Use of Information Technology

October 2024

Version 1.2

Date of approval: 24.09.24

Date of ratification: 16.10.24

Date of next review: October 2026

1 Introduction

1.1 Information technology has become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work.

1.2 For the purposes of this document, IT includes the use of computers, laptops, tablets, iPads, cameras, mobile phones and any other devices used to access the school networks and the internet, including use of social media.

1.3 This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of Information Technology (IT) at Sonning Common Primary School (SCPS). It also gives guidance for staff when remote working and guidance for remote teaching of students not on school premises.

1.4 This policy also explains use of IT in school to parents, carers, volunteers, contractors and anyone else involved with the school.

1.5 The policy will ensure:

- *All users (staff, parents/carers and pupils) clearly understand the rules for use of IT at Sonning Common Primary School.*
- *Staff will be responsible users of IT for both educational and personal use.*
- *The school IT systems and users will be protected from accidental or deliberate misuse that could put the security of the school network and users at risk.*

1.6 This policy supersedes all previous policies including the staff acceptable use policy agreement, the e-safety policy, social media policies and the mobile phone and camera policy.

2 Scope

2.1 This policy applies to anyone using an IT account belonging to SCPS school, including pupils, permanent and temporary staff, contractors, governors, volunteers and visitors regardless of whether the device they are using belongs to SCPS or not.

2.2 It also applies to anyone using IT equipment belonging to SCPS whether they use it on school premises, at home or elsewhere.

2.3 Before receiving access to school IT resources, adults are expected to read and sign the IT Acceptable Use Agreement (Adults), appended to this document.

2.4 Before receiving access to school IT resources, pupils and/or their parents are expected to read and sign the IT Acceptable Use Agreement (Pupils), also appended to this document.

3 Summary of main points

3.1 This policy contains details of these main points:

- The school computer networks will be used responsibly, legally and for professional purposes only.
- The school IT systems and users will be protected from accidental or deliberate misuse that could put the security of the school network and users at risk.
- Any data that contains pupil identifying information will only be used on school owned, secure encrypted devices (eg laptop, memory stick, external drive, cloud based storage).
- Images of pupils and staff will only be taken, stored and used for professional purposes with the consent of the parent/carer or staff member. Images will not be distributed outside the school network without the permission of the parent. Where these images are published (eg on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- Mobile phone usage **by adults** is not permitted in classrooms when pupils are present, and only permitted in other areas when not on duty at lunchtimes and breaktimes. Only **Y6 pupils** are permitted to bring mobile phones onto school premises, they must be handed in on arrival and their use is not permitted anywhere on school premises. Use of mobile phones is of particular concern as they allow unlimited and unrestricted access to the internet (via 3G, 4G and 5G networks).
- Smart wearable technology is permitted at all times by adults, so long as the device is not used in the way in which a mobile phone is used (calls, emails, photos).
- Users must understand the value of the school's reputation, they must not engage in inappropriate use of the internet, including (but not limited to) social media which may bring themselves, the school and wider school community or their employer into disrepute.
- It is essential children are safeguarded from potentially harmful and inappropriate online material. The school's approach to online safety will protect and educate pupils and staff in their use of technology. The four main areas of risk within online safety are content (being exposed to harmful content), contact (being subjected to harmful interaction with other users), conduct (online behaviour eg images) and commerce (phishing, access to gambling sites etc).
- All use of internet resources are monitored and logged in order to identify, intervene in and escalate any concerns where appropriate.

4 Using and protecting SCPS IT resources

4.1 Everyone using an account that belongs to SCPS should adhere to these guidelines. The SCPS IT resources include the school's IT networks (servers, wifi access points etc) and accounts that are accessed via the internet (for example MS365, BromCom, White Rose, Twinkl etc).

