Sherwell Valley Primary School - Online Safety Policy

This policy has been written by the Online Safety Lead with the oversight of the school's online safety team, building on best practice, government guidance and suggestions from the 360 degrees safe survey. It has been agreed by the online safety team, senior management, governors and digital leaders.

This policy and its implementation will be reviewed annually. The next review will be **April 2019** or more regularly in the light of any significant new developments in technology, new threats to online safety or incidents that have taken place in school. The demands of the 21st Century mean that our pupils will need to be alert to the new technologies and possibilities the internet can provide. We aim to ensure pupils are independently minded and confident citizens of the future.

Development / Monitoring / Review of this Policy

This online safety policy has been developed by a working group made up of:

- Online Safety Lead (Vicky Nevisky – August 2017)
- Headteacher Deputy Head DSL (Jonathan Gower)
- Deputy Head SLT (Jeremy Kingston)
- ICT Manager (Sharon Gilbert)
- Support Staff /Computing Technical staff (Deb Matthews – August 2017)
- Governor (Davina Schwarz)
- Parents (Andy Martin)
- Digital Leaders

Scope

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 Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying 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 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. 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 out of school.

Teaching and Learning

- Internet use is part of the statutory curriculum and a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction.
- Sherwell Valley Primary School has a duty to provide pupils with quality internet access as part of their learning experience.
- Pupils use the internet widely outside school and need to learn how to keep themselves safe online.
- The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

Benefits of using the Internet in education include:

- Access to worldwide online educational resources
- Learning and creating through apps
- Online learning platforms in school and at home.
- Access to experts in many fields for pupils and staff.
- Professional development for staff through access to national developments, educational materials and effective curriculum practice.
- Collaboration across networks of schools, support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system updates.

Online Safety Expectations

Education – pupils:

The education of Online Safety for pupils is an essential part of our school's online safety provision. The school will help and support the children to recognise and avoid online safety risks and to also build their resilience.

Online Safety education will be provided in the following ways:

- A planned online safety curriculum is provided as part of Computing and PSHE lessons and is regularly revisited.
- Key online safety messages are reinforced to children in assemblies and in lessons.
- Pupils are taught in lessons to be critically aware of the materials / content they access online and are guided to validate the accuracy of information.
- Pupils understand the need for the Pupil AUP **(See Appendix A)** and are encouraged to adopt safe and responsible use of Information and Communication Technology (ICT), the internet and mobile devices both within and outside school.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

Education – parents / carers:
Parents and carers play an essential role in the education of their children and in the monitoring of their online experiences, therefore Sherwell Valley Primary School will communicate effectively with parents to bridge the digital divide. The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, the School web site and Classdojo messenger
- Online safety evenings
- Parents evenings
- Reference to useful websites

Education & Training – Staff:
It is essential that all staff receive online safety training and understand this school policy and their responsibilities to it. Training will be offered as follows:

- Regular online safety training and updates will be made available to staff.
- 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 Staff and Volunteer Acceptable Use Policies **(See Appendix B)**.
- All staff must read this online safety policy

How will information systems security be maintained?

Virus protection is currently provided by Sophos.
Portable media may not be used without specific permission followed by a virus check.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓						✓	
Use of mobile phones in				✓				✓

lessons								
Use of mobile phones in social time	✓							✓
Taking photos personal camera devices (not mobile phones)				✓			✓	
Use of hand-held devices eg iPods, PDAs, PSPs, Nintendo DSs (provided by school)	✓					✓		
Use of personal email addresses in school, or on school network	✓							✓
Use of school email for personal emails	✓							✓
Use of online storage facilities (e.g. Dropbox, G-Suite) to store non-sensitive data	✓							✓
Use of chat rooms / facilities				✓				✓
Use of instant messaging				✓				✓
Use of social networking sites				✓				✓
Use of blogs	✓					✓		

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

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents / carers (email, chat, Class Dojo, Basecamp, and Instant Messenger) must be professional in tone and content.

•Personal email addresses, text messaging or public chat / social networking programmes must not be used to communicate with parents.
•Whole class or group email addresses will be used throughout the school
•Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
•Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

How will email be managed?

- Email accounts are provided by G-Suite and Office 365.
- Pupils may only use accounts provided by the school.
- Pupils must tell a designated member of staff if they receive offensive/inappropriate emails.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Staff will only use official school accounts to communicate with pupils and parents/carers.
- The forwarding of chain messages is not permitted.

Website and Newsletters

Permission is sought from parents, when they arrive at the school, before uploading photographs of their children on the school website. Children's first names and classes are to be used instead of full names.

How will social networking, social media and personal publishing be managed?

