Online Safety Policy
Effective for Academic Year 2022-25

A non-statutory policy

Date effective from	19th May 2022
Signed, Head Teacher	Gary Price
Signed, Chair of Governors	David Savage
Approved by governing body	19th May 2022
Date of next review	19th May 2025

Introduction
This policy aims to give all School community members clear guidance concerning the rationale, principles, strategies, and expectations of Online Safety at Horsley C of E Primary School Primary.

We aim to:
• Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
• Deliver an effective approach to online safety which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
• Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The four key categories of risk
Our approach to online safety is based on addressing the following categories of risk:

1. ***Content*** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
2. ***Contact*** – being subjected to harmful online communication with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults in order to exploit them for sexual, criminal, financial or other purposes
3. ***Conduct*** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g., consensual and non-consensual sharing of nudes and semi-nudes and pornography), sharing other explicit images; and
4. ***Commerce*** – risks such as online gambling, inappropriate advertising, phishing and financial scam

Development, Monitoring and Review of this Policy
This Online Safety policy has been developed by the Headteacher, Mr. Price (Designated Safeguarding Lead) and Online Safety Officer/Computing Lead, Mr. Feldon. It is developed in consultation with technical staff, staff, parents/carers, children and governors. In addition, consultation with the school community has taken place through a range of formal and informal meetings.

Schedule for Development, Monitoring and Review
The school will log incidents via CPOMS where appropriate.

Full Governing Body approved this Online Safety policy	19th May 2022
The implementation of this Online Safety policy will be monitored by:	Online Safety Lead –Mr. Peter Feldon DSL – Headteacher, Mr. Gary Price
Monitoring will take place at regular intervals:	Annually by the Computing Lead
The Governing Body will review the implementation of the Online Safety policy (including anonymous details of Online Safety incidents) at the end of each academic year.	Every three years
Should serious Online Safety incidents take place, the following external persons/agencies should be informed:	Police, the multi-agency safeguarding hub (MASH) 01452 426565 and select option 3 and CEOP.

Scope of the Policy

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

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place outside of School.

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of the internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Therefore, neither the school nor the Local Authority can accept liability for the material accessed or any consequence of internet access.

Roles and Responsibilities

Governors are responsible for the approval of the Online Safety Policy and reviewing the policy's effectiveness. This will be carried out by the Governors reviewing information about Online Safety incidents and monitoring reports. In addition, a member of the Governing Body has taken on the role of Online Safety Governor, Rev Caroline Bland.

The role of the Online Safety Governor will include: Annual meetings with the Online Safety Officer; Regular monitoring of Online Safety incident logs; Reporting to relevant Governor's meeting.

Head Teacher

- Have a duty of care for ensuring the safety (including Online Safety) of members of the school community, though the day-to-day responsibility for Online Safety will be delegated to the Online Safety Officer.
- Will ensure they are aware of the procedures to be followed in the event of a serious online safety allegation against a staff member.
- Will ensure that the Online Safety Lead and other relevant staff provide suitable training to enable them to carry out their Online Safety roles and to train other colleagues, as relevant.
- Will ensure that there is a system 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 support colleagues who take on important monitoring roles.
- Will receive annual monitoring reports from the Online Safety Officer.

The Designated Safeguarding Lead (Mr. Gary Price) should manage all online issues and incidents in relation to safeguarding and children protection in line with the school's safeguarding policy (supported by the DDSL, Mr. Peter Feldon). Serious child protection/safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line conduct with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Computing Lead (Mr. Peter Feldon)

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the School's Online Safety policies and documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident.
- Provides training and advice for staff.
- Liaises with school technical staff (currently provided by Thomas Keble Secondary School)
- Receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments.
- Meets annually with Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs.
- The production, review and monitoring of the school's Online Safety policy.
- Mapping and reviewing the Online Safety curricular provision – ensuring relevance, breadth and progression.
- Alongside IT support, monitoring network and internet.
- Consulting stakeholders: including parents/carers and the children about the Online Safety provision.

