Online Safety Policy
2025/2026

Date of Approval	Date of Review
September 25	September 26
Status and Review Cycle	Annually

Online Safety Committee

Role	Person(s) Responsible	Responsibility
PSCHE Lead	Lesley Harris	4.2
Designated Safeguarding Lead	Maxine Kurzberg	4.2
Online Safety Lead	Maxine Kurzberg	4.2
Governor Representative (Safeguarding)	Thora Ray	4.1

1. Policy Aims

- This online safety policy has been written by South Camberley Primary and Nursery School with specialist advice and input as required.
- It takes into account the DfE statutory guidance "Keeping Children Safe in Education" 2025 Early Years and Foundation Stage 2024, Working Together to Safeguard Children 2023, Surrey Safeguarding Children Partnership and Online Safety Act 2023 procedures.

- The purpose of South Camberley Primary and Nursery School's online safety policy is to:
    - Safeguard and protect all members of the South Camberley Primary and Nursery School community online.
    - Identify approaches to educate and raise awareness of online safety throughout the community.
    - Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
    - Identify clear procedures to use when responding to online safety concerns.

- South Camberley Primary and Nursery School identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:
    - **Content:** being exposed to illegal, inappropriate or harmful material
    - **Contact:** being subjected to harmful online interaction with other users
    - **Commerce:** online gambling, inappropriate advertising, phishing and or financial scams
    - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

2. Policy Scope

- South Camberley Primary and Nursery School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm online.
- South Camberley Primary and Nursery School identifies that the internet and associated devices, such as computers, tablets, mobile phones, smart watches and games consoles, are an important part of everyday life.
- South Camberley Primary and Nursery School believes that pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as pupils and parents/carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where pupils, staff or other individuals have been provided with school issued devices for use off-site, such as work laptops, tablets or mobile phones.

2.1 Links with other policies and practices

- This policy links with a number of other policies, practices and action plans including:
  - Code of conduct
  - Child Protection & Safeguarding Policy
  - Behaviour policy
  - Curriculum policies, such as: Computing and RHSE
  - Data Protection
  - Searching, screening and confiscation policy (Department for Education)

3. Monitoring and Review

- South Camberley Primary and Nursery School will review this policy at least annually
  - The policy will also be revised following any national or local policy requirements; any child protection concerns or any changes to the technical infrastructure
- To ensure they have oversight of online safety, the Executive Headteacher will be informed of online safety concerns, as appropriate.
- The named Governor for safeguarding will report on a regular basis to the governing body on online safety incidents, including outcomes.
- Any issues identified will be incorporated into the school's action planning.

4. Roles and Responsibilities

- South Camberley Primary and Nursery School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The leadership and management team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including an Acceptable Use Agreement which covers acceptable use of technology. This is included for parents & carers as well as pupils in their induction pack when joining the school.
- Ensure that suitable and appropriate filtering and monitoring systems are in place. This includes our internet filtering system and proxy (Talk Straight in-line proxy) as well as our anti-virus software maintained by Eduthing.
- Ensure that Senso is regularly monitored and any concerns followed up on as necessary.
- Work with technical staff to monitor the safety and security of school systems and networks.
- Ensure that online safety is embedded within a progressive whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.
- Ensure there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology. Audit and evaluate online safety practice to identify strengths and areas for improvement. South Camberley Primary and Nursery School will use 360safe, an online safety practice audit tool provided by South West Grid for Learning (SWGfL) to audit and evaluate practice in this area.
- Support staff and pupils to develop their understanding of AI and Generative AI so that they are able to identify the associated risks and opportunities within the school context in line the DfE guidance on product safety and policy.

4.2 The Online Safety Lead and Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Keep up to date with current research, legislation and trends regarding online safety and communicate this

with the school community, as appropriate.

- Ensure all members of staff receive regular, up-to-date and appropriate online safety training including on the use of AI in line with DfE guidance.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the schools safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the management team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet termly with the governor with a lead responsibility for safeguarding and online safety.

4.3 It is the responsibility of all members of staff to:

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and AUA (Acceptable Use Agreement) .
- Take responsibility for the security of school systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues, including the use of AI, and how they may be experienced by the children in
  their care.
- Identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

4.4 It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures *(including password policies and encryption)* to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised. For South Camberley Primary and Nursery School this is implemented by external contractor, Eduthing.
- Ensure that the schools filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Report any filtering breaches to the DSL and leadership team, as well as the school's Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL, in accordance with the school's safeguarding procedures.

