Winslow Church of England School

Online Safety Policy

Approved by:	Governors	**Date:** 1st October 2026
Last Reviewed on :		
Next Review due by:	30th September 2027	

Vision

Our vision is 'Let your light shine'. The rainbow symbolises God's unconditional love for each individual. We seek to reflect that light in all we do: in our community, both local and wider, our communication, both word and action, with curiosity and courage, and with care and compassion for everyone, inspiring a love of learning.

At Winslow CE School, we see Online Safety as a fundamental part of children's education. The term "online safety" encompasses internet safety, digital technologies, artificial intelligence (AI), mobile devices, gaming platforms, social media and all forms of online communication. We believe that these procedures set out to make our pupils effective Digital Citizens who understand the dangers around them and can make effective reasoned choices in order to keep themselves safe. In a rapidly changing digital world we believe that this policy should be developed and reviewed annually.

Online technologies continue to evolve rapidly and now include artificial intelligence (AI), generative AI tools, social media platforms, messaging services, gaming environments and immersive technologies. At Winslow CE School we recognise both the educational benefits and safeguarding risks associated with these technologies. We are committed to ensuring pupils develop the knowledge, skills and resilience needed to use technology safely, responsibly and ethically.

1. Scope of the Procedures:

These procedures apply to all members of the school community (including staff, pupils, volunteers, parent /carers, visitors, community users) who have access to and are users of school IT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of 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 cyberbullying, child-on-child abuse or other Online Safety incidents covered by these procedures, which may take place outside of the school, but is linked to membership of the school.

The school will deal with such incidents within these procedures and associated behaviour and anti-bullying (including cyber bulling) policies and will, where known, inform parents/carers of incidents of inappropriate Online Safety behaviour that take place out of school.

These procedures are informed by:

- Keeping Children Safe in Education (KCSIE) (current version)
- Working Together to Safeguard Children (2023)
- The Online Safety Act 2023
- Data Protection Act 2018
- UK GDPR
- Education Act 2002
- Education and Inspections Act 2006
- The Prevent Duty Guidance
- DfE Meeting Digital and Technology Standards in Schools

- DfE Filtering and Monitoring Standards (2023)
- Teachers' Standards

The Online Safety Act 2023 places new duties on technology providers to reduce children's exposure to illegal and harmful online content. Although the Act primarily regulates online services rather than schools, schools continue to have a statutory safeguarding responsibility to educate pupils about online risks, respond appropriately to incidents and provide effective filtering, monitoring and education.

Artificial Intelligence (AI)

Artificial Intelligence (AI), including Generative AI tools such as chatbots and image generators, is becoming increasingly common within education and everyday life.

The school recognises that AI can:

- enhance learning
- support accessibility
- improve productivity
- develop digital literacy.

However, AI also presents safeguarding, privacy and educational risks. These include:

- inaccurate or misleading information
- age-inappropriate content
- bias and discrimination
- creation of harmful or inappropriate images
- deepfakes
- cyberbullying
- plagiarism
- sharing personal or confidential information with AI systems.

Staff Responsibilities

Staff will:

- only use AI systems approved by the school where appropriate;
- never input confidential or personal pupil information into public AI systems;
- verify AI-generated content before using it for teaching or communication;
- ensure AI supports rather than replaces professional judgement;
- teach pupils about responsible AI use;
- follow DfE guidance on Generative AI.

Pupil Responsibilities

Pupils will:

- use AI only when authorised by staff;
- understand that AI can produce inaccurate information;
- never use AI to bully, harass or create harmful content;
- never upload personal information into AI tools;

- acknowledge AI assistance where appropriate;
- understand that AI should support learning rather than replace independent thinking.