-

IT Support is responsible for ensuring that:

- The school's technical infrastructure is secure and is not open to misuse or malicious attack.
- The school meets the required Online Safety technical requirements and any Local Authority Guidance that may apply.
- Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- They keep up to date with Online Safety technical information to effectively carry out their Online Safety role and to inform and update others as relevant.
- That monitoring software/systems are implemented and updated as agreed in School policies.
- They adhere to all measures detailed in the school's data protection policy, safeguarding policy, Governor's confidentiality statement and GDPR legislation.

Teaching and Support Staff are responsible for ensuring that:

- They read, understood and signed the Staff Acceptable Use Policy (AUP) at the start of their contract.
- They have an up-to-date awareness of Online Safety matters and the current school Online Safety policy and practices.
- They report any suspected misuse or problem to the Headteacher or SLT for investigation.
- All digital communications with children/parents/carers should be professional and only carried out using official school systems (e.g., not Facebook).
- Interactions on their social media should not reference or discuss children, parents or staff where School matters are concerned.
- Online Safety issues are embedded in all aspects of the curriculum and other activities.
- Children understand and follow the Online Safety and acceptable use policies.
- Staff monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- In lessons where the internet is used, children should be guided to sites checked as suitable for their use.
- Processes should also be in place to deal with any unsuitable material found in internet searches.

Children

- Are responsible for using the school's digital technology systems in accordance with the Pupil Acceptable Use Policy.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good Online Safety practice when using digital technologies out of school that the school's Online Safety Policy covers their actions 'in' and 'out' of school.

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/ mobile devices appropriately. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, the school's Acceptable Use Policy, website and information about national/local Online Safety campaigns. Parents and carers will be encouraged to support the school's good Online Safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school's events.
- Their children's devices in the school (where this is allowed).

Visitors

Visitors and community members who use the school's systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

Policy Statements

Education for children. Whilst regulation and technical solutions are very important, their use must be balanced by educating children to take a responsible approach. Therefore, the education of children in Online Safety is an essential part of the school's Online Safety provision. Children need the help and support of the school to recognise and avoid Online Safety risks and build their resilience.

Online Safety should focus in all areas of the curriculum and staff should enforce Online Safety messages across all learning. 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 the Computing/PHSE/wider curriculum and should be regularly revisited.
- Key Online Safety messages should be reinforced as part of a planned worship and pastoral activities programme.
- Children should be taught in all lessons to be critically aware of the materials/content they access on-line to validate the accuracy of information when appropriate to the lesson.
- Children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Children should be helped to understand the need for the Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school should act as good role models in their use of digital technologies, the internet and mobile devices.
- During learning times where the internet is used, children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material found in internet searches.

- Where children are allowed to freely search the internet be vigilant in monitoring the content of the websites the young people visit.
- In the unlikely event that inappropriate/unsuitable content is found/searched for on a device by a child, the child is explicitly taught to close the device and report the incident to an adult immediately.
- It is accepted that from time to time, for good educational reasons, children 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 request that the Technical Staff (or other relevant designated person) temporarily remove those sites from the filtered list for the study period. Any request to do so, should be auditable, with clear reasons for the need.

Education for Parents and Carers. Parent/Carers play an essential role in the education of their children and the monitoring/regulation of the children's on-line behaviour. Parents may underestimate how often children 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, website.
- Parents/Carers Online Safety Workshops.
- High profile events/campaigns e.g., Safer Internet Day.
- Information about professional organisations such as CEOPs.

Education for Staff. It is essential that all staff receive Online Safety training and understand their responsibilities, as outlined in this policy. Therefore, training will be offered as follows:

- A planned programme of formal Online Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of all staff's Online Safety training needs 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's Safety policy and Acceptable Use Agreements.
- The Online Safety lead will receive regular updates by attending external training events and reviewing guidance documents released by relevant organisations.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff meetings.
- The Online Safety lead will provide advice as required.

