SVPS Online Safety Policy 2023-2024

Governor Committee Responsible:	C & S	**Staff Lead**	Mr. G. Mills
Status	Non-Statutory	**Review Cycle**	Annual
Last Review	27th April 2023	**Next Review Date**	March 2024

Designation	Name	Date	Signature
Chair of C&S	Mrs S. Hulbert	27th April 2023	
Head Teacher	Mr. G. Mills	27th April 2023	

Introduction

We all have a responsibility to safeguard and promote the welfare of children. That responsibility must apply to the online world which is such an important part of the everyday life of children and young people.

At Swindon Village Primary School, new technologies open up many exciting benefits and opportunities for children but they can also present some risks. Technology is becoming all pervasive, touching all areas of society, with children and young people having access to an increasingly more complex technological world. We must ensure, therefore, that a framework is in place to help children stay safe when using new technology, and to ensure that where problems do occur, children (and their parents and carers) have support in dealing with them effectively.

Whilst the list grows on a daily basis, new technologies include:

- Websites
- Email and instant messaging
- Chat rooms and Social Networking
- Blogs
- Podcasting
- Video Broadcasting
- Video Conferencing (e.g. Zoom)
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web accessibility
- Other mobile devices with web accessibility

At Swindon Village, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the Internet and related technologies, both within and beyond the classroom.

Both this policy and the Acceptable Use Agreements (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by school (such as PCs, laptops, tablets, whiteboards, digital video) and technologies owned by pupils and staff which are brought onto the school premises (such as laptops, mobile phones and portable media players, etc…)

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by a variety of stakeholders:

- Headteacher
- Computing Subject Lead
- Staff
- Governors

1. 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 the *school*.

The latest Education and Inspections Act empowers Headteachers to such an 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 cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the *school*, but is linked to membership of the school. The latest Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Swindon Village Primary 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 out of school.

The policy has also been written in line with the recommendations of the latest 'Keeping Children Safe in Education Guidance'.

2. Roles and Responsibilities

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

2.1 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 receiving regular information

about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor (At Swindon Village, this role has been combined with that of the Child Protection / Safeguarding Governor).

The role of the Online Safety Governor will include:

- regular meetings with the Computing subject lead
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors / Committee / meeting

2.2 Headteacher 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 subject lead.
- The Headteacher and (at least) another member of the 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. To report an incident staff should follow the school safeguarding policy. The LADO should also be contacted.
- The Headteacher / Senior Leaders are responsible for ensuring that the Computing Subject Lead and other relevant staff receive suitable training 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. At Swindon Village this will be the designated governor for safeguarding.
- The Senior Leadership Team will receive regular monitoring reports from the Computing Lead.

2.3 Online Safety Coordinator / Officer: Mr Mills [HT and DSL] & Computing Lead(s)

- 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.
- liaises with the Local Authority / Gloucestershire Safeguarding Board / relevant body.
- liaises with school technical staff.

- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs.
- attends relevant meeting / committee of Governors.
- reports regularly to Senior Leadership Team.

2.4 Network Manager / Technical staff: Focus Network

The Network Manager / Technical Staff / Co-ordinator for ICT / Computing is responsible for ensuring:
- that the school's technical infrastructure is secure and is not easily open to misuse or malicious attack.
- that the school meets required online safety technical requirements and any relevant Online Safety Policies / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (Filtering provided by SWGfL and/or Focus)
- 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 / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Senior Leader; Computing Subject Lead for investigation / action / sanction.
- that monitoring software / systems are implemented and updated as agreed in school policies.

2.5 Teaching and 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 practices.
- they have read, understood and signed the Staff Acceptable Use Policy (AUP).
- they report any suspected misuse or problem to the Headteacher / Senior Leader / Computing Subject Lead for investigation / action / sanction.
- all SVPS-related digital communications with pupils / 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 Policy and acceptable use policies.

- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they 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 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 (Incidents recorded on the E-safety Recording Log sheet).

2.6 Designated Safeguarding Lead (DSL): Mr G Mills

The DSL has been trained in Online Safety issues and is aware of the potential for serious child protection / safeguarding issues to arise from:

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

It is important to emphasise that these are safeguarding issues, not technical issues, simply that the technology provides additional means for safeguarding issues to develop.

At Swindon Village, the Designated Safeguarding Lead is Mr G Mills and in his absence, the Deputy Designated Safeguarding Leads are Mr T Philcox, Mrs S O'Leary and Mrs L Brown – all of whom are on the Senior Leadership Team.

