curriculum of Wales. All users understand the primary purpose of the mobile/ personal devices in school is educational. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's online safety education programme.

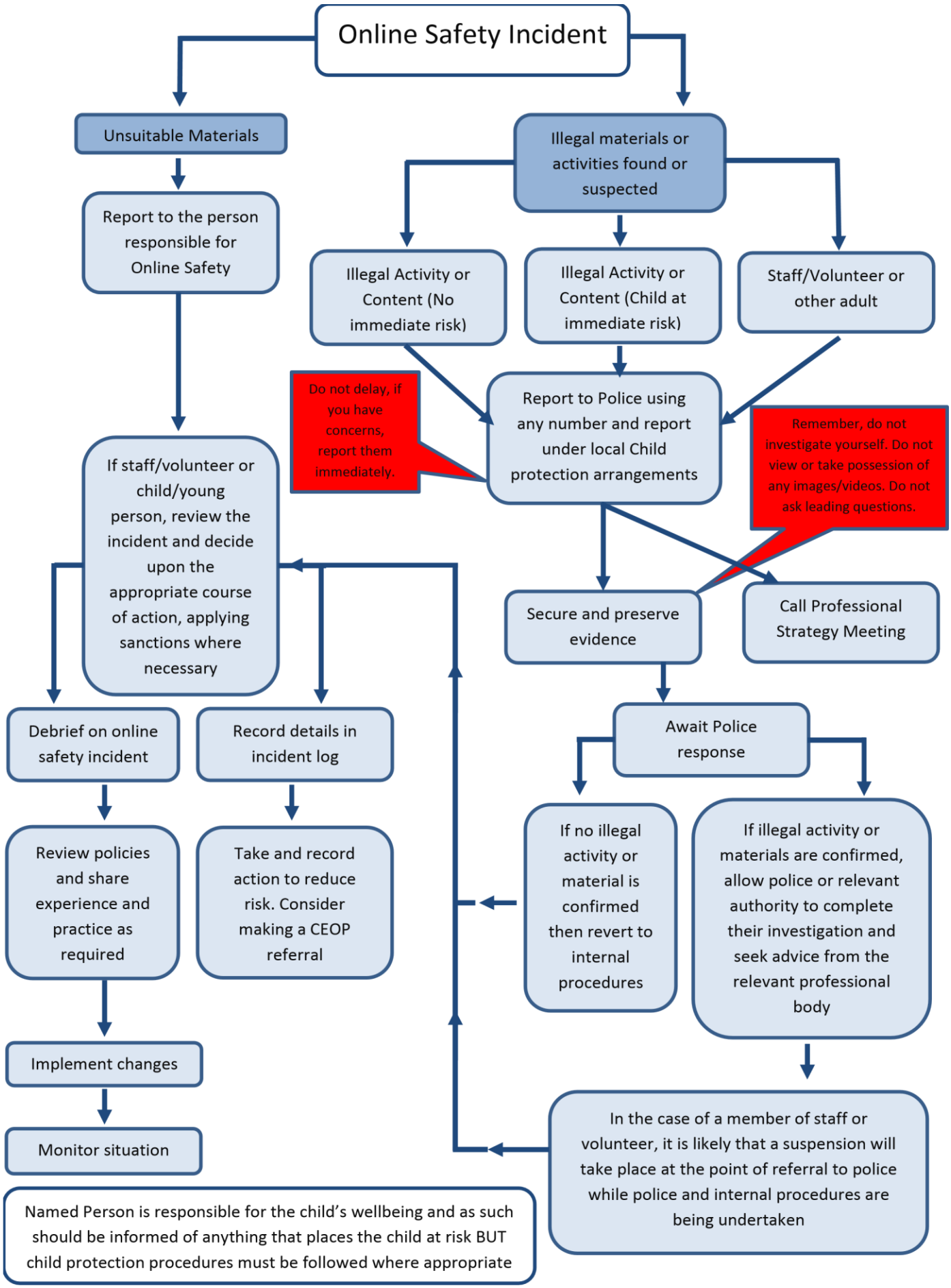
All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to those for safeguarding, behaviour, anti-bullying, acceptable use, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

All school equipment remains the property of Marlborough Primary School and are subject to routine monitoring without prior notice. They must be surrendered immediately upon request by the headteacher, deputy headteacher or member of the SLT.

