SOHO PARISH PRIMARY POLICY

IT and Internet Acceptable Use Policy

Last reviewed:	June 2020	Next review date:	June 2023
Committee responsible	SAW	Written by	Louise Ritchie

1. Scope

E-Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology.

This policy highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for the users to enable them to control their online experiences. It also covers internet & electronic media use by staff.

2. Internet

2.1. Why is internet use in school important?

- 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 personal safety and security whilst 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.

2.2. How can Internet use enhance learning?

- Internet access will be planned to enrich and extend learning activities. Access levels will reflect the curriculum requirements and age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Staff should guide pupils in 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.

2.3. How will pupils learn to evaluate Internet content?

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop skills in selection and evaluation.

- The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law. Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

3. Managing Information Systems

3.1. IS Security

Internet Filtering

- The school works in partnership with our Internet Service Provider (LGfL) to ensure systems to protect pupils are reviewed and improved.
- LGfL provides a comprehensive web filtering service in support of schools' safeguarding responsibilities. Inappropriate sites are blocked, all use of the Internet is monitored and can be traced by IP address and authenticated USO username

System security

- Virus protection is installed and maintained by our technical support provider (currentlyAdept) and updated regularly.
- Security strategies will be discussed with the LA, particularly where a wide area network connection is being planned.
- Administration rights, including permission to install software, is managed using a hierarchical system by our technical support provider

Data protection

- Personal data sent over the Internet will be encrypted or otherwise secured. Personal data should be password protected if sent outside the school lgfl email network.
- Use of portable media such as floppy disks, memory sticks and CD-ROMs is no longer permitted.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Files held on the school's network are backed-up remotely daily.
- The IT lead / network manager will ensure that the system has the capacity to take increased traffic caused by Internet use.
- Pupil data including photographs is held as long as the school is required to process it and destroyed by the term following the pupil being taken off roll. Certain photographs or pieces of work can be kept where the subject is anonymous or special permission has been granted by the pupil's parent (e.g. for showcase work).

3.2. E-mail

- Pupils may only use approved e-mail accounts on the school system (LGfL with a school alias, e.g. _____@sohoparish.co.uk)
- Teachers will monitor any mail sent by children in their class to ensure that the email is

being used responsibly.

- Pupils must immediately tell a teacher if they receive offensive e-mail.
- If pupils' accounts have been set up to allow them to communicate with email addresses outside their own class community, they must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.
- Access in school to pupils' external personal e-mail accounts is not allowed.
- E-mail sent 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 letters is not permitted.

3.3. Published content - website

- We use our school website as well as a variety of social networks to celebrate pupils work and achievements, promote the school, post news of events and publish resources for projects.
- Social networks may be either public (such as Twitter, Facebook) or closed (such as ParentMail).
- In all cases access to publishing rights will be strictly controlled by the IT lead. Although the IT lead and Headteacher will take overall editorial responsibility for ensuring that content is accurate and appropriate, staff given permission to publish on the website or social networks should follow the school's guidelines for publication.
- The point of contact on the Web site is the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

3.4. Publishing pupils' images/videos

- Photographs published online that include pupils will be selected carefully to portray them in a positive light and will not enable individual pupils to be clearly linked with their full name.
- Written permission from parents or carers will be obtained before photos/videos of pupils are published electronically. This is done via a one-time form which parents sign when they arrive at the school. Please see our Use of Images Consent Form.

3.5. Use of newsgroups / Chatrooms

- Children are not normally permitted to access newsgroups or chat rooms except where the class teacher deems it educationally valuable, in which case all access will be carefully monitored.

3.6. Use of social media

- Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content.
- 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.

- 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.
- No member of staff should use social networking sites or personal publishing sites to communicate with students, past or present.
- 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, chatrooms, instant messenger and many others.
- Teachers should consider carefully any references to their working lives on any social media to ensure that they uphold the highest professional standards and that their private interests do not conflict with their public duty.
- The school will control access to social media and social networking sites.
- 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 are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- 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.
- Staff are advised not to run social network spaces for pupil use on a personal basis.

