Sudell Primary School

Internet-Safety Policy

Policy written by Vice Principal, October 2015

Reviewed: March 2019
Reviewed: March 2020
Reviewed: May 2021
Reviewed: September 2022
Review Date: September 2023

Principal: Helena Lewis

Chair of Governors: Phil Holden

Scope of the Policy

Internet-Safety encompasses internet technologies and electronic communications such as mobile phones and other digital devices. This policy highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

This policy will operate in conjunction with other school policies including those for computing, behaviour, remote learning and safeguarding.

- Our Internet–Safety Policy has been written by the school, by studying government guidance
- The Internet -Safety Policy and its implementation will be reviewed annually
- The school has appointed an Internet–Safety Lead

<u>Teaching and Learning</u>

Why is Internet use important?

- 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
- 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. The school has a duty to provide students with quality Internet access as part of their learning experience
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security
- Enabled remote learning and remote working

How does Internet use benefit education?

- Educational and cultural exchanges between pupils world-wide
- 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
- Access to learning wherever and whenever convenient
- Access to world-wide educational resources including museums and art galleries
- Access to on-line activities that will support the learning outcomes planned for the pupils' age and maturity
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

- Enable remote learning

How can we ensure legal compliance?

- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work
- School will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law

Responsible use and management of the Internet

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material (Lightspeed filters are in place on all links, staff apply strict filter to all Google image searches, internet access forbidden unless in the presence of a member of staff). However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Blackburn Lightspeed can accept liability for the material accessed, or any consequences of Internet access. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks are reviewed regularly
- All users will be informed that network and Internet use will be monitored. Internet-safety and internet access sessions will be taught and rules discussed to raise the awareness and importance of safe and responsible internet use. These will be taught at the beginning of each new school year. All staff at Sudell Primary School will also complete the Acceptable Use Policy (Appendix 2)

How will pupils learn how to evaluate Internet content?

- Pupils are taught to be critically aware of the materials they read and are shown how to validate information before accepting its accuracy
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum
- Pupils will use age-appropriate tools to research Internet content
- If staff or pupils discover unsuitable sites, the URL (address) and content will be reported to the Internet Service Provider via the Computing subject leader or ICT Technician

How will information systems security be maintained?

- Virus protection will be updated regularly
- The security of the school information systems and users will be reviewed regularly
- Personal data sent over the Internet or taken off site will be encrypted or is password protected
- Portable media needs to be scanned with anti-virus/malware scan, this includes usb/memory drives

- Unapproved software will not be allowed in pupils' work areas or attached to email
- Files held on the school's network will be regularly checked
- The Computing co-ordinator / network manager will review system capacity regularly
- The use of user logins and passwords to access the school network will be enforced
- Smoothwall monitoring in place, SLT alerted if any breaches

How will e-mail be managed?

- Staff will only use official school provided email accounts to communicate with each other, as approved by the Senior Leadership Team
- Pupils may only use approved email accounts for school purposes, these are managed by ITDS
- Pupils must immediately tell a designated member of staff if they receive offensive email
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult
- E-mail sent by pupils to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper
- The forwarding of chain emails is prohibited
- Designated staff may communicate with parent or carers via the school Facebook page or Twitter

How will the School Website and published content be managed?

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published
- The Principal/Vice Principal or designated staff will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright

Can pupil's images or work be published?

- Permission from parents or carers will be obtained before photographs of pupils are published on the school controlled social media or Website
- Pupils' full names will not be used anywhere on the Website or social media pages, particularly associated with photographs

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

- The school works with the Aldridge IT Support team and Blackburn/Lightspeed to block/control access to social media and social networking sites
- Pupils will not be allowed access to public or unregulated chat rooms
- Newsgroups will be blocked unless a specific use is approved

- 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
- Staff will sign the Acceptable User Policy before using Social Media tools in the classroom
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parent or carers, particularly when concerning students' underage use of sites
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy

How will filtering be managed?

- The school will work with the Aldridge IT Support team and Blackburn/Lightspeed to ensure that the filtering policy is continually reviewed
- Virus protection is updated regularly
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure. See Appendix 1
- If staff or pupils discover unsuitable sites, the URL will be reported to the senior leadership team who will then record the incident and escalate the concern as appropriate
- The school's broadband access will include filtering appropriate to the age and maturity of pupil
- Smoothwall has been installed on all PC's in school and laptops to aid monitoring

How will videoconferencing be managed?