There is no expectation of privacy for any user and the devices can be monitored at any time. This includes personal devices if they are used on school property or are connected to the school system in any way.

Privacy Policy
Marlborough Primary School follows and agrees with the UN Convention on the Rights of the Child (UNCRC). Article 16 of these rights is a child's right to privacy, should an online incident occur where a child is at risk/breach of the policy, the child will forego this right and Article 3 (best interests of the child) will take priority.
Teaching staff, SLT, the Headteacher or DSP may ask to see communications from both school owned accounts and those privately owned on personal devices.

Responding to Incidents 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
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Take and record action to reduce risk. Consider making a CEOP referral
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at immediate risk)
Staff/Volunteer or other adult
Do not delay, if you have concerns, report them immediately.
Report to Police using any number and report under local Child protection arrangements
Remember, do not investigate yourself. Do not view or take possession of any images/videos. Do not ask leading questions.
Secure and preserve evidence
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 while 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 child protection procedures must be followed where appropriate

Responding to Incidents of Misuse Continued…

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. In such event the "Guidance for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal disciplinary procedures that follows.

Social Media – Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and online safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Password Security

The school will be responsible for ensuring that the technology is as safe and secure as is reasonably possible and that users can only access data to which they have permission and access to personal data is securely controlled.

Responsibilities

The management of the password security policy will be the responsibility of the online safety Co-ordinator. Each user (adults and young people from KS2 onwards) should have their own password and be responsible for its security.

Training / Awareness

It is essential that users should be made aware of the need for keeping passwords secure, not written down or shared with anyone else.

- Adult users will be made aware of the password protocol:
  - at induction
  - through the Acceptable Use Agreement

Children / young people will be made aware of the password protocol:
- when joining the school
- informally through reminders from staff / volunteers
- through the Acceptable Use Agreement

The following rules apply to the use of passwords:
- the "master / administrator" passwords for the school should be held by more than one person (including the senior leader), should not be used for day to day use and must be stored securely.
- the master/administrator passwords for the Network, Hwb+ and other VLE's, and any other systems as appropriate will also be kept by the schools ICT team.
- passwords must be changed annually
- the password should be a minimum of 6 characters long and:
- should include a mixture of types of character
- should not include proper names
- temporary passwords e.g. users with new user accounts or replacement passwords will be forced to change the temporary password when they next log-on
- where users take laptops with personal data off-site these must be encrypted.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

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

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users need to be aware that email communications may 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 concerning school (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Staff should be mindful that if they are communicating information about a child via email to another member of school staff and the child's name is used then the information will be governed under data protection.
- The use of personal email addresses, text messaging or public chat / social networking programmes must not be used for professional purposes. Staff should remain professional in tone and content when discussing school online and should not bring the school into disrepute.
- 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.

Acceptable Use Agreement for Foundation Phase children

This is how we stay safe when we use computers:

- I will ask an adult if I want to use the computer equipment.
- I will only use activities that an adult has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong..
- I will tell an adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer.

Signed (child):……

Signed (parent): ……..

Acceptable Use Agreement for Key Stage Two children

I understand that while I am a member of Marlborough Primary School I must use technology in a responsible way.

For my own personal safety:

- I understand that my use of technology will be supervised and monitored.
- I will keep my password safe and will not use anyone else's (even with their permission)
- I will keep my own personal information safe as well as that of others.
- I will tell a trusted adult if anything makes me feel uncomfortable or upset when I see it online.