4. Managing hardware technology

4.1. Emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

4.2. Portable electronic devices

4.2.1. School devices

Use of school iPads and other mobile devices are managed in a similar way to fixed assets – i.e. all content will be overseen by the school leadership, IT lead and technical support provider and pupil use will always be supervised by an adult.

4.2.2. Personal devices

- Mobile phones for pupils are not permitted in school, unless a letter is sent by parents giving permission and it has been approved by the Headteacher.
- Pupils are not permitted to bring in other personal portable electronic devices.
- Children who have received approval to bring in their mobile phone must switch it off and hand it in to the office at the start of the school day.
- The school will make every effort to keep handed-in mobile phones safe but will not accept any liability in the event of loss or damage.

- Staff should follow the guidelines in the staff handbook for the use of personal portable devices. Personal phones are not to be used to take photos of pupils.

5. Staff responsibilities

5.1. Access

All computer users are permitted access only to those parts of the computer system which they need to enter in order to carry out their normal duties. Any other access will be regarded as unauthorised.

Should a computer user believe that they need to gain access to other parts of the computer system, they must first seek clearance from the System Manager.

5.2. Security

- All PC software that is purchased, installed and supported by our IT network support provider can be assumed to be free of viruses. However, software introduced via a route other than the IT network support provider will not necessarily be free of viruses.
- Staff have a responsibility to contact technical support or IT Lead as soon as possible if they believe the virus checking package on any device is not up to date or if they think a device has a virus.
- Staff should never
    - make copies of school software. Copying commercial software for use on more than one machine is illegal.
    - install copies of software from others unless you have permission. If you have a legitimate need for the software you are being offered, then arrange for the school to either purchase it for you, or to check it thoroughly BEFORE it is loaded onto our systems.

5.3. E-mail

5.3.1. Language

All communications by e-mail (both external and internal) are to be treated as if they are permanent written communications and appropriate language and style should therefore be used at all times.

5.3.2. Private use of e-mail

Whilst it is accepted that computer users may send and receive limited personal communications by e-mail, these should be minimal and the privilege not abused just as in the case of personal telephone calls. All computer users must ensure that any private use does not occur during the performance of their duties.

5.3.3. Unacceptable use of e-mail

There are certain types of communication which could give rise to liability both for yourself and potentially for us. For this reason, staff should not send internally or externally or (where preventable) receive any personal or business e-mail which:

- contains pornographic, obscene, defamatory, discriminatory or insulting material, whether or not you are offended personally by it;

- contains information that is confidential, or may have contractual or other legal implications for us, except as part of your duties;
- may damage our reputation or that of any person or organisation with which we deal;
- includes derogatory remarks about other people or organisation (even if only sent internally);
- makes representations or expresses opinions purporting to be ours. except where authorised;
- may constitute sexual, racial or other harassment.

Computer users are expressly warned that e-mail messages can be recreated even after deletion and may be used in legal proceedings.

5.4. Internet access

5.4.1. Personal use

As in the case of e-mail, the school recognises that employees will have a legitimate need to access the Internet and also that a reasonable amount of access for personal purposes is acceptable.

Internet use for personal banking, ordering goods, searching for information outside of the scope of work is allowed provided it is reasonable and does not infringe on the performance of your duties.

5.4.2. Professional use

Internet use to support activity connected with our ongoing operation, including communication, research, administration and the development of professional knowledge is non-restricted except in so much as certain sites may be blocked by our firewall.

5.4.3. Inappropriate sites

Use of the school internet facilities to access, view, download, print or distribute pornographic, indecent, sexually explicit or obscene material or material likely to cause offence, whether or not this would constitute a criminal offence and irrespective of whether you do so during working hours or whether you personally find such material insulting or distasteful is also prohibited.

You may inadvertently access inappropriate material because of misleading site descriptions or innocent searches. If this should happen you should exit the site immediately and report to the Headteacher or, in their absence, the most senior staff member. Failure to do so with due speed may result in management concluding that you deliberately viewed the material.

5.5. Monitoring of Internet and E-mail Use

5.5.1. Internet use

All internet usage is logged automatically for security purposes. The source and destination of connection, time and number of bytes transferred are all logged.

5.5.2. Email use

A list of mail coming in and going out (including sender, recipient, time and subject) can be viewed by senior management, via the Adept/LGFL support site, at all times.