4.5 It is the responsibility of pupils (at a level that is appropriate to their individual age, ability and vulnerabilities) to:

- Engage in age-appropriate online safety education opportunities.
- Contribute to the development of online safety policies.

- Read and adhere to the school's PAUP (Pupil Acceptable Use Agreement).
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

4.6 It is the responsibility of parents and carers to:

- Read the school's AUP and encourage their children to adhere to them.
- Support the school in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the school's home-school agreement and/or PAUA. Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Use school systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

5.1 Education and engagement with pupils

- The school will establish and embed a progressive online safety curriculum throughout the whole school, to raise awareness and promote safe and responsible internet use amongst pupils by:
    - Ensuring education regarding safe and responsible use precedes internet access.
    - Including online safety in the PSHE and Computing programmes of study, covering use both at school and home.
    - Reinforcing online safety messages whenever technology or the internet is in use.
    - Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
    - Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- The school will support pupils to read and understand the AUA (Acceptable Use Agreement) in a way which suits their age and ability by:
    - Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
    - Rewarding positive use of technology by pupils.
      Seeking pupil voice when writing and developing school online safety policies and practices, including curriculum development and implementation.
    - Using support, such as external visitors, where appropriate, to complement and support the schools internal online safety education approaches.

5.1.1 Vulnerable Pupils

- South Camberley Primary and Nursery School is aware that some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- South Camberley Primary and Nursery School will ensure that differentiated and ability appropriate online

safety education, access and support is provided to vulnerable pupils.

- South Camberley Primary and Nursery School will seek input from specialist staff as appropriate.

5.2 Training and engagement with staff

The school will:

- Provide and discuss the online safety policy with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates.
    - These updates will take place in school communications, such as staff meetings/briefings and safeguarding updates.
    - This will cover the potential risks posed to pupils (Content, Contact and Commerce and Conduct) as well as our professional practice expectations.
- Make staff aware that school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices.
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.

5.3 Awareness and engagement with parents and carers

- South Camberley Primary and Nursery School recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies.
- The school will build a partnership approach to online safety with parents and carers by:
    - Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings.
    - Drawing their attention to the school online safety policy and expectations in newsletters, letters, our prospectus, and our website.
    - Requiring them to read the school PAUA and discuss its implications with their children.
    -

6. Safer Use of Technology

6.1 Classroom Use

- South Camberley Primary and Nursery School uses a wide range of technology. This may include but is not limited to:
    - Windows Computers
    - Chrome Books, iPads, Internet
- All school owned devices will be used in accordance with the school's AUA and with appropriate safety and security measures in place.
- Staff must be vigilant when using school-owned devices, that they are kept safe during school trips and on other occasions when they are taken off site, with a focus on preventing their theft.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

- The school will ensure that the use of internet-derived materials, by staff and pupils, complies with copyright law and acknowledge the source of information.
- Supervision of pupils will be appropriate to their age and ability.
    - **Early Years Foundation Stage and Key Stage 1**
        - Pupils' access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the pupils' age and ability.
    - **Key Stage 2**
        - Pupils will use age-appropriate online tools.
        - Children will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils' age and ability.

6.2 Managing Internet Access

- The school will maintain a record of users who are granted access to the school's devices and systems.
- All staff; pupils and visitors will read and sign a AUA before being given access to the school computer system, IT resources or internet.

6.3 Filtering and Monitoring

The following information regarding filtering and monitoring has been taken from the Safer Internet advice website *https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring*

6.3.1 Decision Making

- South Camberley Primary and Nursery School governors and leaders have ensured that the school has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.
- Where filtering has failed, concerns should be raised with the Online Safety Lead.
  Appropriate actions can then be taken to rectify the situation and, if necessary, suggest alterations to the filtering systems.
- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding.
- The school's decision regarding filtering and monitoring has been informed by a risk assessment, taking into account our school's specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team.
  The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

6.3.2 Filtering

- The school uses educational broadband connectivity through Talk Straight. /London Grid for Learning
- The school uses an in-line proxy, provided through Talk Straight/London Grid for Learning, which blocks sites categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
    - The school filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- The school works with Eduthing to ensure that our filtering policy is continually reviewed.
- An additional monitoring system, Senso, uses search terms or visual threats to log concerns and automatically notify senior leaders as necessary.