4.2 To keep accounts safe, users should:

- Make sure personal login details do not become known to another person or are in any way compromised.
- Inform the IT technician if equipment has become infected by a virus, malware, spyware or similar.
- Inform their line manager under the Whistle Blowing procedure if you believe that others are using IT systems inappropriately.
- Ensure that personal use of SCPS IT equipment remains occasional and reasonable and does not interfere with everyday workload and commitments or endanger the school's IT services. Use of school equipment by anyone else (family friends etc) is not permitted.

4.3 To safeguard personal information, users should:

- Safeguard personal and confidential data (for example any pupil identifying data) by ensuring it is only stored on encrypted school owned devices or on the school secure cloud storage areas (for example MS365, Google's Workspace for Education drives, BromCom, MAS or any other systems used by the school).
- Ensure that school e-mail accounts are checked on a regular basis.
- Not use a personal e-mail account for any school business, for both safeguarding and GDPR reasons.
- Not install any personal software on a school owned device. Users may install school software on a personally owned device providing it meets the terms of the software licence (eg MS365).

4.4 To use IT in a professional manner, users should

- Not access, copy, remove or otherwise alter any other user's files, without their express permission.
- Only communicate with pupils and parents / carers using official school systems. Any such communication must be professional in tone and manner.
- Not engage in any on-line activity that may compromise their professional responsibilities and/or bring the school name into disrepute.

- Not create, download, upload, display or access knowingly, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene or offensive. Unsuitable material might also include data, images, audio files or video files.

5 Use of images / videos and audio recordings

5.1 Permissions

- Staff are permitted to take photographs, videos and make audio recordings of all children in school to provide evidence of their achievements for development records. Recording is only permitted using school owned equipment. Recordings on personal devices (for example cameras, mobile phones, computers, tablets) is NOT permitted without the prior explicit written consent of the headteacher.
- Parents/carers must give permission for their child's images to be used in any other way, for example on the school website or printed for display in the classroom.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes with the written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent. Where these images are published (eg on the school website) it will not be possible to identify by name, or other personal information, those who are featured.

5.2 Taking images (still photos and videos)

- Images must only be taken using school equipment (camera, iPads etc) and must not be taken using personal devices (eg personal mobile phones). School equipment (including memory cards etc) must not leave the school premises unless being used on an educational visit off site. The use of cameras is not permitted in areas considered most vulnerable, for example changing areas, toilets, swimming pool, unless for a previously agreed use (for example gathering evidence of teeth cleaning).

5.3 Storage of images

- Images should be removed from the camera as soon as is practicable and will be stored on the school network (including cloud based storage). Images may be kept on these school networks until the child leaves the school in which case they will be deleted within one year of the child leaving, unless they are required by statutory purposes.

5.4 Use of images at school events

- School events may be recorded by staff/parents/carers providing all images are taken in full view of those attending. Parents/carers may only post online photographs containing

images of their children (and no others, even if in the background of the image) unless they have obtained prior permission from the headteacher.

6 Mobile phones/smart technology

6.1 Mobile phone usage **by adults** is not permitted in classrooms when pupils are present and is only permitted in other areas when not on duty at lunchtimes and breaktimes. Personal phones must be stored out of sight.

6.2 Smart wearable technology is permitted at all times by adults, so long as the device is not used in the way in which a mobile phone is used (to take calls, emails, photos). Using devices in this way is not permitted in classrooms when pupils are present and is only permitted in other areas when not on duty at lunchtimes and breaktimes

6.3 Mobile phone / smart wearable technology usage **by pupils** is not permitted anywhere in school including in the playground.

6.4 Only Y6 pupils are permitted to come to school with a mobile phone or smart technology device capable of accessing the internet. However devices must not be used on the school premises and must be handed into the class teacher on arrival for safe storage to be returned at the end of the school day. Use of these devices by pupils is of particular concern as they allow unlimited and unrestricted access to the internet (via 3G, 4G and 5G networks).

6.5 Pupils in Kites through to Y5 are **not permitted** to bring mobile phones to school unless they have prior written permission from the headteacher (for example use by diabetic children who use a smart pump connected to their phone to monitor glucose levels.