2. Education and Training

2.1 Pupils

Children and young people need the help and support of the school to recognise and avoid Online Safety risks and build their resilience. Online Safety is a focus in all areas of the curriculum and staff reinforce Online Safety messages across the curriculum. The Online Safety curriculum ensures that:

- Online Safety is part of a planned curriculum which provides progression
- Key Online Safety messages are reinforced as part of assemblies
- Pupils are taught in all lessons to be critically aware of the materials and content they access on-line.
- Pupils are encouraged to adopt safe and responsible practices 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 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. Many sites are blocked however teachers must remain vigilant about the content enabled.
- Pupils will learn about Artificial Intelligence and Generative AI, recognising AI-generated content, misinformation and deepfakes. This will include responsible use of AI tools and protecting personal information when using AI systems.

2.2 Parents and 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:

- Curriculum activities
- Letters, newsletters, web site
- Parents/Carers workshop
- High profile events / campaigns e.g. Safer Internet Day, Online Safety week
- Reference to relevant websites and publications

2.3 Staff and Volunteers

It is essential that all staff receive Online Safety training and understand their responsibilities, as outlined in these procedures. Training will be offered as follows:

- A planned programme of Online Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the Online Safety training needs of all staff will be carried out regularly.
- Annual safeguarding training for all staff will include developments in online safety, Artificial Intelligence, emerging safeguarding risks ad filtering and monitoring responsibilities.
- All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety procedures and Acceptable Use Agreements.
- These Online Safety procedures and their updates will be presented to and discussed by staff in staff meetings/phase meetings, and/or INSET days.
- The Computing Lead will provide advice, guidance and training to individuals as required.

2.3 Governors

Governors should have an awareness of Online Safety as part of their safeguarding training and monitor the implementation of this policy. This may take place in a number of ways:

- Attendance at a training event
- Attendance of a lesson
- Attendance of a school Online Safety assembly

3. Roles and Responsibilities

The following section outlines the Online Safety roles and responsibilities of individuals and groups within the school.

3.1 Governors:

Governors are responsible for the approval of the Online Safety Procedures and for reviewing the effectiveness of the procedures. This will be carried out by the Governors receiving regular information about Online Safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Safeguarding Governor. The role of the Safeguarding Governor will include:

- Regular meetings with the Computing Lead and Headteacher
- Regular monitoring of Online Safety incident logs
- Reporting to relevant Governors

3.2 Headteachers and Senior Leaders:

- The Headteacher has 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 Computing Lead.
- The Headteacher and DSLs are aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that the Computing Lead and other relevant staff receive suitable training to enable them to carry out their PREVENT and Online Safety roles and to train other colleagues, as relevant.
- The Senior Leadership Team will receive regular updates from the Computing Lead.

3.3 Computing Lead:

- Takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety procedures/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.
- Liaises with the Local Authority/relevant body.
- Liaises with school technicians.
- Receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments.
- Meets regularly with Safeguarding Governor to discuss current issues, review incident logs and filtering / change control logs.
- Attends relevant meetings.
- Reports regularly to Senior Leadership Team.

3.4 Technical Staff:

Technicians will ensure that:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required Online Safety technical requirements.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- That 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.
- That the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher and/or Computing Lead for investigation.

3.5 Teaching and Support Staff:

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of PREVENT, Online Safety matters, and of the current Online Safety procedures and practices.
- They have read, understood and signed the NetSmart Code of Practice (Appendix 2)
- They report any suspected misuse or problem to the Headteacher/Computing Lead for investigation.
- All digital communications with pupils and parents/carers should be on a professional level and only carried out using official school systems.
- Online Safety issues are embedded in all aspects of the curriculum and other activities.
- Pupils understand and follow the Online Safety and acceptable use procedures.
- Pupils have a good understanding of research skills.
- Pupils understand that information on the internet is not always reliable.

- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current procedures 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.

3.6 Designated Safeguarding Lead (DSL):

Technology provides additional means for child protection issues to arise therefore, we believe that the DSL should be trained in Online Safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- Access to illegal / inappropriate materials
- Sharing of personal data and GDPR
- Cyber-bullying
- Child-on-child abuse
- Child Sexual Exploitation
- Female Genital Mutilation
- Extremism, terrorism and Radicalisation
- Inappropriate on-line contact with adults /strangers
- Up-skirting (cameras and mobile phones)
- Potential or actual incidents of grooming
- AI generated abuse, including online coercion, sextortion and radicalisation

3.7 Pupils:

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand procedures on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images, child-on-child abuse 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 Procedures covers their actions out of school.