- Parents and teachers need to be aware that the internet has emerging online spaces and social networks which allow individuals to publish unmediated content. A supportive guide for parents can be found in **(Appendix C)**.
- Social networking sites can connect people with similar or even very different interests.
- Users can be invited to view personal spaces and leave comments, over which there may be limited control.
- Although primary age pupils should not use Facebook, Instagram, Snapchat or similar sites, pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published and their privacy settings.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.

- Pupils will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location.
- No member of staff should use social networking sites or personal publishing sites to communicate with students, past or present.
- This message is shared annually with staff.
- Staff need to be aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. Examples include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chat-rooms, instant messenger and many others.
- All staff are encouraged to maintain a professional digital footprint/profile.
- The school occasionally uses Facebook and Twitter as a source of engagement with our community.

How will filtering and monitoring be managed?

- Filtering is managed by Lightspeed Rocket, which falls in line with government recommendations. Weekly suspicious search reports are generated by Lightspeed Rocket for the school to analyse and act upon.
- The school has a filtering policy to mitigate risks of inappropriate activities **(see Appendix D)**.
- The school will work with Schools Broadband and Lightspeed Rocket to ensure that filtering policies are continually reviewed.

- The school has a procedure for reporting breaches of filtering. All members of the school community will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the ICT manager, who records the incident and escalate the concern as appropriate.
- The school filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Patterns and behaviours of students are identified in the suspicious search reports and are escalated as seen fit by the Headteacher.

Technical – Infrastructure/Equipment

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

•School ICT systems will be managed in ways that ensure that the school meets the online safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance
•There will be regular reviews and audits of the safety and security of school ICT systems
•Servers and cabling must be securely located and physical access restricted
•All users will have clearly defined access rights to school ICT systems, as set out in the user profiles and filter access. User profiles and filter access rights are clearly defined in the School ICT system. Details of the access rights available to groups of users will be recorded by the ICT Manager and will be reviewed, as and when required, by the On-line Safety Committee (or other group).
•Children in Years Three, Four, Five and Six will be provided with an individual username and individual password **(see Appendix E)**; children in Year Two will be provided with an individual username and class password; Children in Year One and Key Stage Zero will have an individual username but no password and Nursery pupils have a class username and no password. If required, Guest Users will be allocated an appropriate username and password with no access to shared drives.
•The ICT Manager will keep an up to date record of all usernames. Children's passwords will be recorded to aid memory. Users will be required to change their password every term.
•The "master / administrator" passwords for the school ICT system, used by the ICT Manager and ICT technician must also be available to the Headteacher and kept in the school safe.

•Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log-on details and must immediately report any suspicion or evidence that there has been a breach of security.

•In the event of the ICT Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher. Filtering requests are dealt with by the Deputy Head.

•Requests from staff for sites to be removed from the filtered list will be considered by the ICT Manager and the Deputy Head. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Committee.

•The school ICT manager will regularly (once a term) monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.

•An appropriate system is in place for users to report any actual / potential online safety incident to the ICT Manager. This will be displayed on all relevant ICT information boards, in the School office and in the Acceptable Use Policies for any issues to be highlighted to the ICT Manager immediately.

•Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices from accidental or malicious attempts which might threaten the security of the school systems and data.

•In the event of temporary access of “guests” (e.g. trainee teachers, visitors) onto the school system, “guests” will be allocated a profile which is appropriate for their usage requirements.

•The Staff Device Policy **(See Appendix F)** is in place regarding the extent of personal use that staff are allowed on devices and other portable devices that may be used out of school.

•The Staff Device policy is in place to inform users regarding the use of removable media (e.g. external HDDs, memory sticks / CDs / DVDs / cameras / memory cards / video cameras / any other USB devices) by users on school workstations / portable devices.

•The school infrastructure and individual workstations are protected by up to date virus software provided by Sophos.

How will online safety safeguarding concerns be handled?

All staff record online safety concerns on CPOMS. The Head and Online Safety Lead, as well as linked members of staff, are alerted to these incidents and add the necessary actions to resolve them. Strong communication links are maintained between all staff to ensure incidents are acted upon with immediate effect. The head teacher reviews all Online Safety Concerns on a regular basis.

How will cyber- bullying be managed?

Sherwell Valley aims to promote a culture of confident, responsible users of ICT so that pupils and staff are safe and responsible online. Cyber bullying (along with all types of bullying) will not be tolerated. All online-safety safeguarding incidents/concerns will be recorded on CPOMS by staff members, using the Online Safety tab button. Staff will specifically state the concern (cyber-bullying/inappropriately aged content). The necessary adults (parents/teachers/Headteacher) will communicate effectively to help the child resolve the problem. The Designated Child Protection Officer will also be informed of any online safety incidents involving child protection concerns and will be escalated appropriately.