6.6 Mobile phones with cameras are never permitted in areas considered most vulnerable, for example changing areas, toilets, swimming pool, unless for a previously agreed use (for example gathering evidence of teeth cleaning).

6.7 Staff, visitors, volunteers and pupils are **not permitted** to use their own mobile phones to take or record any images of children within school (or on educational visits out of school) unless there is no alternative and providing it is in full view of all attending and the images are removed as soon as practicable. They should also not be used to contact parents or carers, unless in an emergency.

6.8 Mobile phones can be used in designated areas by adults for specified purposes, for example for lone working protection \ to use multifactor sign on to specific software provided the headteacher has given explicit permission in advance.

7 Use of Social Media

7.1 Staff use within school

- Social media can be used in school to promote the school, for example the school has a Facebook page for promoting events, and to inform parents. Care should be taken to ensure any images used meet the Use of Image conditions in this policy.
- It is acceptable for staff to have closed groups, for example WhatsApp, to facilitate communication between staff members. However this should be limited to social discussions and especially must not be used to discuss any aspect of the children at school.

7.2 Pupil use within school

- Social media should only be accessed by pupils under the direction of a teacher and for a purpose clearly apparent from the learning objectives of the lesson. If social media sites are used staff must carry out a risk assessment before the lesson and ensure the pupils have reached the minimum age for the use of these sites.

7.3 Personal use of social by staff

- Staff should protect the school's reputation by ensuring they use personal accounts appropriately. Teaching staff should abide by the current National Teacher's Standards for social media.
- Staff must not add pupils or ex-pupils under 16 as 'friends' on their personal accounts.
- Staff are **strongly advised** not to add parents as 'friends' into their personal accounts
- Staff must not post comments about the school, pupils, parents or colleagues including members of the Governing Body.
- Staff must not access their personal accounts during lesson times.
- Staff should review and adjust their privacy setting to give them an appropriate level of confidentiality.

7.4 Personal use by parents/carers/governors

- Parents, carers and governors need to be aware of their responsibilities regarding their use of social media relating to school activities and follow this guidance:
    - Do not post images of children other than their own where these images have been taken at a school event.
    - Do not make malicious or fictitious comments about any member of the school community.
    - Use the school complaints procedure rather than posting comments on social media.

- The school's Anti-Bullying Policy sets out the processes and sanctions regarding any type of bullying by a child on the school roll including online bullying and inappropriate use of social media/
- In the case of inappropriate use of social networking by parents, the Governing Body will contact the parent asking them to remove such comments and seek redress through the appropriate channels such as the Complaints Policy
- The Governing Body understands that "there are circumstances in which police involvement is appropriate. These include where postings have a racist element or where violence is threatened or encouraged." Furthermore, laws of defamation and privacy still apply to the web and it is unlawful for statements to be written…which:

    - expose (*an individual*) to hatred, ridicule or contempt
    - cause (*an individual*) to be shunned or avoided
    - lower (*an individual's*) standing in the estimation of right-thinking members of society or
    - disparage (*an individual in their*) business, trade, office or profession.

8 Online safety

8.1 It is essential children are safeguarded from potentially harmful and inappropriate online material. SCPS's approach to online safety will protect and educate pupils and staff in their use of technology. The four main areas of risk within online safety are

- **content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying,
- **commerce:** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

8.2 Teachers will teach online safety to pupils at an appropriate level, as part of Computing / PHSE lessons and as part of other topics in order that pupils can:

- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

- Know and understand policies on the use of mobile devices / smart wearable devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the policy covers their actions out of school, if related to their membership of the school.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the pupils visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the those sites are removed from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/teaching-resources

8.3 All use of internet resources via the SCPS network are filtered, monitored and logged in order to identify, intervene in and escalate any concerns where appropriate. Users are made aware of this in the IT Acceptable Use Agreement – see Appendix 1.