Dealing with Filtering breaches

- The school has a clear procedure for reporting filtering breaches.

- If pupils discover unsuitable sites, they will be required to turn off monitor/screen immediately and report the concern to a member of staff.
- The member of staff will report the concern (including the URL of the site if possible) to the Designated Safeguarding Lead, Computing lead and/or technical staff.
- The breach will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving their child.

- Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as: Internet Watch Foundation (IWF), Surrey Police or Child Exploitation and online Protection Command (CEOP).

6.3.4 Monitoring

- The school will appropriately monitor internet use on all school owned or provided internet enabled devices. This is achieved by:
  - Requesting a report from Eduthing and monitoring all websites
- The school has a clear procedure for responding to concerns identified via monitoring approaches.
  - Concerns reported to DSL/Leadership team
  - Content blocked
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

6.4 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with the Data Protection Act 1998 and 2018.

6.5 Security and Management of Information Systems

- The school takes appropriate steps to ensure the security of our information systems, including:
  - Virus protection being updated regularly. (Sophos Antivirus)
  - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
  - Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
  - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
  - Regularly checking files held on the school's network,
  - The appropriate use of user logins and passwords to access the school network.
    - Specific user logins and passwords will be enforced for Key Stage 2 pupils.
  - All users are expected to log off or lock their screens/devices if systems are unattended.

6.5.1 Password policy

- All members of staff will have their own unique username and private passwords to access school systems; members of staff are responsible for keeping their password private.
- Pupils are provided with their own unique QR codes and Emoji passwords to access school systems, pupils are responsible for keeping these codes for their own use only.
- We require all staff to:
  - Use strong passwords for access into our system.
  - Always keep their password private; users must not share it with others or leave it where others can find it.
- In the event that a member of staff is concerned that there is a breach of privacy then they report any concerns to the Online Safety Lead.

6.6 Managing the Safety of the School Website

- The school will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE)
- The school will ensure that our website complies with guidelines for publications including accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or pupils' personal information will not be published on our website; the contact details on the website will be the school address, email and telephone number.
- The administrator account for the school website will be secured with an appropriately strong password.
- The school will post appropriate information about safeguarding, including online safety, on the school website for members of the community. Members of the community will be informed as new information is published.

6.7 Publishing Images and Videos Online

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified by their full name.
- Only pupils' first names and first initial of their surname will be used on the website, including in blogs, forums or wikis, particularly in association with photographs.
- Permission will be obtained from parents for pupils' photographs to be published on the school website.

6.8 Managing Email

- Access to school email systems will always take place in accordance with Data Protection legislation and in line with other school policies, including Code of conduct.
    - The forwarding of any chain messages/emails is not permitted. Spam or junk mail will be blocked and reported to the email provider.
    - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
    - School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the school community will immediately tell a Designated Safeguard Officer if they receive offensive communication, and this will be recorded in the school safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted, access to external personal email accounts may be blocked in school.

6.8.1 Staff

- The use of personal email addresses by staff for any official school business is not permitted.
    - All members of staff are provided with a specific school email address, to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff and parents.
- Members of staff have 5 days to respond to any parental enquiries. Staff do not respond directly to parents, agreed communications are sent through the school office email.
  Internal emails between those with an @southcamberley.surrey.sch.uk email address will still be able to be sent and received.
- Management of Applications (apps) used to Record Children's Progress

6.9.1 Arbor

- The school uses Arbor is used to track pupils' progress and share appropriate information with parents and carers.
- In order to safeguard pupils data:

- As Arbor is cloud based, and so accessible from any internet-connected device, where data is downloaded, that it is stored on school-owned devices.
- School devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
- All users will be advised regarding safety measures, such as using strong passwords and logging out of systems. When staff are off site staff they are required to access the school systems using 2 step authentication

6.9.2 Tapestry

- The school uses Tapestry (https://tapestry.info) to track pupils' progress, log observations and share appropriate information with parents and carers.
- In order to safeguard pupils data:

    - Only school issued devices will be used to access Tapestry that records and stores children's personal details, attainment and photographs.
    - Personal staff mobile phones or devices will not be used to access or upload content of any kind to Tapestry
    - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
    - Permission slips are sought for pupils' personal details, including photos or videos of their observations, to be stored within Tapestry. Where permission is not granted, staff will not be able to report to parents and carers through the Tapestry app on their pupils' progress.
    - Further details, specific to the use of Tapestry, can be found in the schools' Tapestry policy.