- If pupils are ever involved in videoconferencing, including the use of Teams, this will be appropriately supervised by a DSL and only involve those whose parents or carers have given consent. Children will not be able to make or receive a video conference call unless they are supervised

How can emerging technologies be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed
- Mobile phones in school will be limited to Year 5 and Year 6. Parents or carers must give written permission for their children and the phones should be kept in a locked place in the classroom
- The senior leadership team should note that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications

How should personal data be protected?

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998

<u>Policy Decisions</u>

How will Internet access be authorised?

- All staff must read and sign the 'Staff Acceptable Usage Agreement' before using any school computing resource. (See Appendix 2)
- At Key Stage 1, access to the Internet will be by adult demonstration with supervised access to specific, approved on-line materials or links through internet shortcut folders. At Key Stage 2 pupils will be supervised when on the Internet. Pupils will use age-appropriate search engines (e.g. BBC Search) and online tools and online activities will be teacher-directed where necessary. There will be no use of the internet on any computers by pupils before, after school or during breaks unless they are directly supervised by a member of staff
- Parents or carers will be informed that pupils will be provided with supervised Internet access
- Parents or carers will be asked to sign and return a consent form when they start school
- Internet safety rules are displayed in classrooms and the Computer suite. These rules are reinforced to the children whenever the internet is accessed. Pupils are informed that internet access is monitored

How will risks be assessed?

The school will take all reasonable precautions to ensure that users access only appropriate material.

- All staff including teachers, supply staff, classroom assistants and support staff, will be made aware of this policy, and its importance explained
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential
- Staff development in safe and responsible Internet use and on school Internet policy will be provided as required
- Staff are also expected to use the internet appropriately in school. Expectations of staff are outlined in the staff Acceptable Use Agreement
- The school will audit Computing provision to establish if the Internet-Safety policy is adequate and that its implementation is effective
- The school will take all reasonable 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 Blackburn/Lightspeed can accept liability for the material accessed, or any consequences resulting from Internet use

How will the school respond to any incidents of concern?

- All members of the school community will be informed about the procedure for reporting Internet-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc). See Appendix 1
- All incidents should be recorded on CPOM's
- Staff should report any internet safety issues on CPOM's. The Principal will record any Internet-Safety incidents which become CP concerns as a follow action on CPOM's. Designated Child Protection Coordinator will be informed of any Internet-Safety incidents involving Child Protection concerns, which will then be escalated appropriately
- The school will manage Internet-Safety incidents in accordance with the school discipline/behaviour policy where appropriate
- The school will inform parents or carers of any incidents of concerns as and when required
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguarding Team and the Principal will act swiftly based on any advice given
- If the school is unsure how to proceed with any incidents of concern, they will seek advice from the Area Children's Officer or the County Internet-Safety Officer and act accordingly
- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the Internet-Safety officer to communicate to other schools in the area/Local Authority if appropriate

How will internet-safety complaints be handled?

- Complaints about internet safety should be made under the school's complaints policy which can be found on the school website
- If a child misuses the internet then sanctions are in place to address the inappropriate behaviour
- Parents' attention will be drawn to the School Internet Policy and Rules in newsletters and on the school Web site
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures
- All Internet–Safety complaints and incidents will be recorded by the school on CPOM's, including any actions taken
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community

- Internet issues will be handled sensitively to inform parents or carers without undue alarm
- A partnership approach with parents or carers will be encouraged. This could include communications through the school newsletter, practical sessions and suggestions for safe Internet use at home

How is the Internet used across the community?

- This policy will be made known to any members of the community who may access the internet in school e.g. Adult Education classes

How will Cyberbullying be managed?

- Cyberbullying (along with all other forms of bullying) of any member of the school/community will not be tolerated
- Details are set out in the school's policy on anti-bullying and behaviour
- All incidents of Cyberbullying reported to the school will be recorded
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children and young people within or outside of the setting in a professional capacity
- Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Senior Leadership Team in emergency circumstances
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose
- If a member of staff breaches the school policy then disciplinary action may be taken

Equal Opportunities and Racial Equality (Refer also to these specific policies)

All school policies have an explicit aim of promoting race equality and will be reviewed in terms of their contribution and effectiveness in achieving this aim.