5.5.3. Monitoring

The school may also monitor staff e-mails and internet usage:

- where the title of e-mail arriving on our server or the content of or attachment to a mail checked by an IT technician or IT lead alerts them to a breach of this policy or other inappropriate behaviour and they notify an appropriate senior manager accordingly;
- where a breach of this policy, a breach of another policy, or other inappropriate behaviour is suspected;
- to check for viruses;
- if a member of staff is absent and e-mails need to be checked for work-related reasons.

In most cases the IT lead or senior management will specifically warn staff before introducing continuous monitoring of their internet usage or e-mails. However, in limited circumstances (for example - where warning staff in this way would prejudice an investigation) the school may monitor without giving specific warning of this first.

Monitoring and checking of internet usage and e-mail will be conducted only by an appropriate senior manager.

All computer users should note that marking e-mails as 'personal' does not mean that management will not in some circumstances see their content or attachments. If staff do not wish senior management to read private e-mails they should make alternative arrangements that do not involve school property (for example, text messaging or web based email).

Senior management may override any passwords or require computer users to disclose any passwords in order to facilitate access to any e-mail message for a reason set out above.

5.6. Consequences of breach of this policy

Failure to comply with any aspect of this policy without good reason could result in the removal of privileges to use the computer system for personal purposes and/or, in the case of employees, in disciplinary action being taken, and in the case of non-employees (such as volunteers and student teachers), termination of the relationship and/or legal action.

5.6.1. Misconduct

The following will be regarded as gross misconduct;

- Serious breach of the school virus policy;
- sending an e-mail which may materially damage the school's reputation or that of one of any person or organisation with which we deal;
- sending an email which constitutes sexual, racial or other harassment;

- deliberately using school internet facilities to access, view, download, print or distribute pornographic, indecent, sexually explicit or obscene material or material likely to cause offence.

Computer users are specifically warned that there are a number of criminal offences that may arise from the misuse of our computer systems and that the school reserves the right to inform the police if we believe that such an offence may have been committed.

5.7. Data protection

5.7.1. Guidance on handling personal data in the computer system

We all need to be mindful of our legal obligations when creating, storing or circulating information about individuals. Information relating to any identifiable individual which is created on our computer systems (e.g. a word document or e-mail) counts as "personal data" for the purposes of the Data Protection Act 1998.

Once we hold personal data about an individual we have obligations relating to that data. We must ensure that the data is accurate, not excessive or irrelevant and we can "process" the data only if strict conditions are satisfied. In brief, most data can be processed for legitimate reasons but sensitive information {e.g. about an individual's health) cannot usually be processed without specific consent. Circulating, retaining and even deleting information counts as processing.

See our Data Protection policy for more information

5.7.2. Right to access personal data

Individuals have a right to see personal data that is held about them on our computer system. We may also have to disclose documents, including e-mails in the context of legal proceedings (whether or not they count as personal data.).

5.7.3. Guidance on handling personal data in the computer system

Against this background here is some practical guidance on handling information about individuals held on computer:

- Beware what you say in e-mail messages. If sending an e-mail about an individual, remember that this is likely to be processing personal data. This means that the individual may seek access to it and we have data protection obligations in respect of it.
- Consider whether a telephone call would be a more appropriate means of communicating the information.
- Never ask for or send information about someone's health or other sensitive details unless they have specifically agreed to this or you know that you are acting within the limits of the Data Protection Act.
- Remember that describing an individual by their initials ("ABC") or indirectly ("you know who..') will often still count as processing data about the individual.
- Be careful about creating documents containing opinions about an individual. Personal data includes opinions about individuals, not just facts.
- Never make "throw-away" remarks about individuals in e-mails, assuming that they won't see them. Subject access requests are becoming more common and this sort of

remark can lead to legal liability. Remember that e-mails are not a secure method of communication and can be forwarded very easily to individuals other than the intended recipients both deliberately and by mistake.

6. Managing risk & concerns

6.1. Internet access authorisation

- Authorisation is as individuals and usage is fully supervised. Normally all pupils will be granted Internet access.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign an acceptable use form for their child and grant permission for them to access the internet, which lasts the duration of their child's education at the school (see Appendix A)
- The school will keep a record of all pupils who are granted Internet access or if a pupil's access is withdrawn.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials, usually within closed systems such as Espresso.