7. Social Media

7.1 Expectations

- The expectations regarding safe and responsible use of social media applies to all members of the South Camberley Primary and Nursery School community.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of the South Camberley Primary and Nursery School community are expected to engage in social media in a positive, safe and responsible manner, at all times.
    - All members of the South Camberley Primary and Nursery School community are asked not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The school will control pupil and staff access to social media whilst using school provided devices and systems on site.
    - The use of social media during school hours for personal use **is not** permitted on school devices.
    - Inappropriate or excessive use of social media during work hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of the South Camberley Primary and Nursery School community on social media, should be reported to the school and will be managed in accordance with our complaints procedure.

7.2 Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the staff code of conduct.
    - Prior to appointment online searches will be conducted.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within school. Civil, legal or disciplinary action may be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
    - Setting the privacy levels of their personal sites as strictly as they can.
    - Being aware of location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Keeping passwords safe and confidential.
    - Ensuring staff do not represent their personal views as that of the school.
- Members of staff are encouraged not to identify themselves as employees of South Camberley Primary and Nursery School on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with school policies and the wider professional and legal framework.
    - Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Senior Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role in the school.

Communicating with pupils and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles.
    - South Camberley Primary and Nursery School recognises that there will be exceptions to this, where members of staff live within the area that we serve and have children that attend the school and so relationships with other parents may form as a result. In these situations, staff are reminded of the staff code of conduct and referred to the reputation statements as above.
    - Any concerns regarding pre-existing contacts should be discussed with Designated Safeguarding Lead and/or the Executive Headteacher.
- Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Executive Headteacher.
- Any communication from pupils and parents received on personal social media accounts will be reported to the schools Designated Safeguarding Lead.

7.3 Pupils' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources.
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts specifically for children under this age.
- Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies including Preventing Bullying and Behaviour. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.
- Pupils will be advised:

- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs.
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
- To use safe passwords.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications and report concerns both within school and externally.
- The risks involved with generative AI and its uses to create misinformation, deepfakes, scams and other abusive materials.

7.4 Official Use of Social Media

- South Camberley Primary and Nursery School's official social media channels are:
- Instagram, Youtube, Instagram and Facebook these are managed through the use of school devices and through school accounts.
- The official use of social media sites, by the school, only takes place with clear educational or community engagement objectives, with specific intended outcomes.
  - The official use of social media as a communication tool has been formally approved by the Executive Headteacher.
  - Leadership staff have access to account information and login details for the social media channels.
- Official school social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
  - Staff use school provided email addresses to register for and manage any official school social media channels.
  - Official social media sites are suitably protected and, where possible, run and/or linked to/from the school website.
  - Public communications on behalf of the school will, where appropriate and possible, be read and agreed by at least one other colleague.
  - All communication on official social media platforms will be clear, transparent and open to scrutiny.
  - Any official social media activity involving pupils will be moderated by the school.
- The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff expectations

- Members of staff who follow and/or like the school social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the school, they will:
  - Consider the implication of the code of conduct when using social media accounts.
  - Be professional at all times and aware that they are an ambassador for the school.
  - Disclose their official role and/or position, but make it clear that they do not necessarily speak on behalf of the school.
  - Be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
  - Always act within the legal frameworks they would adhere to within the workplace, including:
  - Libel, Defamation, Confidentiality, Copyright, Data protection and Equalities laws.
  - Ensure that they have appropriate written consent before posting images on the official social

media channel.
    - Not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.
    - Not engage with any direct or private messaging with current, or past, pupils, parents and carers.
    - Inform their line manager, the Designated Safeguarding Lead and/or the Executive Headteacher of any concerns, such as criticism, inappropriate content or contact from pupils.

8.Use of Personal Devices and Mobile Phones

8.1 Expectations

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies, including, but not limited to: Behaviour and Child protection.
- Electronic devices of any kind that are brought onto site are the responsibility of the user at all times.