Staff must be made aware that technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse and can abuse their peers online through harassing, and misogynistic messages

- Non-consensual sharing of indecent nude and semi-nude images and videos, especially around chat groups
- Sharing abusive images and pornography, to those who do not want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Education for Governors. In addition, governors should take part in Online Safety training/awareness sessions, with particular importance for link governors for computing/Online Safety/health and safety/child protection. This may be offered in a number of ways:

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

Technical: Infrastructure, equipment, filtering and monitoring

- The school will be responsible for ensuring that the school/infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. They will also need to ensure that the relevant people named in the above sections will effectively carry out their Online Safety responsibilities.
- School technical systems will be managed in ways that ensure that they meet recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling are securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- Internet access is filtered for all users. In addition, illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated, and internet use is logged and regularly monitored.
- School technical staff regularly monitor and record the activity of users on the school's technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate place for users to report any actual/potential technical incident/ security breach to the relevant person, as agreed.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school's infrastructure and individual workstations are protected by up-to-date virus software.
- An agreed process is in place for the provisionary access of "guests" (e.g., trainee teachers, supply teachers, visitors) onto the school's systems.
- Staff are made aware that removable media containing school data (e.g., memory sticks) must be encrypted 'in' and 'out' of school's data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Bring Your Own Device (BYOD)

- Children who bring their own mobile phone into school must leave it in the school office and collect it at the end of the school day. Children who bring in their own mobile phones do so at their own risk.
- Any staff who BYOD must adhere to the Staff Acceptable Use Agreement (see appendices).

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents, and children need to be aware of the risks associated with publishing on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or long term. It is common for employers to carry out internet searches for information relating to potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should educate children about the risks associated with the taking, use, sharing, publication and distribution attached to publishing their own images on the internet e.g., on social network sites.
- In accordance with, e.g., guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their own children at school events for their own personal use (. To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other children in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Children must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include children will be selected carefully and will comply with good practice guidance on the use of such images.
- Children's full names should not be used anywhere on a website or blog, particularly in association with photographs.
- Parents or carers will be given the opportunity to tell the school whether their child's photograph can be used when they fill in the school's registration forms.

Data Protection

- All data is managed in line with our Data Protection Policy

The school will ensure that

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary

- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data and up to date obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with our Data Protection Policy written with guidance from the LA.
- It has clear and understood arrangements for the security, storage and transfer of personal data.
- Data subjects have rights of access and there are clear procedures for this to be obtained.
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.

Staff must ensure that they

- 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, memory stick or any other removable media:
  - The data must be encrypted, and password protected.
  - The device must be password protected
  - The device must offer approved virus and malware checking software.
  - The data must be securely deleted from the device, in line with school's policy once it has been transferred or its use is complete.

Communications

When using communication technologies, the school considers good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school's policy, the receipt of communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and parents/carers (email, Twitter, social media etc.) must be professional in tone and content. These communications may only take place on official (monitored) school's systems. Personal email addresses, text messaging or social media must not be used for these communications.
- The contact details on the web should be the school address, e-mail and telephone number. Staff or children's personal information will not be published, with staff only contactable through: admin@horsley.gloucs.sch.uk.
- Whole class/group email addresses may be used at KS1, while children at KS2 and above may be provided with individual school email addresses for educational use.
- Children should be taught about Online Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communication and be reminded of the need to communicate appropriately when using digital technologies.

Social Media - Protecting Professional Identity and confidentiality

All schools and local authorities have a duty of care to provide a safe learning environment for children 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 harm must be in place. The school provides the following measures to ensure reasonable steps are in place to minimise the risk of harm to children, 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.

Staff should ensure that:

- No reference should be made in their social media to children, parents/carers or staff.
- They do not engage in online discussions on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority.