For the safety of others:

- I will not interfere with the way that others use their technology.
- I will be polite and responsible when I communicate with others, • I will not take or share images of anyone without their permission.

For the safety of the School:

- I will not try to access anything illegal
- I will not download anything that I do not have the right to use.
- I will only use my personal device if I have permission and use it within the agreed rules
- I will not deliberately bypass any systems designed to keep the school safer.
- I will tell a responsible person if I find any damage or faults with technology, however this may have happened.
- I will not attempt to install programmes of any type on the devices belonging to the school, without permission.

I understand that I am responsible for my actions and the consequences. I have read and understood the above and agree to follow these guidelines: ***Name***

Signature	
Date	

Acceptable Use Agreement for Marlborough Primary School staff/volunteers

Background

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe Internet access at all times.

Awareness

- Staff and volunteers will act responsibly to stay safer while online, being a good role model for younger users.
- effective systems are in place for the online safety of all users and the security of devices, systems, images, personal devices and data.
- staff and volunteers are aware of and can protect themselves from potential risk in their use of online technologies.

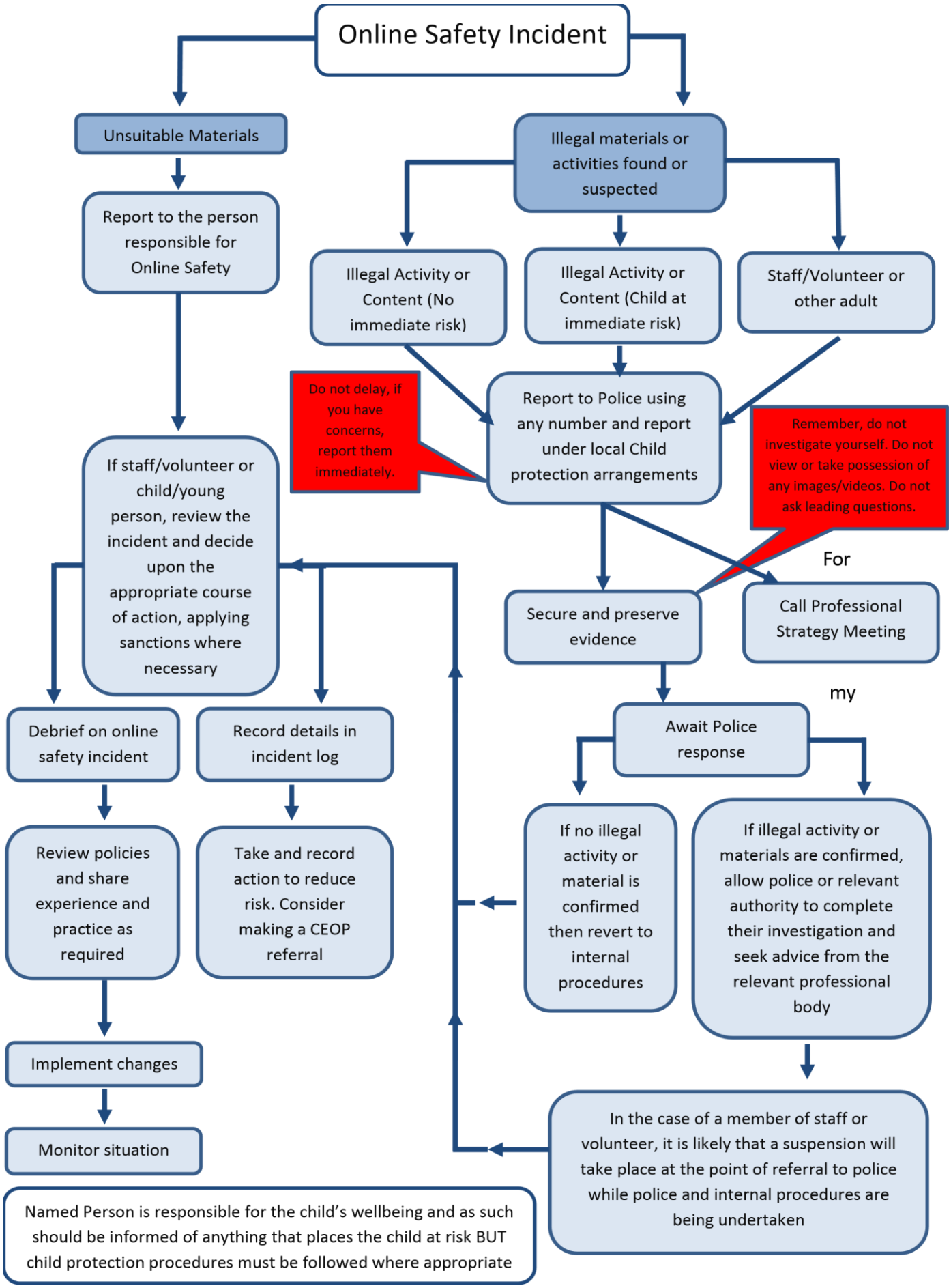
The term "professional" is used to describe the role of any member of staff, volunteer or responsible adult.

