Head teacher	Mrs D Scott
Date	drafted Nov 2021
Chair of Governors	Mrs S Harrison
Person responsible	R. Howard acting ICT Lead
Next review date	TBA - 1 year after ratification

Simonside Primary School

Acceptable use policy

INTRODUCTION

Digital technology has become integral to the lives of children and young people in today's society, both within and outside of school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone; these technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put people at increased risk, and it is the responsibility of all members of Simonside Primary School's community to adhere to our robust policies to safeguard everyone when using digital technologies.

This agreement has been written to adhere to the guidance outlined in the following documents:

- Keeping Children Safe in Education (2021)
- Teaching online safety in school (2019b)
- Working together to safeguard children (2018).
- Cyberbullying: Advice for headteachers and school staff (2014)
- Children Act (1989)
- Children Act (2004)
- Communications Act (2003)
- Computer Misuse Act (1990)
- Criminal Justice and Courts Act (2015)
- Data Protection Act (1998)
- Data Protection Act (2018)
- Education Act (2011)
- Education and Inspections Act (2006)
- Freedom of Information Act (2000)
- Malicious Communications Act (1988)
- Serious Crime Act (2015)
- Voyeurism (Offences) Act (2019)

This agreement should be read in conjunction with the following school policies / documents:

- Online Safety Policy
- Remote Learning Policy
- Behaviour Policy
- Child Protection / Safeguarding Policy
- Allegation Management / Whistleblowing Policy
- Anti-bullying Policy
- Staff Code of Conduct
- Complaints Procedure
- GDPR Policy
- SEND Policy

DRAFT

INFORMATION SYSTEMS SECURITY, FILTERING & MONITORING

- School security systems for digital technology will be reviewed regularly, in conjunction with OpenZone (Local Authority support for IT services)
- The Computing Subject Leader will ensure that the school community is updated regularly with online safety issues and guidance, in collaboration with the LA, BECTA and Child Protection authorities
- Security of digital technology devices will be discussed with the Local Authority and adapted following advice given
- Virus protection will be updated regularly by the Local Authority ICT in Schools Service
- The school will work in partnership with South Tyneside LA, the NGfL and BECTA, to ensure that filtering systems are as effective as possible
- Senior staff will ensure that regular checks of online safety incidents and their frequency are carried out, accurately recorded, and that actions are taken as a result
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Computing Subject Lead (or DSL in their absence), who will - in turn - report it to the Head Teacher; the actions taken will depend on the incident, and will follow a discussion between the Computing Subject Leader and the Head Teacher
  - All users must observe password protocols for network and internet access ● Device screens should be sited so they can be monitored by the teaching and support staff, and Apple Classroom utilised to further enhance monitoring within the classroom (particularly where social distancing should be maintained) ● The school, under the authority and guidance of the Head Teacher, maintains the right to regularly monitor internet traffic, and the school's network and user email through the use of 'e-safe' software. We are obliged to monitor this to fulfil our responsibilities with regard to UK law; monitoring of internet access and email is provided by the LA internet provider.

MANAGING APPROVED EMAIL ACCOUNTS

- All users who log on to the learning platform and school email system at home or at any other location, must only use these systems for educational use, and are bound by the acceptable use guidelines
  - Emails sent to an external organisation should be written carefully, and authorised before sending, in the same way as a letter sent on school headed paper
  - No users should ever use the school's communication systems to access or send inappropriate materials such as pornographic, racist or offensive material, or to send or forward anonymous messages and chain letters
- Users should not access personal, public chat rooms and messaging systems (e.g. Messenger, Facebook, twitter etc.)
- Users should not use the school's communication technologies for personal financial gain, gambling, political purposes or advertising
- Pupils are advised when using personal email systems to never disclose personal details such as name, address, age or telephone number
- Whole class or group email addresses should be used at Key Stage 1 or below, when available (email software may be used if deemed suitable by the Computing Subject Leader or Head Teacher)

- Individual pupil accounts may be given once Key Stage 2 pupils have gained the knowledge and understanding about security implications. It is the duty of teaching staff to ensure children understand security implications and are made aware of the Acceptable Use Policy