Unsuitable/inappropriate activities

The school believe that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside School when using school equipment or systems.

Responding to incidents of misuse

This guidance is intended for use when Staff need to manage incidents that involve the use of online content. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

If there is any suspicion. For example, incidents the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below) and report immediately to the police.

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Record all evidence of the incident on CPOMS.
- Inform parents/carers of any investigation that may involve their child and update the parents/carers of any outcomes where legally entitled to.
- Ensure that the child's welfare, if involved in an incident, is at the forefront of any investigation.

- Preventative and educational measures should be implemented to minimise the risk of the same incident happening again in the future. Where any stress has been caused to the child (as a result of an online incident. The school will provide a counselling 'aftercare' service to help with the recovery of the child.
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the 'url' of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - ➢ Internal response or discipline procedures
  - ➢ Involvement by Local Authority.
  - ➢ Police involvement and action.

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

- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material or other criminally racist conduct, activity or materials.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes.

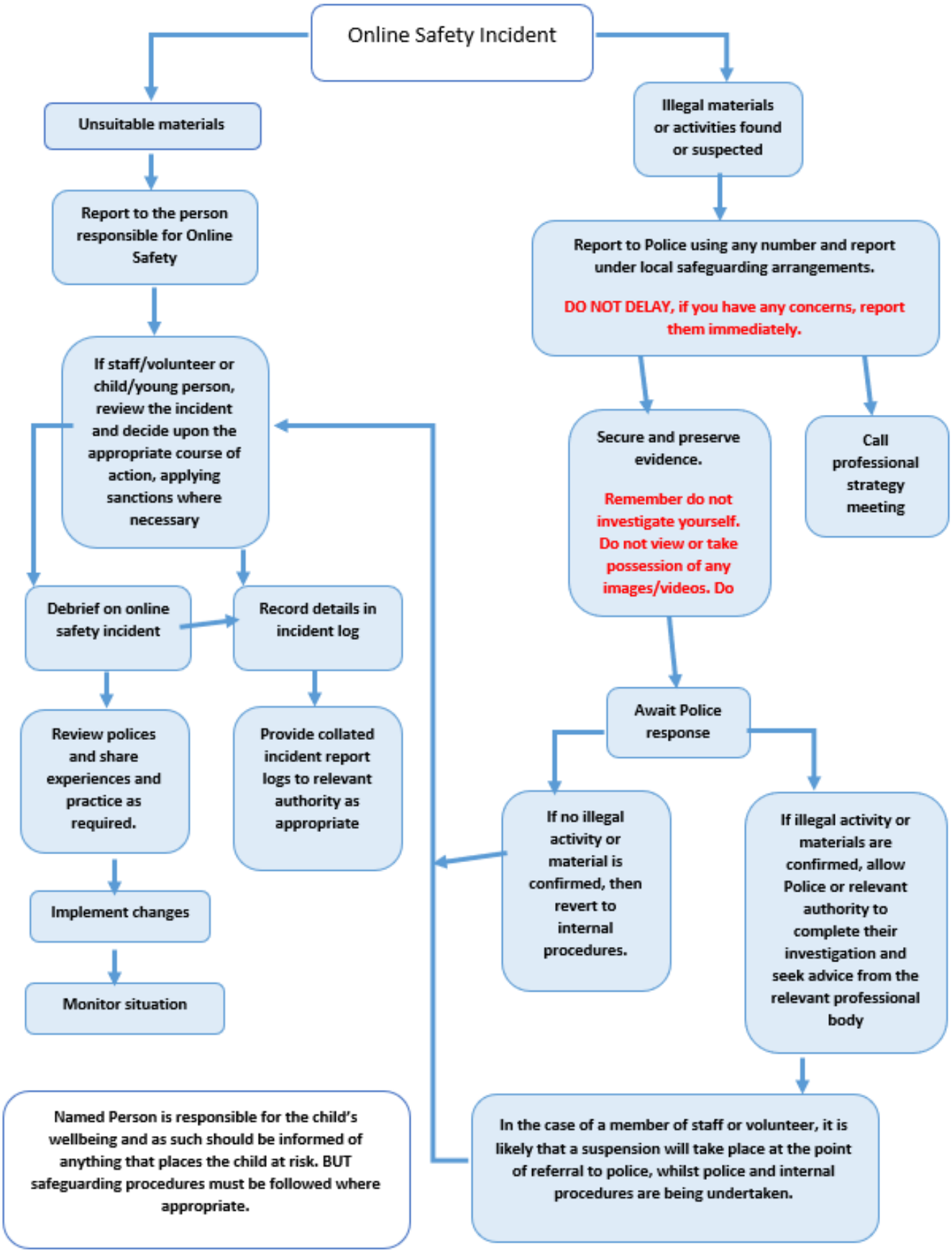
List of Appendices

- SMART Rules
- Online Safety Reporting Flowchart
- School Actions and Sanctions
- Staff (and Volunteer) Acceptable Use Policy
- Staff (and Volunteer) Acceptable Use Policy

SMART Rules


S
SAFE
Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.
m
MEETING
Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.
a
ACCEPTING
Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!
r
RELIABLE
Information you find on the internet may not be true, or someone online may be lying about who they are.
t
TELL
Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.
You can report online abuse to the police at www.thinkuknow.co.uk
THINK U KNOW .CO.UK

Online Safety Reporting Flowchart



School Actions and Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse when staff are using school equipment or BYOD on school premises. 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:

	Actions/Sanctions								
Students/Pupils Incidents	**Refer to class teacher/tutor**	**Refer to Head Teacher /Year/ other**	**Refer to Headteacher/Principal**	**Refer to Police**	**Refer to technical support staff for action re filtering/security etc.**	**Inform parents/carers**	**Removal of network/internet access**	**Warning**	**Further sanction e.g.**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).	X	X	X						
Unauthorised use of non-educational sites during lessons	X	X	X						
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	X	X	X						
Unauthorised/inappropriate use of social media/ messaging apps/personal email	X	X	X						