2.7 Pupils:
- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy.
- have a good understanding of the benefits and dangers of technologies that may be encountered both in and outside school.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- are aware of the impact of online (cyber) bullying and know how to seek help if they are affected by these issues.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- know and understand the correct use of taking and using images and to be aware of the dangers of cyber-bullying and sexting.

- 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.

2.8 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. The *school* will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature.* Parents and carers will be encouraged to support the *school* in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- online games & APPS
- video conferencing
- email and other digital platforms (e.g. Tapestry)
- social media

3. Education & Training Stake Holders

3.1 Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *pupils* to take a responsible approach. The education of *pupils* in online safety 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 and PHSE curriculum.
- Key online safety messages should be reinforced as part of a planned programme of assemblies.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils should be helped to understand the need for the pupil Acceptable Use Policy 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 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.

3.2 Educating 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:

- *Curriculum activities*
- *Letters, newsletters, web site links*
- *Parents / Carers evenings / sessions*
- *High profile events / campaigns e.g. Anti-bullying Week*
- *Reference to the relevant web sites / publications e.g.*
    - *swgfl.org.uk*
    - *www.saferinternet.org.uk/*
    - *http://www.childnet.com/parents-and-carers*
    - *www.thinkuknow.co.uk*

3.3 Staff / Volunteers

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. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly. (TES: Educare)
- 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 Agreements.
- The Computing Subject Lead (or other nominated person) will receive regular updates through attendance at external training events (e.g. from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days (where this is not possible information and training will be communicated through emails
- The Computing Subject Lead (or other nominated person) will provide advice / guidance / training to individuals as required.

4. Governors

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

- When available, attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (e.g. SWGfL/Educare).
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

5. Technical – infrastructure / equipment, filtering and monitoring

The school is 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. It will also ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- 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.
- All users will be provided with a username and secure password by the IT Technical Team.
- Users are responsible for the security of their username and password.
- The "master / administrator" passwords for the school Computing system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place.
- The IT Technical Team are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users by the SWGfL. 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. There is a clear process in place to deal with requests for filtering changes
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person.
- 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.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices (without permission from Computing Lead or Head Teacher).
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices.

6. Mobile Technologies

Mobile technology devices may be school 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 wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational.

- The school Acceptable Use Agreements for staff, pupils and parents/carers provides further information on the use of mobile technologies.

- The school allows:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*No (year 6 exception - switched off and stored by class teacher)*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet only				*No*	*Yes*	*No*
No network access				*No*	*Yes*	*No*

Personal devices:

- Staff are allowed to use personal mobile devices in school but Headteacher's permission must be sought and device will be routinely checked if required.
- Restrictions on where, when and how they may be used in school are made clear to staff.
- Staff will be allowed to use personal devices for school business.
- Filtering of the internet connection to these devices will be the same as with other filtering.
- Data Protection should be considered at all times.
- The right to take, examine and search users devices in the case of misuse can be requested at anytime if there is 'just' Safeguarding reasons.
- Taking (without seeking HT permission) / storage / use of images is not allowed.
- The school will not be liable for loss/damage or malfunction following access to the network.
- Visitors will be informed about school requirements on entry.
- Education about the safe and responsible use of mobile devices is included in the school Online Safety education programmes and on information found on the school website.

7. 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press.
- 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 negatively on any activities involving other *pupils* in the digital / video images.
- Staff and volunteers (where agreement has been sought and the images are viewed before leaving) 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 (in exceptional circumstances photos/videos may be used to communicate to parents but these will be deleted immediately from the device).
- 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 on the use of such images.
- Pupils' full names will not be used anywhere on a website or social media, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

8. Data Protection

Personal data will be recorded, processed, transferred and made available according to GDPR legislation 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.

8.1 The school must 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 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.
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA).
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO – Head Teacher) and Information Asset Owners (IAOs – Focus Network).
- Risk assessments are carried out.
- 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 and understood policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from information risk incidents.
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner's Office (see Acceptable Use Policy).

8.2 Staff must ensure that they:

- 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.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system:

- the device must be password protected.
- the device must offer approved virus and malware checking software.
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

9. Communication

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 (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, 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. (Online Safety BOOST includes an anonymous reporting app Whisper – https://boost.swgfl.org.uk/)
- Any digital communication between staff and pupils or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- 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.

10. Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies 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:

- Ensuring that personal information is not published
- Training is provided including: 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.