DRAFT

- Any inappropriate communications received must be reported to a member of staff immediately
- Staff concerns about emails sent to their own, or children's accounts, should report these to the Computing Subject Leader or Head Teacher
- All staff are aware of their responsibilities regarding online safety and internet use; they should refer to these as part of their teaching of the curriculum

LOGINS AND EMAILS

● All staff will be given a login for the school server on joining the school ● Email accounts will be given to staff and children in KS2 (email accounts *may* be issued to KS1 children if deemed appropriate by the Head Teacher) ● On leaving the school, staff and children's accounts will be deactivated; this is the responsibility of the ICT in Schools service

ACCESSING INTERNET SITES

- Users should not visit sites that contain illegal, obscene, hateful or other objectionable material
- Users should use the school's internet for professional/educational purposes only and not for personal reasons, without the permission of the Computing Subject Leader or Head Teacher
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials
- At Key Stage 2, pupils will be allowed to search the web, as long as they have specific teaching on how to search the internet in a safe manner
- Children must report anything inappropriate they find to their teacher, who in turn, must direct this to the Computing Subject Leader
- Teaching staff should always research potential sites before directing pupils to them

● Teaching staff must be aware of any issues there may be when asking the children to search the web, and ensure every step has been taken to avoid this ● Staff will always use a child-friendly, safe search engine when accessing the web with pupils

SCHOOL WEBSITE

The school website includes the following protocols:

- Staff and pupil contact information will not be published; The contact information give will be that of the school office
- The Head Teacher and Computing Subject Leader will take overall editorial responsibility to ensure that content is accurate and appropriate
- Photographs that include pupils will be carefully selected so that individuals cannot be identified or their image misused
- Pupils' names will not be used
- The permission of parents will be sought before photographs or work is published on the school website

MANAGING VIDEO CONFERENCING AND WEBCAM USE

- Videoconferencing should use the educational broadband network to ensure quality of service and security

DRAFT

- Pupils must ask permission from the supervising teacher before making or answering a video conference call
- Videoconferencing and webcam use will always be supervised by adults ● Webcams/devices with this feature, should be checked and monitored to ensure that misuse does not occur accidentally or otherwise

SOCIAL NETWORKING, INSTANT MESSAGING AND PERSONAL PUBLISHING

The term 'social networking' refers to online communities where typically text, photos, music, video are shared by users. Instant messaging refers to online chatting to others in 'real time'.

- ● The school will not allow pupils access to social networking and instant messaging sites, whilst using a school device / on school premises
- ● Staff will be allowed to access Twitter for professional use only, using their personal, professional account (this means an account set up for the sole purpose of sharing education-related content)
- No pupil names will be used alongside any images
- Staff must not use school social media for any personal discussions or for any individual personal matters, even if initiated by other members of the school community. Users must be directed to more appropriate communication channels
- Staff must be particularly careful to not reveal any details of staff, pupils, parents or other members of the school community that make it possible to identify any individuals
- Staff must use appropriate behaviour and language at all times. As a guide, this should be similar to that which would be used when taking part in a face-to-face meeting with other education professionals
- The school does accept that there can be educational benefits to the use of social media (e.g. collaborative work on a national and international scale) and will, therefore, examine their use for teaching and learning, as the need arises ● The school will consider how to educate pupils in the safe use of social media:

- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location
- Pupils will be advised that the use of social network spaces outside of school brings a range of dangers, particularly for primary-aged pupils o Pupils will be advised to use nicknames and avatars when using social networking sites
- Pupils will be encouraged to carefully consider who they are 'friends' with online, with the emphasis being on only having friends you know in a 'real world context'

- Outside of school, we encourage appropriate use of social media by staff and parents. We encourage staff to use social media for the range of CPD opportunities available, however, it is vital that staff follow clear guidelines for safeguarding purposes:

- It is recommended that all staff regularly check the security settings on any social media accounts, and ensure these are set to the highest possible level ● The personal use of social media must neither interfere with a member of staff's ability to maintain their professional reputation nor impact on the reputation of the school
- Staff must take all reasonable steps to ensure the proper separation of their professional and personal lives

DRAFT

- Staff must not use school social networking accounts for personal content ● Staff must respect the wishes and privacy of any other members of their school community with whom they have personal social media contact
- Staff must not use personal social media with any child with whom they solely have, or have had, a staff/pupil relationship. This includes ex-pupils, until they reach the age of 18
- School staff can have social media contact with pupils or ex-pupils where other appropriate relationships exist. For example, a pupil who is also a family member or a family friend. These relationships must be open and transparent. The member of staff can report these social media relationships to senior leaders for their own protection
- Staff must retain any communications to pupils or ex-pupils rejecting any approaches made on social media, and ensure that they are professional in tone (it is recommended that individuals are 'blocked' from making future contact with members of staff). Staff should also consider reporting these to senior leaders to ensure transparency
- Staff must not use personal social media with anyone with whom they solely have a staff/parent relationship
- Staff at schools can often have more complex relationships than just being a member of staff or a parent. For example, staff can also be parents (of pupils at the school), in relationships or have friendships with other staff or parents; or also governors. Any member of staff can report any social media relationships to senior leaders for their own protection
- Staff must make sure that their personal social media activities take into account who they have social media relationships with – particularly any other members of the school community – and moderate their social media behaviour accordingly

SEESAW

The use of Seesaw is to allow for easier - and paperless - communication of school messages between staff and parents. Seesaw allows for children's work to be shared with parents, through posting and linking it to their account.

- All teachers must ensure that the access QR codes are given directly - and securely - to parents/carers; once these have been shared, the security of the QR code becomes the responsibility of the parent/carer

- Teachers will ensure that pieces of work are linked to that correct child's account, and will ensure that other children's work remains private to the child, parent and teacher, except in the circumstances of collaborative work.

- Teachers must ensure that any children that do not have permission for photographs to be shared, do not appear in pictures for any collaborative work on Seesaw, or their faces must be covered in the picture and this post should NOT be linked to that child's account
- When using Seesaw, teachers must ensure that the children are logging into their own accounts and are not acting as another child whilst on the app. Teachers must also disable the option for children to be able to comment on each other's work
- When teachers are using Seesaw to communicate with parents, they must ensure they remain professional at all times, and report any concerns they have about the appropriateness of parental comments or messages to the Head Teacher

DRAFT

COPYRIGHT AND PLAGIARISM

- The school will ensure that copyright and intellectual property right laws are not infringed
- Pupils will be taught to reference all material used from the internet and other sources, as they develop their research skills

MANAGING EMERGING TECHNOLOGIES

The technology available to schools is constantly evolving and the range of data and ICT services and products ever increasing. The school will therefore:

- Examine emerging technologies for educational benefit, and a risk assessment will be carried out before use in school is allowed
- 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; children are not permitted to use their mobile phones in school (*please refer to the 'Mobile Phones' information in this policy)*

MOBILE DEVICES:
TAKING DIGITAL IMAGES

It is recognised that the taking of digital images is an integral part of teaching and learning, but there must be a clear, educational reason for creating, storing, distributing and/or manipulating images of members of the school community.

- Staff and pupils may take digital photographs or videos using school equipment, providing that they support educational activities; it is best practice for staff and children to ask permission before taking photographs of an individual
- Staff must not take any pictures of pupils using personal equipment of any kind; school equipment must always be used
- Images/video should not be taken with personal mobile phone cameras (e.g. whilst on school visits)
- All images of children should be saved in the 'Photographs' folder on the shared drive, as soon as possible after being taken; photographs of children should not be stored in staff's personal areas of the drive, and should be deleted from devices as soon as they have been saved to the shared drive
- All images of children should be deleted from devices (including those used by staff) at the end of the academic year

- Pupils will be taught how images can be misused, as part of the online safety curriculum

MOBILE PHONES

- Pupils should not bring mobile phones into school, however, if deemed necessary by the parent, the phone must be handed to the teacher immediately; these will be stored until the end of the school day
- Pupils will be advised that the sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden
- Personal mobile phones of all staff should be left on silent or switched off during working hours (during direct contact time), unless expecting an emergency call regarding private welfare matters

DRAFT

- Staff are advised to avoid social media, gaming and gambling during working hours

PORTABLE STORAGE DEVICES

- The use of portable storage devices is discouraged; only those which are encrypted and password protected are permitted for use in school.