User Actions

In addition to there being clearly illegal activity, the school believes the activities referred to in the following section would be inappropriate in a school context and that users, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain Internet usage as follows:

User Actions		Acceptable	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978				X

sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**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	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute			X	
Using school systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
Use of social media on behalf of the school, including posting texts *1			X		
Use of social media on behalf of the school, including video/images *2			X		
***1 – The set up of an account on social media sites/apps MUST be approved by the school's online safety co-ordinator and that security settings are set high, so that the content is not visible to the general public.**					
***2 – There is a compiled list which identifies children who are NOT PERMITTED to be included in any image/video reproduction. The nominated users are responsible for ensuring that they are aware of the list and the children do not appear on any online platforms/social media/website.**					


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Take and record action to reduce risk. Consider making a CEOP referral
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at immediate risk)
Staff/Volunteer or other adult
Do not delay, if you have concerns, report them immediately.
Report to Police using any number and report under local Child protection arrangements
Remember, do not investigate yourself. Do not view or take possession of any images/videos. Do not ask leading questions.
Secure and preserve evidence
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 while 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 child protection procedures must be followed where appropriate

Professional and personal safety I understand that:

- I will ensure that my on-line activity does not compromise my professional responsibilities, nor bring the school into disrepute.
- My use of technology will be monitored.
- When communicating professionally I will use the technology provided by school (e.g.
  email and school social media accounts). I am fully aware of the staff handbook regarding the use of my mobile device.
- These rules also apply when using the school's technology either at home or away from the school site.
- Personal use of school technology is only acceptable with permission.

For the safety of others:

- I will not access, copy, remove or otherwise alter any other user's files, without authorisation.
- I will communicate with others in a professional manner and I am aware that any communication made about a pupil to a member of staff via email is subject to data protection law.
- I will share other's personal data only with their permission.
- I understand that any images I publish will be with the owner's permission and follow the school's code of practice.
- I will only use school equipment to record any digital and video images.

For the safety of the school I understand that

- I will not try to access anything illegal, harmful or inappropriate.
- It is my responsibility to immediately report any illegal, harmful or inappropriate incident.
- I will not share my online personal information (e.g. social networking profiles) with the children and young people in my care.
- I will not deliberately bypass any systems designed to keep school safe.
- Where personal data leaves the school site, it must be encrypted.
- I understand that data protection policy requires that any personal data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by a school policy to disclose such information to an appropriate authority.
- Personal passwords and those of other users should always be confidential.
- I will not download anything that I do not have the right to use.
- I will only use my personal device if I have permission and use it within the agreed rules.
- I will inform the appropriate person if I find any damage or faults with technology.
- I will not attempt to install programmes of any type on the devices belonging to the school, without permission.

I have read and fully understand the contents of the school's online safety policy.

Staff / Volunteer Name	
Signed	
Date	