3.8 Parents and 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. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national and 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.

4. Filtering and monitoring

The school complies with the Department for Education's Filtering and Monitoring Standards. Whilst the Computing Lead has overall responsibility, together, the Headteacher and Technical Lead ensure that the school's infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within these procedures are implemented.

Filtering systems are designed to:

- block illegal content
- reduce exposure to harmful material
- support safeguarding
- protect against malware and phishing
- identify safeguarding concerns.

Monitoring systems are proportionate and help identify:

- bullying
- self-harm concerns
- extremist material
- inappropriate searches
- attempts to bypass filtering
- safeguarding concerns requiring intervention.

Filtering and monitoring systems are reviewed regularly by senior leaders and governors.

The school uses Bucks Schools Technical Support and Network Team for its computing requirements. The Bucks network uses Cisco Talos, part of Cisco's security solutions, known for being one of the largest and most trusted threat intelligence teams globally. Cisco Talos is used for content filtering within the network, ensuring that appropriate categories are blocked in line with statutory requirements, and sites are added as they are scanned and updated by Cisco Talos.

The school will work with Buckinghamshire Council to ensure that systems to protect pupils are regularly reviewed. If staff or pupils discover unsuitable sites, the URL must be reported to the Online Safety Lead. The Headteacher and Technical lead will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Any material that the school believes is illegal must be reported to appropriate agencies such as IWF (Internet Watch Foundation: http://www.iwf.org.uk/) or CEOP (Child Exploitation and Online Protection Centre: http://www.ceop.gov.uk/).

- School/technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school / technical systems and devices.
- The Technician and the Computing Lead are responsible for ensuring that software licence logs are accurate and up-to-date.
- Content 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 systems and users are made aware of this in the staff code of conduct.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, 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 infrastructure and individual workstations are protected by up to date virus software (Sophos).

- Staff are not permitted to download executable files and install programmes on school devices. Should this be necessary, staff members should consult either the computing Lead or the school's technician.
- The use of removable media (e.g. memory sticks) is not permitted by users on school devices. Files are shared on Teams or P Drive.
- Bring Your Own Device (BYOD) are permitted within school but staff are unable to access the network on them or use them for teaching purposes.

5. Use of digital and video images

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, parents/carers and pupils need to be aware of the risks associated with publishing digital images 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 longer term. It is common for employers to carry out internet searches for information about 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 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.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). 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 pupils 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 pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance and consent on the use of such images.
- 'Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Consent from parents or carers will be obtained before photographs of pupils are published on any media forum.

6. Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school ensures 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 for the purposes it was collected for.

- 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 will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy.
- The Headteacher is named as its Data Protection Officer (DPO).
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- It has clear and understood arrangements for the security, storage and transfer of personal data.
- There are clear and understood procedures and routines for the deletion and disposal of data.
- There are procedures for reporting, logging, managing and recovering from information risk incidents.
- There are clear procedures about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office (ICO).

Staff must ensure that:

- At all times take care to ensure the safe keeping 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.

7. 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. Users should be aware that email communications are monitored. Staff

and pupils should therefore use only the school email service to communicate with others when in school, or on school systems.

- Users must immediately report, to the Headteacher the receipt of any 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, parent mail etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems.
- Pupils 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 communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
- The school uses SIMS ID Outlook e-mail accounts and pupils are only permitted to use class group approved e-mail accounts with adult supervision.

8. Social Media – Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes procedures that set out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012' and all staff are expected to adhere to the school's code of conduct.

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
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk.