Unauthorised downloading or uploading of files	X	X	X						
Allowing others to access school/academy network by sharing username and passwords	X	X	X						
Attempting to access or accessing the school/academy network, using another student's/pupil's account	X	X	X						
Attempting to access or accessing the school/academy network, using the account of a member of staff	X	X	X						
Corrupting or destroying the data of other users	X	X	X						

Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X						
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X					
Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the School	X	X	X						
Using proxy sites or other means to subvert the school's/academy's filtering system	X	X	X						
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X						
Deliberately accessing or trying to access offensive or pornographic material	X	X	X						
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X						

	Actions/Sanctions							
Staff Incidents	**Refer to line manager**	**Refer to Headteacher**	**Refer to Local Authority/HR**	**Refer to Police**	**Refer to Technical Support Staff for action re filtering**	**Warning**	**Suspension**	**Disciplinary action**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).	X	X						
Inappropriate personal use of the internet/social media/personal email	X	X						
Unauthorised downloading or uploading of files	X	X						
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X						
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X						
Deliberate actions to breach data protection or network security rules	X	X						
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X						
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X					
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils								
Actions which could compromise the staff member's professional standing	X	X	X					
Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school/academy	X	X						

Using proxy sites or other means to subvert the school's/academy's filtering system	X	X						
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X						
Deliberately accessing or trying to access offensive or pornographic material	X	X	X					
Breaching copyright or licensing regulations	X	X						
Continued infringements of the above, following previous warnings or sanctions	X	X	X					

HORSLEY C of E PRIMARY SCHOOL

Staff (and Volunteer) Acceptable Use Policy

This Acceptable Use Policy is intended to ensure that:

- Staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for both educational and recreational use.
- School computing systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Staff and volunteers are protected from potential risks in using technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work and, therefore, also learning opportunities for pupils. In return, the school expects staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must responsibly use school systems to ensure that there is no risk to my safety, the safety of other users or the safety and security of the school's computing systems. I recognise the value of digital technology to enhance learning and ensure that pupils receive opportunities to gain from digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology.