    - All members of the South Camberley Primary and Nursery School community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; the school accepts no responsibility for the loss, theft or damage of such items on school premises.
    - All members of the South Camberley Primary and Nursery School community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used in specific areas within the school site such as changing rooms and toilets.
- The sending of abusive or inappropriate messages/ content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our Behaviour policy.
- All members of the South Camberley Primary and Nursery School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school Behaviour or Child protection policies.

8.2 Staff Use of Personal Devices and Mobile Phones

- All members of staff adhere to the code of conduct policy.
- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as relevant school policy and procedures, such as: Confidentiality, Child protection, Data security and Acceptable use.
- Staff are to:
    - Keep mobile phones and personal devices in a safe and secure place during lesson time.
    - Keep mobile phones and personal devices switched off or switched to ‘silent’ mode during lesson times.
    - Not use personal devices during teaching periods, unless permission has been given by the ELT, such as in emergency circumstances.
    - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and carers.
    - South Camberley Primary and Nursery School recognises that there will be exceptions to this, where members of staff live within the area that we serve and have children that attend the school and so relationships with other parents may form as a result. In these situations staff are reminded of the staff code of conduct and referred to the reputation statements as above.
    - Any concerns regarding pre-existing contacts should be discussed with Designated Safeguarding Lead and/or the Executive Headteacher.

    - A further exception to the above will be in emergency cases, such as school trips, where the use of staff phones is absolutely necessary. In these cases, it is advised that members of staff take necessary precautions to mask their number by dialling 141 followed by the number to be called.
- Staff will not use personal devices, such as: mobile phones, tablets or cameras:
    - To take photos or videos of pupils and will only use work-provided equipment for this purpose.
    - Directly with pupils and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches the school policy, action will be taken in line with the school behaviour and allegations policy
    - If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

8.3 Pupils' Use of Personal Devices and Mobile Phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- South Camberley Primary and Nursery School expects pupil's personal devices and mobile phones to be switched off as they enter the school premises. At the beginning of registrations, phones will be placed in class trays, which are then stored in the office during the school day. Pupils will receive their phones at the end of the day and they may be switched on only as they leave the school premises.
- If a pupil needs to contact his/her parents or carers they will be allowed to speak to the school administrator who will decide the best cause of action.
    - Parents are advised to contact their child via the school office during school hours; exceptions may be permitted on a case-by-case basis, as approved by the Executive Headteacher.
- Mobile phones or personal devices will not be used by pupils during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff.
    - The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
    - If members of staff have an educational reason to allow children to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the Senior Leadership Team.
- If a pupil breaches the school policy, the phone or device will be confiscated and will be held in School office.
    - School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the school's Behaviour or Preventing Bullying policy, or could contain nudes and/ or semi-nudes or other illegal or harmful material .
    - Searches of mobile phone or personal devices will only be carried out in accordance with the Department for Education Searching, Screening and Confiscation advice (www.gov.uk/government/publications/searching-screening-and-confiscation)
    - Pupils' mobile phones or devices may be searched by a member of the senior leadership team if it contravenes school policies.
    - Mobile phones and devices that have been confiscated will be released to parents or carers from the school office at the end of the school day.
    - If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

8.4 Visitors' Use of Personal Devices and Mobile Phones

- Parents, carers and visitors (including volunteers and contractors) must only use their mobile phones and personal devices in accordance with the school's Acceptable use policy and other associated policies, such as: Preventing Bullying, Behaviour and Child Protection.
- The school will ensure appropriate information is provided to inform parents, carers and visitors of expectations of use.

- For South Camberley Primary and Nursery School, parents are allowed to take pictures and videos of their own child but should be clearly advised that any photos/videos are not permitted to be uploaded to any Social Media sites.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the Designated Safeguarding Lead of any breaches of school policy.

9. Responding to Online Safety Incidents and Concerns

- All members of the school community will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, the sharing of nudes or semi—nudes, cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns.
  Pupils, parents and staff will be informed of the school's complaints procedure and staff will be made aware of the whistleblowing procedure.
- The school requires staff, parents, carers and pupils to work in partnership to resolve online safety issues.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the Education Safeguarding Team.
- Where there is suspicion that illegal activity has taken place, the school will contact the Education Safeguarding Team or Surrey Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with Surrey Police and/or the Education Safeguarding Team first, to ensure that potential investigations are not compromised.