6.2. How will the risks be assessed?

- Methods to identify, assess and minimise risks will be reviewed regularly.
- Governors will ensure that the E-safety policy is implemented and compliance with the policy monitored.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the IT lead.

6.3. Reporting unsuitable content

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider (currently LGfL) via the IT lead and/or our IT Technical service provider (currently Adept: Rajib Ahmed <rajib.ahmed@adept.co.uk>)
- Training should be available to staff in the evaluation of Web materials and methods of developing students' critical attitudes.

6.4. Complaints

- Complaints of Internet misuse will be dealt with under the School's Complaints Procedure.
- Any complaint about staff misuse must be referred to the Head teacher; if the complaint is about the Head teacher this should be reported to the Chair of Governors.
- All e–Safety complaints and incidents will be recorded by the school — including any actions taken.
- Pupils and parents will be informed of the complaints procedure. Parents and pupils should work in partnership with staff to resolve issues.

7. Communication of the policy

7.1. How will the policy be introduced to pupils?

- Rules for Internet access will be posted in all rooms where computers are used.
- Pupils will be informed that Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.
- The first lesson of every half term will be on E-Safety, including responsible Internet use covering both school and home use.

7.2. How will staff be consulted/trained?

- All staff must accept the terms of the 'Responsible Internet Use' statement (see Appendix 3) before using any Internet resource in school.
- All staff will be provided with a copy of this policy, and its importance and the requirement to read and abide by the terms explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by SLT.
- Staff development in safe and responsible Internet use, and on the school Internet policy will be provided as required.

7.3. How will parents' support be enlisted?

- Parents' attention will be drawn to the School E-safety Policy in newsletters and on the website.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organisations such as PIN, Parents Online and NCH Action for Children (URLs in reference section).

8. E-safety

8.1. Cyberbullying

Cyberbullying is defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007.

It is essential that pupils, staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse.

Promoting a culture of confident users will support innovation and safety. DfE and Childnet have produced resources and guidance that will be used to give practical advice and guidance on cyberbullying

Cyberbullying (along with all forms of bullying) will not be tolerated in school. As for bullying generally, procedures in place to investigate incidents or allegations of bullying and all incidents of cyberbullying reported to the school will be recorded.

Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

The school will take steps to identify bullying behaviour, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

8.2. Sexting

Children in Year 5 and 6 will be informed about the implications of sexting and how, once a picture has been sent, this image can never fully be removed from the world wide web.

8.3. Pornography

Many children will come across some type of pornographic content when searching the Internet. Children are taught about what to do if they come across this type of material and who to speak to.

8.4. Consequences

Any concerns with content may be recorded and dealt with in the following ways:

a) The user will be asked to remove any material deemed to be inappropriate or offensive.

b) The material will be removed by the site administrator if the user does not comply.

c) Access to the LP for the user may be suspended.

d) The user will need to discuss the issues with a member of SLT before reinstatement.

e) A pupil's parent/carer may be informed.

For more serious cases, pupils posting inappropriate material may be dealt with according to our Behaviour policy.

APPENDIX 1: SOHO PARISH PRIMARY SCHOOL
INTERNET USE & PG FILM CONSENT FORM

Full name of child (in BLOCK CAPITALS):	

INTERNET ACCESS - ACCEPTABLE USE AGREEMENT

As part of the school's curriculum we offer pupils supervised access to the Internet.

In order to reduce the risk of accidentally accessing inappropriate material, the school employs a service provider that prevents access to listed undesirable sites and has a stringent fire-wall; however, no system is fool proof.

We require your written permission for your child to have access to the Internet.

I understand that my child will use the Internet at school. I understand that the school will take all reasonable precautions to ensure that my child does not gain access to inappropriate material. I understand that pupils will be held accountable for their own actions.

Parent's or guardian's signature: _____ Date: _____

WATCHING PG FILMS & VIDEO CLIPS

We like to make use of modern technologies throughout the curriculum and sometimes take the opportunity to use feature films and associated resources for education or enrichment activities.