School staff should ensure that:

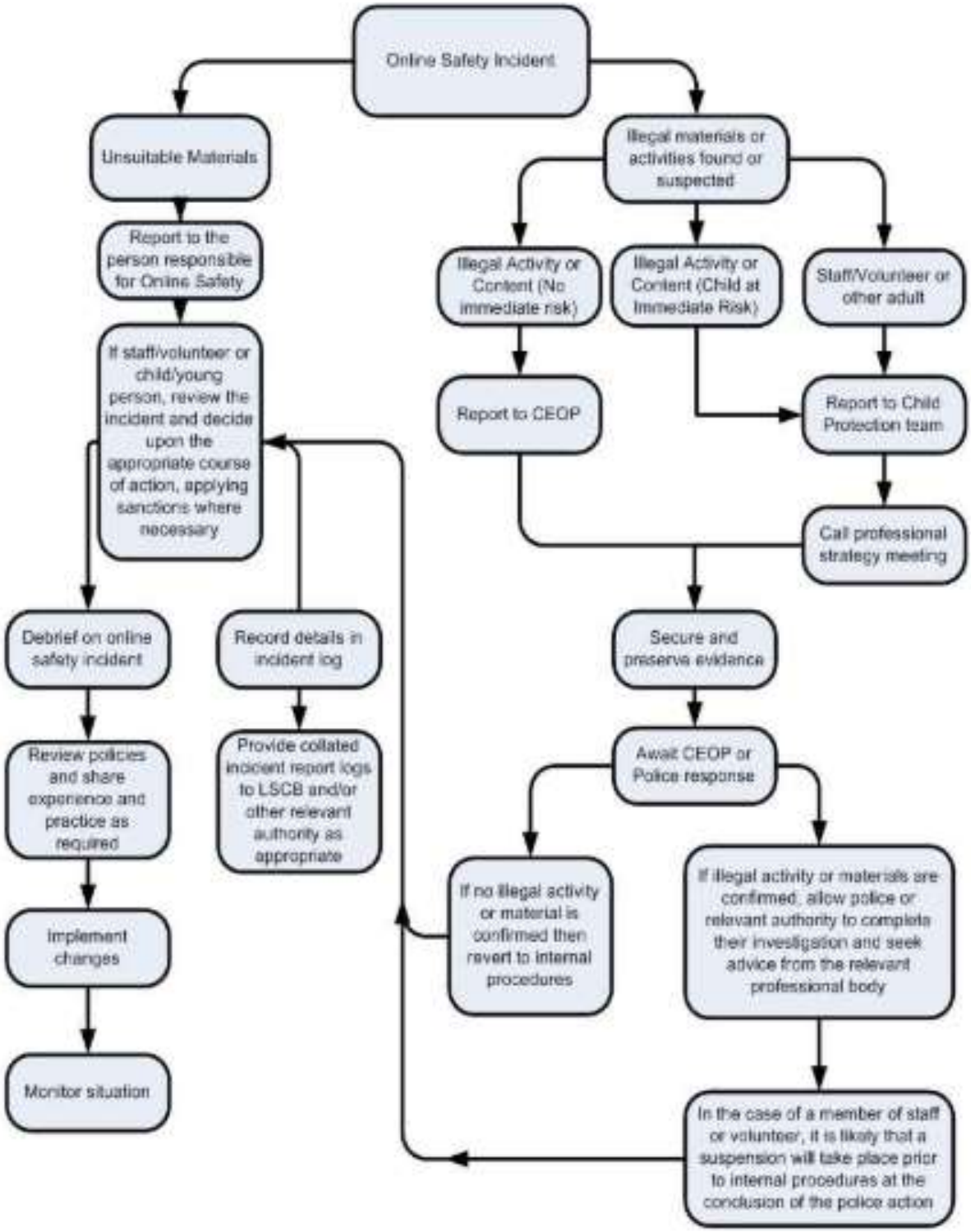
- No reference should be made in social media to pupils or parents/carers.
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school and/or local authority
- Security settings on personal social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

9. Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal incidents

If there is any suspicion that 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 appendix) for responding to online safety incidents 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 procedure. However, there may be times when infringements of the procedures 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:

- Has more than one member of staff/volunteer been involved in this process? This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should 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)
- 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 Designated Officer for Safeguarding (LADO) or national / local organisation (as relevant).
- Police involvement and/or 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
    - other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions and Sanctions