10.1 School staff and governors should ensure that:

- No reference should be made on private social media accounts to pupils and/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 or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

10.2 When official school social media accounts are established there should be:

- A process for approval by senior leaders.
- Clear processes for the administration and monitoring of these accounts
- Systems for reporting and dealing with abuse and misuse.
- Understanding of how incidents may be dealt with under school disciplinary procedures.

10.3 Personal Use:

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used, which associates itself with the school or impacts on the academy, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The school permits reasonable and appropriate access to private social media sites.

10.4 Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.

The school's use of social media for professional purposes will be checked regularly by the senior risk officer to ensure compliance with the school policies.

11. 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. Staff should follow the Safeguarding Policy.

11.1 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 / volunteer 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 – 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 / Academy Group 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
  - promotion of terrorism or extremism
  - 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 safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

11.2 School Actions & 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:

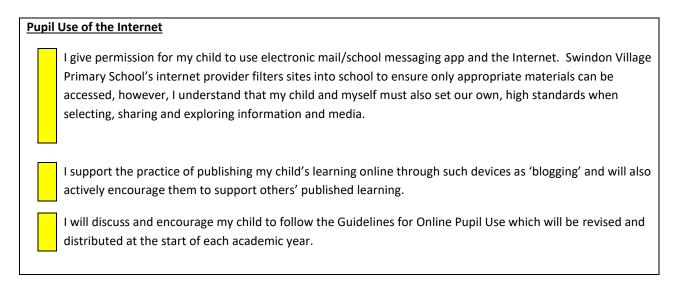|	Possible Actions / Sanctions								
Pupils Incidents	Refer to class teacher	Refer to member of Leadership Team	Refer to Headteacher	Refer to Police (dependent on circumstance)	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X	X	X	X	X	X
Unauthorised use of non-educational sites during lessons	X	X	X		X	X	X	X	X
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X	X	X	X	X	X	X	X	X
Unauthorised / inappropriate use of social media / messaging apps / personal email	X	X	X		X	X	X	X	X
Unauthorised downloading or uploading of files	X	X	X	X	X	X	X	X	X
Allowing others to access school network by sharing username and passwords	X	X	X	X	X	X	X	X	X
Attempting to access or accessing the school network, using another pupil's account	X	X	X		X	X	X	X	X
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X		X	X	X	X	X
Corrupting or destroying the data of other users	X	X	X	X	X	X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	X	X	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X		X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X	X	X	X	X	X	X
Using proxy sites or other means to subvert the school's filtering system	X	X	X	X	X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X	X	X	X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X	X	X	X	X	X	

	Possible Actions / Sanctions							
Staff Incidents	Refer to Headteacher / Deputy	Refer to DSL or DDSL	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	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	X	X	X	X	X	X
Inappropriate personal use of the internet / social media / personal email	X	X	X	X	X	X	X	X
Unauthorised downloading or uploading of files	X	X	X	X	X	X	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	X	X	X	X	X
Careless use of personal data e.g. holding or transferring data in an insecure manner	X				X	X	X	X
Deliberate actions to breach data protection or network security rules	X	X	X	X	X	X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X	X	X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	X	X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	X	X	X	X	X	X	X	X
Actions which could compromise the staff member's professional standing	X	X	X	X	X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X	X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X	X	X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X
Breaching copyright or licensing regulations	X	X	X	X	X	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X	X

eSafety Appendices

Appendix 1 - Useful Internet Safety Sites – COVID 19

- Internet matters - for support for parents and carers to keep their children safe online

- South West Grid for Learning - for support for parents and carers to keep their children safe online

- Net-aware - for support for parents and careers from the NSPCC

- Parent info - for support for parents and carers to keep their children safe online

- Thinkuknow - for advice from the National Crime Agency to stay safe online

- UK Safer Internet Centre - advice for parents and carers

- Free additional support for staff in responding to online safety issues can be accessed from the Professionals Online Safety Helpline at the UK Safer Internet Centre.

Appendix 2 – Registration Form Internet Section

Pupil Use of the Internet
I give permission for my child to use electronic mail/school messaging app and the Internet. Swindon Village Primary School's internet provider filters sites into school to ensure only appropriate materials can be accessed, however, I understand that my child and myself must also set our own, high standards when selecting, sharing and exploring information and media.
I support the practice of publishing my child's learning online through such devices as 'blogging' and will also actively encourage them to support others' published learning.
I will discuss and encourage my child to follow the Guidelines for Online Pupil Use which will be revised and distributed at the start of each academic year.

Swindon Village Primary School Online Reporting Log 2022-23

Class: ....

Date:	Time:	Incident:	Action Taken:		Incident Reported By?	Signature:
			What?	By Whom?		