9.1 Staff Misuse

- Any complaint about staff misuse will be referred to the Executive Headteacher, according to the Allegations policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with the Behaviour policy and Code of conduct.

10. Procedures for Responding to Specific Online Incidents or Concerns

10.1 Youth Produced Sexual Imagery or the sharing of nudes and semi-nudes

- South Camberley Primary recognises the sharing of nude and semi nudes, including those created using generative AI, as a safeguarding
  issue; therefore all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- The school will follow the advice as set out in the non-statutory UKCCIS guidance:

Sharing nudes and semi-nudes: advice for education settings working with children and young people

10.1.1 Dealing with the sharing of nudes and semi-nudes

- If the school are made aware of any incident involving the creation or distribution of youth produced sexual Imagery, nudes or semi-nudes, the school will:
  - Act in accordance with our Child protection and Safeguarding policies and the relevant Surrey Safeguarding Child Board's procedures.
  - Immediately notify the Designated Safeguarding Lead.
  - Store the device securely.
    - If an indecent image has been taken or shared on the school network or devices, the school will take action to block access to all users and isolate the image.
  - Carry out a risk assessment which considers any vulnerability of pupil(s) involved; including carrying

out relevant checks with other agencies.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - Make a referral to Specialist Children's Services and/or the Police, as appropriate.
    - Provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
    - Implement appropriate sanctions in accordance with the school's Behaviour policy, but taking care not to further traumatise victims where possible.
    - Consider the deletion of images in accordance with the UKCCIS: Sharing nudes and semi-nudes: advice for education settings working with children and young people guidance.
        - Images will only be deleted once the school has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
    - Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

- The school will take action regarding youth produced sexual imagery, including nudes and semi-nudes, regardless of whether the incident took place on/off school premises, using school or personal equipment.

- The school will not:
    - View any images suspected of being youth produced sexual imagery, including nudes and semi-nudes, unless there is no other possible option, or there is a clear need or reason to do so.
        - In this case, the image will only be viewed by the Designated Safeguarding Lead and their justification for viewing the image will be clearly documented.
    - Send, share, save or make copies of content suspected to be an indecent image of children (i.e. youth produced sexual imagery) and will not allow or request pupils to do so.

10.2 Indecent Images of Children (IIOC)

- South Camberley Primary and Nursery School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC), including those produced through the use of generative AI.
- The school will take action regarding IIOC on school equipment and/or personal equipment, even if access took place off site.
- The school will take action to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If the school is unclear if a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through Surrey Police and/or the Education Safeguarding Team.

- If made aware of IIOC, the school will:
    - Act in accordance with the schools child protection and safeguarding policy and the relevant Surrey Safeguarding Child Boards procedures.
    - Immediately notify the school Designated Safeguard Lead.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Surrey police or the LADO.

- If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet, the school will:

- Ensure that the Designated Safeguard Lead is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Report concerns, as appropriate to parents and carers.

- If made aware that indecent images of children have been found on the school devices, the school will:
  - Ensure that the Designated Safeguard Lead is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
  - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
  - Report concerns, as appropriate to parents and carers.

- If made aware that a member of staff is in possession of indecent images of children on school devices, the school will:
  - Ensure that the Executive Headteacher is informed.
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
  - Quarantine any devices until police advice has been sought.

10.3 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at South Camberley Primary and Nursery School.
- Full details of how the school will respond to cyberbullying are set out in the Preventing Bullying policy.

10.4 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at South Camberley Primary and Nursery School and will be responded to in line with existing school policies, including Preventing Bullying and Behaviour.
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If the school is unclear on how to respond, or whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice through the Education Safeguarding Team and/or Surrey Police.

10.5 Online Radicalisation and Extremism

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school.
- If the school is concerned that a child or parent/carer may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately and action will be taken in line with the Child protection policy.
- If the school is concerned that member of staff may be at risk of radicalisation online, the Executive Headteacher will be informed immediately and action will be taken in line with the Child protection and Allegations policies.

Appendices

Acceptable Use Policy (September 2025)

Acceptable Use Policy (September 2025) **AUP Review Date**	
Date of Next Review	**September 2025**
Reviewer	**Computing Subject & Online Safety Leader**

Covers use of all digital technologies in school: i.e. email, Internet, intranet, network resources, learning platform, software, communication tools, equipment and systems.