- All users should ensure that data stored on portable storage devices has been downloaded using anti-virus software
- All users are responsible for the security of mobile storage devices. Images of children should not be stored on portable storage devices. Pupils are not allowed to use their own portable storage devices.

DVD / FILMS

We recognise that the use of film can be of educational benefit to children, and can enhance their learning experience. Where film is used, this should be age appropriate, as outlined by the film classification authority. Permission from parents/carers should always be obtained if the film certificate is rated PG.

HANDLING OF ONLINE SAFETY ISSUES

In the handling of incidents, this policy should be used alongside other applicable policies such as our: Online Safety Policy, Remote Learning Policy, Behaviour Policy, and Safeguarding Policy. All issues surrounding online safety must be reported following these procedures:

Reporting Accidental Access to Inappropriate Material

Any user of the school and/or other networks who accidentally comes across inappropriate or offensive material should do the following:

1. Inform the school's Computing Subject Leader of the incident and give the website address.

2. Ask the Computing Subject Leader to log the web address, time, user & device.
3. The school's Computing Subject Leader should contact ICT in Schools Service immediately, and report the web address, asking for an investigation as to whether the website should be permanently blocked (under no circumstances should the Subject Leader or reporting staff member log onto this website to research the issue themselves).
4. If ICT in Schools decide that the website is not sufficiently inappropriate for permanent blocking, the school should ensure it is blocked via its own CachePilot or other proxy server

Reporting Accidental Access to Illegal Material

Any user who accidentally comes across illegal material should do the following:

1. Report the incident to the Computing Subject Leader / Head Teacher immediately
2. Do not show anyone the content or make public the URL

DRAFT

3. Ensure a record of the incident is made
4. Go to the IWF website at www.iwf.gov.uk and click the report button.
5. If reporting a URL, do not use copy and paste - type the URL

Reporting Suspected Deliberate Abuse or Misuse

Any person suspecting another of deliberate misuse or abuse of the network should take the following action:

1. Report in confidence to the Computing Subject Leader / Head Teacher.

2. The Head Teacher should inform the Local Authority
3. The Local Authority should complete an internal RIPA form, requiring Northern Grid to complete an internal investigation.
4. If this investigation results in confirmation of access to illegal materials, or the committing of illegal acts, Northern Grid will inform the relevant police authority who will complete their own investigations.
5. If the investigation confirms that inappropriate behaviour has occurred, Northern Grid will inform the relevant authority; this may be the Local Authority or the School's Board of Governors.
6. In exceptional circumstances, where there are reasonable grounds to suspect that a user has committed a serious criminal offence, the police will be informed and a criminal prosecution may follow.

Communicating this policy

- All staff will receive online safety training at least annually
- All staff will ensure that online safety teaching remains an integral part of their teaching throughout the year
- All staff will sign the acceptable use policy at the beginning of each year
- All staff will follow the reporting procedures as outlined in the policy and report any concerns to the Computing Subject Leader
- All children will be made aware of the monitoring systems we use in school to ensure that they are using technology correctly in school

DRAFT

SIMONSIDE PRIMARY SCHOOL

Acceptable & Responsible Use Agreement

STAFF

I hereby confirm that I have read and understood the following school policies: Acceptable & responsible Use Policy, E Safety Policy, and Remote Learning Policy, and will use all means of electronic communication equipment provided to me by the school, and any personal devices which I use for school activity, in accordance with this documentation. In particular:

- I will only use the school's email and internet for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body, and not as a personal email account
- I will only use the approved, secure email system(s) for any school business
- If I use any form of electronic communication for contacting pupils or parents, I will use the school's systems, never a personal account
- I will not browse, download or send material that could be considered offensive
- I will report any accidental access to material which might be considered unacceptable immediately to my line manager and ensure it is recorded
- I will not download any software or resources from the Internet that can compromise the network, or that is not adequately licensed
- I will ensure all documents are saved, accessed and deleted in accordance with the school's network security and confidentiality protocols
- I will not connect a computer or laptop to the network / Internet that does not have an up-to-date version of anti-virus software
- I will not use personal digital cameras or camera phones for transferring images of pupils or colleagues without permission
- I will ensure I am aware of digital safeguarding issues so they are appropriately embedded in my classroom practice
- I will only allow visitors to access a school's computer/laptop using the school's supply log in details
- I will not access or allow unauthorised individuals to access email / Internet
- I will not use my personal mobile phone during teaching hours, or in front of the children, unless I am awaiting an emergency phone call / message and have permission from the Head Teacher
- I understand that personal use of social media should not be used to discuss children, staff or the daily life of school.
- I will only use my professional twitter account when making posts linked to school, and all tweets regarding school/containing images of children will include the school tag @simonsideschool

DRAFT

- I will take all reasonable steps to ensure the safety and security of school IT equipment which I take off site, and will remove anything of a personal nature before it is returned to school.

- I will follow school policy on compliance with the General Data Protection Regulations (GDPR). In particular:

    - Confidential school information, pupil information or data which I use will be stored on a device which is encrypted or protected with a strong password. Computers will have a password protected screensaver and will be fully logged off or the screen locked before being left unattended

- All device/network passwords will remain confidential and will not be shared with others in school.

- I understand that I have the same obligation to protect school data when working on a computer outside school.

- I will report immediately any accidental loss of personal or sensitive information so that appropriate action can be taken.

- I understand that the school may monitor or check my use of IT equipment and electronic communications.

- I understand that the school has the right to examine or delete any files that may be held on its computer system, to monitor any internet sites visited and emails exchanged and, if necessary to report anything which may constitute a criminal offence.

- I understand that by not following these rules I may be subject to the school's disciplinary procedures.

Name .....

Signed .....

Date .....

DRAFT

SIMONSIDE PRIMARY SCHOOL
Acceptable & Responsible Use Agreement

SUPPLY STAFF & VISITORS

As a visitor to the school, I recognise that it is my responsibility to follow school procedures and that I have a responsibility to ask for advice if I am not sure of a procedure.

I confirm that I will use all electronic communication equipment provided by the school, and any personal devices which I bring into in school, in a responsible manner and in accordance with the following guidelines:

- I will only use the school network for the purpose I have been given access, related to the work I am completing in the school.
- I will not use a personal computer I have brought into school for any activity which might be considered inappropriate in the school.
- I will not use my personal mobile phone or other electronic equipment to photograph or video pupils.
- I will not publish photographs or videos of pupils without the knowledge and agreement of the school or the pupils concerned.
- I will not give my personal contact details such as email address, mobile phone number, or social media details to any pupil or parent in the school; contact will always be through a school approved route.
- I will not arrange to communicate online or use a web camera with pupils unless specific permission is given.
- I will take all reasonable steps to ensure the safety and security of school IT equipment, including ensuring that any personal devices or memory devices I use are fully virus protected and that protection is kept up to date.
- I will only use my personal mobile phone during non-teaching time; it will be kept on silent mode during lessons except in an emergency situation with the agreement of my line manager.
- I will report any accidental access to material which might be considered unacceptable immediately to a senior member of staff and ensure it is recorded.
- If I have access to any confidential school information, pupil information or data it will only be removed from the school site with permission and if so, it will be carried on a device which is encrypted or protected with a strong password.
- I will report immediately any accidental loss of personal or sensitive information to a senior member of staff so that appropriate action can be taken.
- I understand that I have a duty of care to ensure that students in school use all forms of electronic equipment and devices safely and should report any inappropriate usage to a senior member of staff.
- I will not publish or share any information I have obtained whilst working in the school on any personal website, blog, social networking site or through any other means, unless I have permission from the school.
- I understand that the school has the right to examine or delete any files that may be held on its computer system, to monitor any internet sites visited and emails exchanged and, if necessary, to report anything which may constitute a criminal offence.