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 behaviour /disciplinary procedures as follows:

Pupils Actions/ Sanctions:

Incidents:	Refer to class teacher	Refer to Phase Leader	Refer to Headteacher	Refer to Technician re: Filtering/ security	Inform Parent/ Carers	Review of Network /internet access	Warning	Further Sanction
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			
Unauthorised use of digital camera / other mobile device			X		X			
Unauthorised downloading or uploading of files		X						
Allowing others to access school network by sharing username and passwords			X					
Corrupting or destroying the data of other users		X						
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X		X			
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X		X			
Using proxy sites or other means to subvert the school'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			

Staff Actions/ Sanctions:

Incidents:	Refer to Phase Leader	Refer to Headteacher	Refer to the LA/ HR	Refer to technical support team for action	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			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			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		X	X		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X			X		
Sending an email, text or message that is regarded as offensive, harassment or of a bulling nature	X	X	X		X	X	X
Using personal email/ social networking/ instant messaging/ text messaging to carry out digital communications with pupils	X	X	X		X	X	X
Actions which could compromise a staff members professional standing	X	X	X		X		
Actions which could bring the school into disrepute or breach the integrity of the school	X	X			X		
Using proxy settings or other means to subvert the school's filtering system	X	X		X	X		
Accidentally accessing offensive or pornographic material and failing to report it	X	X		X	X		
Deliberately accessing or trying to access offensive or pornographic material	X	X	X		X	X	X
Breaching copyright or licensing regulations	X	X			X		
Continuous infringements of the above, following previous warnings or sanctions	X	X	X		X	X	X

Use of Digital/ Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras and IPads to record evidence of activities in lessons and out of school.

These images may then be used in presentations in subsequent lessons. Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). 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 pupils in the digital / video images.

Smart Technology

Smart technology is part of everyday life for most children, parents and staff members. Smart technology includes mobile phones, cameras, tablets, smart watches and internet or AI enabled devices.

Mobile Phones:

- Members of staff can bring in their own personal mobile device into school but they are not permitted to make/receive calls/texts during contact time with children.
- Staff should have their phones on silent or switched off and out of sight (e.g. in their bag or classroom cupboard) during class time.
- Mobile phones can be used during break and lunchtimes but should not be used in a space where children are present.
- No pupils are permitted to bring in phones or any other hand held electronic devices unless pre-arranged as a special event.
- We recognise there are occasions when children may need to bring a mobile phone to school. This needs to be requested in writing to the Headteacher. If granted, the mobile phone must be placed in a named jiffy bag by parents and this should be handed into reception before the start of the school day.
- Only pupils in Years 5 and 6 who walk to or from school independently may bring a mobile phone into school. All mobile phones must be turned off while pupils are on the school site and handed to the class teacher on arrival (see Mobile Phone and Smart Watch Policy).
- Any phones found in school bags will be confiscated and parents required to collect these in person.
- The school accepts no responsibility for any loss or damage to a mobile phone whilst the device is on the school premises.
- Staff will have access to a school mobile phone for off site visits when required.

Smart Watches:

- Children are not permitted to wear Smart Watches to school.
- Any Smart Watches found to be used inappropriately will be confiscated and parents required to collect these in person.
- Under no circumstances should a Smart Watch be used by children to record still or video images, or to record audio whilst on the school premises.
- Staff are able to wear Smart Watches to school and they may be visible on a member of staff wrist, but they must be on silent mode and not used during contact time with children.
- Under no circumstances should a Smart Watch be used by teachers to record still or video images, or to record audio of the children.

Internet Access

Pupil usage is always fully supervised and individual usernames are required to access the Internet. Pupils will be informed that network and Internet use will be monitored and Online Safety rules will be posted in rooms with Internet access. Instruction in responsible and safe use will precede Internet access. Parents will be informed that pupils will be provided with supervised Internet access and asked to sign and return a consent form for pupil access - Pupils' NetSmart Code of Practice (Appendix 1). The school will maintain a current record of all pupils who are granted access to the school's electronic communications.