For my professional and personal safety:

- ***I understand*** that the school will monitor my use of the school's digital technology and communications systems.
- ***I understand*** that the rules set out in this agreement also apply to using these devices and technologies (e.g., laptops, tablets, email, etc.) outside of school and to the transfer of personal data (digital or paper-based) outside of school.
- ***I understand*** that the school digital technology systems are primarily intended for educational use. Therefore, I will only use the systems for personal use within the rules set by the school.
- ***I will not*** disclose my username or password to anyone else, nor will I try to use any other person's username and password. I will change this regularly with the appropriate level of security.
- ***I will*** immediately report any illegal, inappropriate or harmful material or incident I become aware of to the appropriate person.
- **I will** only use my own personal device e.g., mobile phone for emergencies only. Other devices, e.g., personal laptops, should only be used with permission by SLT. Devices that require mains power must be PAT tested and be safe to use.

I will be professional in my communications and actions when using the school's computing systems:

- ***I will not*** access, copy, remove or otherwise alter any other user's files without express permission.

- ***I will*** professionally communicate with others. I will not use aggressive or inappropriate language, and I appreciate that others have different opinions.
- ***I will*** ensure that when I take and publish images of others, I will do so with their permission and use digital equipment owned only by the school. This should be then downloaded onto the server as soon as possible.
- ***I will*** not use my personal equipment or devices to record these images. Where these images are published (e.g. on the school website), it will not be possible to identify those who are featured by name or other personal information.
- ***I will*** only use social networking websites or apps at school, including Facebook or Instagram. I will only communicate with pupils and parents/carers using official school systems, including ClassDojo and school email. Any such communication will be professional in content and tone.
- ***I will not*** engage in any online activity that may compromise my professional responsibilities, e.g., gambling.
- ***I will not*** use personal email addresses with the school computing systems.
- ***I will not*** open any hyperlinks in emails or any attachments to emails unless the source is known and trusted or if I have any concerns about the validity of the email (e.g., due to the risk of the attachment containing viruses or other harmful programmes)
- ***I will*** ensure that my data is regularly backed up; this includes your work via a portable storage device or pen drive.
- ***I will not*** try to upload, download or access any materials which are illegal, inappropriate or may cause harm or distress to others. Furthermore, I will not try to use any programmes or software that might allow me to bypass the security systems to prevent access to such materials.
- ***I will not*** install or attempt to install software or apps on any computer or device, nor will I try to alter settings on any computer or device that may affect its integrity
- ***I will not*** disable or cause any damage to the school's equipment or equipment belonging to others. In addition, I will keep computing equipment in a safe and secure location.
- ***I understand*** that the school's data protection policy requires that any staff, volunteer or pupil data to which I have access be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- ***I will*** immediately report any damage to or faults with equipment or software; however, this may have occurred.
- ***I will*** ensure that where I have used the original work of others in my work, I have permission to do so.
- ***I will*** check and verify websites before they are accessible within the classroom environment, and I may only bypass the proxy firewall for educational purposes, including YouTube videos.
- ***I can*** make online purchases, but only school-related, and I know that my browser history can be monitored.
- ***I will not*** download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school

- I understand that this Acceptable Use Policy applies not only to my work and use of the school's digital technology equipment *in* school but also applies to my use of the school's digital technology equipment *offsite* and also use of my personal devices (including mobile phones) on the premises or in situations related to my employment by the school.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/Directors and the Local Authority and in the event of illegal activities, the involvement of the police.

I have read and understood the above and agree to use the school's systems.

Staff / Volunteer Name: _____
Signed: _____
Date: _____