8.4 If devices are lent to pupils for use off site / at home, these will only be SCPS managed devices but these are not subject to school filtering policies and must be managed by parents/carers.

8.5 SCPS will review the online safety risks on an annual basis and make changes as necessary.

8.6 SCPS pupils will be asked to agree to our online safety rules (see Appendix 3)

9 Remote learning

9.1 Where remote learning is needed staff must follow the guidance laid out below. This guidance is to safeguard children, their families and staff. SCPS use Google Workspace for Education for remote learning and we also use a variety of other on-line resources including but not limited to Times Table Rockstars, EdShed Spelling, Oxford Owl (Read, Write Inc) phonics and reading schemes and Nessy.

9.2 Remote contact with pupils, for example via Google Meet or Microsoft Teams, must only happen when the teacher is in school, with at least one other adult in the room. Remote contact should only be made using a SCPS device, e.g. teachers' laptops or school iPads.

9.3 All pupils contacted must have an adult in the room with them for the duration of the session. Pupils must be in a family space, e.g. the dining or sitting room and not in their bedroom. All people involved in the remote contact must be fully dressed, no pyjamas or partial clothing.

9.4 If teachers are delivering a live class:

- It can be recorded so that if any issues were to arise, the video can be reviewed.
- It should be kept to a reasonable length of time
- Language must be professional and appropriate, including any family members in the background.
- Staff must only use platforms provided by SCPS to communicate with pupils.
- Staff should record the length, time, date and attendance of any sessions held.
- GDPR guidelines must be followed at all times, no personal data such as usernames, emails or physical locations must be shared.
- Normal safeguarding rules apply, any concerns must be logged, if a critical concern arises staff must inform the Designated Safeguarding Lead immediately.

10 Dissemination

10.1 The Policy is available on the school web site and a paper copy is available from the school admin office on request.

11 Reviewing the Policy

11.1 This policy will be reviewed every 2 years by the Headteacher and monitored by the Link Governor who will ensure that the Policy is relevant and up to date.

12 Appendix 1 IT Acceptable Use Agreement (Adults)

ICT and the related technologies such as email, the internet and mobile devices are an expected part of daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the ICT coordinator or technician.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- The computers 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 comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will ensure that personal data (such as data held on BromCom) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Data or information relating to individuals in school is not to be stored on personal computers or non-school handheld devices.
- I will not install any hardware or software onto school computers without permission of the ICT-Coordinator or technician.
- I will not browse, download, upload or distribute any material onto school computers that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in-line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use on school computers of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will ensure that my mobile phone is turned off or set to silent when I am in the classroom or in meetings. I will only make personal use of my phone at breaktimes (when not on duty), at lunchtime, before 8:35am or after 3:25pm. The only exception to this being when I am expecting an urgent communication and have discussed this communication, prior to it happening, with the Head Teacher.
- When using any social media websites such as Facebook, Twitter, etc, I will not make any comments that are offensive or derogatory about the school, staff, pupils or parents and I will be careful about any contact made with other staff members or governors. Staff should not make contact with any current pupils on social media websites.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature
I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature ..... Date .....

Full Name..... (printed)

Job title .....

13 Appendix 2 IT Acceptable Use Agreement (Pupils)

Consent

All pupils use information technology including accessing the internet as an essential part of their learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to read the rules and to agreed using MCAS that the attached Online Safety Rules have been understood and agreed.

14 Appendix 3 SCPS online safety rules

Think **before** you click

These rules help us to stay safe on the Internet

I only use the websites my teacher has asked me to use.

I only click on the buttons or links when I know what they do.

I ask before searching the Internet

I always tell an adult if I see anything that makes me feel uncomfortable.

I don't give out personal information or arrange to meet anyone I only know online.

I don't share photos or videos of other people without asking them first.

I don't use any social media (Instagram, TikTok, Twitter, Discord,Whatsapp etc) because I am not old enough.