There are occasions when the materials have been classified PG which stands for Parental Guidance. This means a film is suitable for general viewing, but some scenes may be unsuitable for younger children. A PG film should not disturb a child aged around eight or older.

We will always assess whether or not we feel a film / clip is suitable for the class prior to showing it. We ask for your permission to use PGfilms that we deem to be acceptable for the age, maturity and well-being of your child.

I give permission for my child to watch films and clips that have a PG classification.

Parent's or guardian's signature: _____ Date: _____

APPENDIX 2: Responsible Use of the Internet and E-mail Agreement - PUPIL

The school has installed computers with Internet and email access to help our learning. These rules will keep us safe and help us be fair to others.

• I will not change or create any passwords or login procedures on the computers

• I will not interfere with or knowingly change any settings in the computer

• I will not install or delete any software on the school's computers

• I will not bring in memory storage devices such as hard/flash drives/USB sticks etc. from outside school unless I have been given permission

• I will not access or change other people's work files

• I will only use the computers for school work and homework, unless given permission

• I will ask permission from a member of staff before using the Internet and email. I know that I should not use the internet or be in a room without a staff member present

• I will only use my school e-mail address in school

• I will only email people my teacher has approved. The messages I send will be polite and responsible

• I will never give my home address, telephone number or photograph or arrange to meet someone I have contacted on the Internet or by e-mail

• I will report to an adult any unpleasant material or messages sent to me or that I see while using a search engine

• I understand that the school may check my computer files and may look at the Internet sites I visit

• I understand that if I do not follow these rules I will not be allowed to use the Internet and email or any of the school's computers

• I will follow the school rules when using the internet and treat others with the same respect I afford them in person. I will not use my mobile phone or the internet to send unkind messages or to make somebody else feel threatened, sad or bullied.

• I understand that it is against the rules of social networking sites for children under 13 to become a member, so I will not join Facebook, Twitter or any other similar site.

Pupil name..... Signed..... Date .....

APPENDIX 3 – Responsible Use of the Internet and E-mail Agreement - STAFF

All Staff, Governors and visitors understand that ICT includes a wide range of systems, including mobile phones, digital cameras, laptops and tablets.

- All staff, Governors and visitors understand that it is a disciplinary offence to use the school IT equipment for any purpose not permitted by its owner.
- No staff, Governors or visitors will disclose any passwords provided to them by the school.
- All staff, Governors and visitors understand that they are responsible for all activity carried out under their username.
- Staff, Governors and visitors will not install any hardware or software on any school owned device without the Head's permission.
- All staff, Governors and visitors understand that their use of the internet may be monitored and if anything untoward is uncovered, could be logged and used in line with any disciplinary procedures. This includes all school owned devices. If an E-safety incident should occur, staff will report it to the Senior or Deputy Designated Safeguarding lead as soon as possible.
- All staff, Governors and visitors will only use the school's email / internet /intranet etc and any related technologies for uses permitted by the Head or Governing Body. If anyone is unsure about an intended use, they should speak to the Head beforehand.
- All staff, Governors and visitors will ensure that data is kept secure and is used appropriately as authorised by the Head or Governing Body. No passwords should be divulged and memory sticks should also be encrypted.
- Personal devices must only be used in the context of school business with the explicit permission of the Head. Personal mobile phones or digital cameras must NEVER be used for taking any photographs related to school business.
- Each class has a digital camera specifically for this purpose. These school cameras must NEVER be used for personal use.
- All staff, Governors and visitors using school equipment will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- All staff, Governors and visitors will only use the approved email system for school business.
- Images will only be taken, stored and used for purposes within school unless there is parental permission for alternative use. At the start of each year, our parents are asked to sign if they agree to their children's images being used in our brochure or in the local press. If a parent does not agree to this, we ensure that their child's photograph is not used.

  Filming and photography by parents and the wider community at school events, such as sports days and school productions, <u>are</u> allowed.
- All staff, Governors and visitors will make every effort to comply with copyright and intellectual property rights.
- All staff, Governors and visitors will report any incidents of concern regarding staff use of technology and/or children's safety to the Designated Safeguarding lead in line with our school's Safeguarding Policy.