The school will take all possible precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Buckinghamshire Council can accept liability for the material accessed or any consequences resulting from Internet use however, methods to identify, assess and minimise risks will be reviewed regularly.

Curriculum Online Safety

- Online safety is planned into the curriculum across all year groups and is regularly revisited
- Resources on the CEOP' Think U Know' website is a basis for our Online Safety alongside the Switched On Computing Programme.
- Key Online Safety messages should be reinforced through assemblies and informal conversations when the opportunity arises.
- All teaching staff receive advice, training and guidance when required, on an ongoing basis.
- We support the Online Safety curriculum with pupils and parents by using the Police CEOP officers to give talks to the school community and workshops with the children.
- We reference parents to the 'Think u Know' website to support their understanding.

Appendix 1

Pupils' NetSmart Code of Practice

I'm NetSmart because:

- ✓ I only use the Internet when supervised by a teacher or adult.
- ✓ I never tell anyone I meet on the Internet my home address, my telephone number or my school's name, unless my teacher specifically gives me permission.
- ✓ I never send anyone my picture without permission from my teacher/parents/carer.
- ✓ If I am given a password I will never pass it on to anyone, even my best friend.
- ✓ I never arrange to meet anyone.
- ✓ I never hang around in an Internet chat room or in a Usenet conference if someone says or writes something which makes me feel uncomfortable or worried, and always report it to my teacher.
- ✓ I never respond to nasty, suggestive or rude emails or postings and I will always report it to my teacher.
- ✓ I always tell my teacher if I see bad language or distasteful things while I'm online.
- ✓ I am always myself and do not pretend to be anyone or anything I am not.
- ✓ I know that my teacher and the Internet service provider will check the sites I have visited.
- ✓ I understand that I will not be able to use the Internet if I deliberately misuse it.
- ✓ I understand that information on the Internet may not always be reliable and sources may need checking. Websites may be sponsored by advertisers.
- ✓ I understand that Artificial Intelligence (AI) can make mistakes and that I should always check information carefully.
- ✓ I will only use AI tools when my teacher allows me and I will not use AI to cheat or complete work dishonestly. .
- ✓ I will never upload personal information into AI tools.
- ✓ I will not use AI to create harmful or fake images or messages about other people

Pupil's Name:……

I have read the Pupils' NetSmart Code of Practice and I have discussed it with my son/daughter/ward. We agree to support the school's policy on the use of the Internet.

Signed:…….... (Parent/Guardian/Carer)

Date:……

Signed:……. (Pupil)

Appendix 2

Staff NetSmart Code of Practice

- Teachers closely monitor and scrutinise what their pupils are accessing on the Internet including checking the history of pages.
- Computer monitor screens are readily visible for the teacher, so they can monitor what the pupils are accessing.
- Pupils have clear guidelines for the content of e-mail messages, sending and receiving procedures.
- Pupils only use the Internet when supervised by a teacher or adult.
- Pupils are taught skills and techniques to enable efficient and effective use of the Internet.
- Pupils have a clearly defined focus for using the Internet and e-mail.
- If offensive materials are found the monitor should be switched off, any printed materials or disks will be confiscated and offensive URLs will be given to the Computing Lead or Network Administrator who will report it to the Internet Service Provider (BCC).
- Virus and malware protection is essential, as viruses can be downloaded accidentally from the Internet. Pupils bringing work from home, on a memory stick, could also infect the computer –Beware
- The recommended ISP will check sites visited by schools.
- Participating in Newsgroups/discussion groups – these groups are open to all … therefore be careful! It is recommended that pupils don't use these open forums.
- I will use AI responsibly and professionally and will never enter confidential school information into public AI systems.
- I will verify AI-generated content before using it.
- I understand that I remain accountable for any AI-assisted work.

I have read the NetSmart Code of Practice for pupils and teachers.

I agree to abide by the Teachers' Code of Conduct.

Name:……..……..

Signed:…….……..….. Date:……