- I will follow the Online Safety & Data Protection Policies.
- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Executive Head Teacher and Governing Board.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access my school email address / the Internet / the school network, or other school systems, or any Local Authority (LA) system I have access to without the Executive Head Teacher's prior consent.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's Data Protection Policy.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I understand that I am responsible for any/all IT-related equipment loaned to me in order to fulfil my professional duties, including network access, and accept that any damage caused through negligence may be subject to discipline and the cost of repair or replacement.
- I will only use the approved email system(s) for any school business. This is currently: Office 365.
- I will only use school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the Computing Subject Leader or School Business Manager.
- I will not download any software or resources from the Internet that can compromise the network, might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos,

that is protected by copyright without seeking the author's permission.

- I will not connect any device to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's anti-virus software.
- I will follow school data security protocols when using any such data at any location.
- I will not use personal clouds or any other storage devices in school.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos on personal devices or at home.
- I will only use school-approved equipment and networks for storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the appropriate system or staff-only drive within school.
- I will ensure that mobile phones and personally owned devices are not used during lessons or formal school time. They should be always switched off (or silent) and stored securely away. Use of mobile phones during the school day will be limited to before school, break time, lunch break and after school if not on duty during these times.
- I will ensure that during permitted times, mobile phones and other personally owned devices are used in designated areas which are: staff rooms and classrooms when children are not present.
- I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I understand that the General Data Protection Policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert the Computing Subject Leader and/or Child Protection Officer / appropriate senior member of staff if I feel the behaviour of any user of the school's IT systems may be a cause for concern.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to the Computing and Online Safety Leader or a senior member of staff.
- I understand that all Internet and network traffic / usage is logged through Senso and this information can be made available to the Executive Head Teacher / Safeguarding Lead on their request and is regularly reviewed.
- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- *Staff that have a teaching role only:* I will embed the school's Online Safety and Computing Policy into my teaching.

Acceptable Use Policy (AUP): Agreement Form

All Staff, Volunteers, Governors

User Signature

- I agree to abide by all the points above.
- I understand that I have a responsibility for my own and others' online-safeguarding and I undertake to be a 'Safe and responsible digital technologies user'.
- I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent Online Safety & Data Protection Policies.
- I understand that failure to comply with this agreement could lead to disciplinary action.

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

Full Name ..... (printed)

Job title / Role .....

Authorised Signature (Executive Head Teacher)

I approve this user to be set-up on the school systems relevant to their role.

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

Full Name ..... (printed)

Staff Device Agreement, South Camberley Primary & Nursery School

Damage

Occasionally, unexpected problems do occur with devices that are not the fault of the user (computer crashes, software errors, etc.). The school IT and IT support team will assist staff with having these fixed. These issues will be remedied at no cost.

Accidental Damage vs. Negligence

Accidents do happen. There is a difference, however, between an accident and negligence. The device warranty will cover normal wear and tear along with any defects that may arise during normal use of the device.

After investigation by the school IT and IT support team and possible determination by the manufacturer, if the iPad is deemed to be intentionally or negligently damaged by the member of staff, the member of staff may be subject to discipline and the cost of repair or replacement.

Lost and Stolen Equipment

If any equipment is lost, the member of staff must report it to the Executive Head Teacher immediately.

The circumstances of each situation involving lost equipment will be investigated individually.

If any equipment is reported as stolen, a police report must be filed and a copy of the report must be provided to the school by the member of staff. If there is not clear evidence of theft, or the equipment has been lost due to staff negligence, the member of staff will be responsible for the full cost of replacing the item(s). This includes iPad and accessories.

Financial Responsibility

Outside of school hours, the devices are not covered by the school's insurance policy. Any loss or damage will be the responsibility of the member of staff. The actual cost of replacement will be determined by the manufacturer but will not exceed the retail value of like-for-like replacement.

The staff-assigned device remains the property of South Camberley Primary School. I understand and will abide by this agreement in conjunction with South Camberley Primary School's Acceptable Use Policy. Should I commit any violation, my access privileges may be revoked and school disciplinary action may be taken. I understand that loss or theft of my assigned iPad is my responsibility as well as any neglect toward the device.

User's Full Name: _____

User Signature: _____

Device Type: _____

Asset Tag No: _____

Serial Number: _____

Date: _____