DRAFT

- I understand that by not following these rules I may be subject to disciplinary procedures

Name .....

Signed .....

Date .....

DRAFT

SIMONSIDE PRIMARY SCHOOL
Acceptable & Responsible Use Agreement

COMMUNITY USERS

As a user of the school's computers and technology, I recognise that it is my responsibility to follow school procedures for the safe use of devices, and that I have a responsibility to ask for advice if I am not sure of a procedure.

I confirm that I will use all means of electronic communication equipment belonging to the school and any personal devices which I bring into school, in a responsible manner and in accordance with the following guidelines:

- I will only use the school computers for purposes related to the work I am completing in the school.
- I will not use a personal device I have brought into school for any activity which might be considered inappropriate in a school.
- I will not use my personal mobile phone or other electronic equipment to photograph or video pupils.
- I will not publish photographs or videos of pupils without the knowledge and agreement of the school and the pupils.
- I will not give any personal contact details such as email address, mobile phone number or social media details to any pupil in the school. I will not arrange to communicate online or use a web camera with pupils unless specific permission is given by the school.
- I will take all reasonable steps to ensure the safety and security of school IT equipment, including ensuring that any personal devices or memory devices are fully virus protected and that protection is kept up to date.
- I will report any accidental access to material which might be considered unacceptable immediately to a senior member of staff and ensure it is recorded.
- I will not publish or share any information I have obtained whilst working in the school on any personal website, blog, social networking site or through any other means, unless I have permission from the school.
- I understand that the school has the right to examine or delete any files that may be held on its computer system, to monitor any websites visited and emails exchanged and, if necessary to report anything which may constitute a criminal offence.
- I understand that by not following these rules, my use of school facilities may be withdrawn

Name ……

Signed ……

Date ……

DRAFT

DRAFT

SIMONSIDE PRIMARY SCHOOL

Acceptable & Responsible Use Agreement

KEY STAGE 1 CHILDREN

- I will look after all the school IT equipment and use it properly
- I will only share my username or password with trusted adults
- I will tell an adult if I see anything which upsets me
- I will always ask before downloading something from the internet, because I understand the risks from virus infections
- Any work I upload to the internet or Seesaw will be my own
- I will only take a photograph or video of someone if they give me permission
- All of the messages I send will be polite
- I will not post anything online which upsets other people
- I will use a safe online name and not give away my personal information or talk to people I do not know using the internet
- I understand that the school may check my use of IT and talk to my parent or carer if they are worried about my online safety
- I understand that if I do not follow these rules, I may not be allowed to use the school equipment or internet for a while (even if my rule break was done outside of school)

Child's name .....

Signed (child) .....

DRAFT

SIMONSIDE PRIMARY SCHOOL

Acceptable & Responsible Use Agreement

KEY STAGE 2 CHILDREN

- I will take care when using the school IT equipment and use it responsibly
- I will keep my passwords private unless I need to share them with a trusted adult.
- I will inform an adult if I see or receive any unpleasant text, images or messages.
- I will not interfere with anyone else's passwords, settings or files on any device.
- I will be careful when downloading material from the internet, because I understand the risks from virus infections.
- Any work I upload to the internet or Seesaw will be my own.
- I know I need permission to take someone's photograph or to video them.
- Any messages I post online or send in an email will be polite and responsible.
- I will not send or forward messages or create material which is deliberately intended to upset other people.
- I know I must take care about giving away my personal information and making contact with people I do not know when using the internet.
- I understand that the school may check my use of IT and contact my parent/carer if they are concerned about my online safety.
- I understand that if I do not follow these rules I may not be allowed to use the school equipment, or access the internet for a period of time, and that this may happen even if my rule break was done outside of school.

Child's name .....

Signed (child) .....

DRAFT