Sudell Primary School provides a broad and balanced curriculum for all pupils. The school accepts the three principles in the statutory inclusion statement for the National Curriculum:

- Setting suitable learning challenges for all pupils
- Responding to pupils' diverse learning needs
- Overcoming potential barriers to learning and assessment for individuals and groups of pupils

We recognise that citizenship presents opportunities for encouraging respect for diversity.

Our curriculum co-coordinators are responsible for ensuring their subject programmes/schemes of work raise awareness of multi-cultural issues and challenge stereotypical views of different racial groups and nomadic communities. In the purchase of resources, our curriculum co-coordinators will ensure that materials reflect and celebrate ethnic and cultural diversity.

Looked After Children

As for all our pupils, Sudell Primary School is committed to helping every Looked After Child to achieve the highest standards they can. To this end staff will ensure that in delivering the curriculum they set suitable learning challenges of LAC, respond to the diverse learning needs of LAC, and help to overcome the potential barriers to learning and assessment for LAC. The Computing coordinator will support staff in doing this within this subject.

How will the policy be introduced to pupils?

- An Internet–Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils
- Pupil instruction regarding responsible and safe use will precede Internet access
- Internet–Safety training will be part of the induction and transition programme
- Internet-Safety rules will be posted in all rooms with Internet access
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas
- Particular attention to Internet-Safety education will be given where pupils are considered to be vulnerable

How will the policy be discussed with staff?

- The Internet–Safety Policy will be formally provided to and discussed with all members of staff
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff
- To protect all staff and pupils, the school will implement a Staff code of conduct – Acceptable Use Policy

How will parents or carers support be enlisted?

- Parents or carers attention will be drawn to the school Internet–Safety Policy in newsletters and on the school website
- Parents or carers will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children
- Information and guidance for parents or carers on Internet–Safety will be made available in a variety of formats
- Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents or care

Appendix 1:

Response to an incident of concern

Internet technologies and electronic communications provide children and young people with the opportunity to broaden their learning experience and develop creativity in and out of school. However, it is also important to consider the risks associated with how these technologies are used.

Any Internet-Safety Policy should also recognise and seek to develop the skills that children and young people need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for other users.

These risks to Internet-safety are, of course, caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in detecting danger to pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to occasional extremely concerning incidents that may involve Child Protection Officers or the Police.

This section will help staff determine what action they can take within the school and when to hand the issue over to the school-based Child Protection Co-ordinator, the Internet–Safety Lead or the Police Liaison Officer.

What does electronic communication include?

• Internet collaboration tools: social networking sites and blogs

• Internet Research: web sites, search engines and Web browsers

• Mobile Phones and personal digital assistants (PDAs)

• Internet communications: e-Mail and instant messaging (IM)

• Webcams and videoconferencing

What are the risks?

• Receiving inappropriate content

• Predation and grooming

• Requests for personal information

• Viewing ‘incitement’ sites

• Bullying and threats

• Identity theft

• Publishing inappropriate content

• Online gambling

- Misuse of computer systems
- Publishing personal information / images
- Hacking and security breaches

How do we respond?

Smoothwall will alert the DSL's in school about any misuse of school devices. The Principal and/or other Designated Safeguarding Leads in school should be informed immediately of any other issues.

Appendix 2: Sudell Primary School - Staff Acceptable Usage Agreement

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for illegal purposes.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will ensure that any school laptop used at home will not be lent to or used by any third party.
- I will respect copyright and intellectual property rights. Resources and planning prepared for school are jointly owned by the school.
- I will report any incidents of concern regarding children's safety to the school Internet-Safety Lead or the Designated Child Protection Coordinator.
- I will ensure that I will not engage with any electronic communications with pupils, including former pupils.
- I will ensure that any communications compatible with my professional role.
- I will promote Internet-Safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- I understand that school information systems may not be used for private purposes without specific permission from the Principal.
- I will ensure that any pupil's portable media devices are scanned before using at school.
- I acknowledge that…"At Key Stage 1, access to the Internet will be by adult demonstration with supervised access to specific, approved on-line materials or links through internet shortcuts folder. At Key Stage 2 pupils will be supervised when on the Internet. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary. There will be no use of the internet by pupils before, after school or during breaks unless they are supervised by a teacher or parent or carer." See Internet-safety Policy for more details.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be

taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Acceptable Usage Policy Signed:

Signature: …….

Print name: ……

Date: ……..