

Sissinghurst Church of England VA Primary



Our School Vision

Let Your Light Shine – Matthew 5:16

At Sissinghurst Church of England Primary School in partnership with the Church, parents, and wider community, we offer an inclusive learning environment to nurture potential that enables all to be successful. Vibrant, rich curricular opportunities equip everyone with knowledge and skills to question, discuss and challenge.

Everyone's talents are discovered and celebrated. We foster spiritual growth and reflection to find wonder and joy in the World together. As light bearers, our shared responsibility is to encourage each other to be compassionate and kind so we can all shine with integrity, humility and wisdom. We find courage to act when we know there is darkness, illuminating the World with God's light and hope.

We are dedicated to providing an education of the highest quality within the context of Christian belief and practice. Our Christian values of:

Kindness Forgiveness Courage Service

Policy Title:	Acceptable Use of Technology Policy Templates for Educational Settings
Date:	Sept 2026
Review Date:	Sept 2027
Reviewed by:	Sarah Holman
Approved by:	FGB

Designated Safeguarding Lead – Sharmila Desai

Governor with Safeguarding responsibility – Elaine Highwood

This policy has been written in accordance with KCSIE and should be read alongside the school Social media, mobile and smart technology and Codes of conduct policies.

Contents

Children/Pupils/Student Acceptable Use of Technology Statements

Early Years and Key Stage 1 (0-6)

Key Stage 2 (7-11)

Key Stage 3/4/5 (11-18)

Children/Pupils/Students with SEND

Children/Pupils/Student Acceptable Use Policy Agreement Form

Acceptable Use of Technology Statements/Forms for Parents/Carers

Parent/Carer Acknowledgement Form

Acceptable Use of Technology for Staff, Visitors and Volunteers

Staff Acceptable Use of Technology Policy

Visitor and Volunteer Acceptable Use of Technology Policy

Wi-Fi Acceptable Use Policy

Remote/Online Learning AUP

Guidance Notes

Staff Statements

Pupil Acceptable Use of Technology Statements

Early Years and Key Stage 1 (Age 0-6)

- I understand that the school rules will help keep me safe and happy when I go online.
- I only go online when an adult is with me.
- I check with a grown-up before I click on links or things online.
- I keep my personal information and passwords safe.
- I only send polite and friendly messages online.
- I know the school can see what I am doing online when I use school computers / devices and systems learners are expected to use, including if I use them at home.
- If I see something online that makes me feel upset, unhappy, or worried I will always tell an adult.
- I can visit www.ceopeducation.co.uk to learn more about keeping safe online.
- I know that if I do not follow the rules my teachers will talk to me and I may need to speak to Mrs Holman and or my parents about how to be safe online.
- I have read and talked about these rules with my parents/carers.

Shortened KS1 version (for use on posters or with very young children)

- I only go online with a grown-up.
- I am kind online.
- I keep information about me safe online.
- I tell a grown-up if something online makes me unhappy or worried.

Key Stage 2 (Age 7-11)

I understand that the school Acceptable Use Policy will help keep me safe and happy online at home and at school.

Safe

- I will be kind and respectful online, just like I am in school.
- I only send messages which are polite and friendly.
- I will only share pictures or videos online if they are safe, kind, and I have asked for permission first.
- I will only click on links if I know what they do, or I will ask a safe adult first.
- I will only chat with people I know online, or I will ask a safe adult to help me decide if someone I don't know is safe to speak with online.
- If someone online asks to meet me, I will tell a safe adult straight away.

Learning

- In school I may use the school laptops, chrome books, ipads or tablets. I always ask an adult before using one.
- I am not allowed to use mobile phones or personal smart devices at school.
- If I need to bring my mobile phone to school it must be switched off and handed into the office when I arrive. The office will keep it safe and I may collect it at the end of the day.
- I always ask permission from an adult before using the internet.
- I only use websites, tools and search engines that my teacher has chosen or given me permission to use.
- I use school devices for school work unless I have permission otherwise.
- If I need to learn online at home, I will follow the same rules in this policy.

True

- I know that some things or people online might not be honest or truthful.
- If I'm not sure something online is true, I will check with other websites, books, or ask a safe adult.
- I always credit the person or source that created any work, images, or text I use.
- I will only use Artificial Intelligence (AI) tools when my teacher says it is allowed.
- I will not put personal information about me or anyone else into AI tools. I will not use AI to make fake images, voices, videos or messages about other people.

Responsible

- I keep my personal information safe and private online.
- I will keep my passwords safe and will not share them.
- I will not access or change other people's files or information.
- I will only change the settings on a device if a member of staff has allowed me to.

Tell

- If I see anything online that I should not or that makes me feel worried or upset, I will minimise the page and tell an adult straight away.
- If I am aware of anyone being unsafe with technology, I will report it to a teacher.
- If an AI tool shows me something worrying, unkind, rude, violent, confusing or unsafe, I will stop and tell a safe adult.
- I understand that the adults at school are responsible for keeping me safe; they may need to speak to other safe adults, or my parents/carers, if I tell them about something that has happened online.
- I can visit www.ceopeducation.co.uk and www.childline.org.uk to learn more about being safe online or to seek help.

Understand

- I understand that the school internet filter is there to protect me, and I will not try to bypass it.
- I know that all school devices, networks and systems are monitored to help keep me safe, including when I use them at home. This means someone at the school may be able to see and/or check my online activity when I use school devices and/or networks if they are worried about my or anyone else's safety or behaviour.
- I have read and talked about these rules with my parents/carers.
- I can visit www.ceopeducation.co.uk and www.childline.org.uk to learn more about being safe online.
- If, for any reason, I need to bring a personal device, like a mobile phone and/or other wearable technology into school then I will hand it in to the office for the day.
- I understand that my behaviour online can affect others and I will not behave in a way that will upset, frighten or embarrass others.
- I have read and talked about these rules with my parents/carers.
- I know that if I do not follow the school rules then my teachers will talk to me and I may need to speak to Mrs Holman and / or my parents about how to be safe online.

Shortened KS2 version (for use on posters)

- I ask an adult about which websites I can use.
- I will not assume information online is true.
- I know there are laws that stop me copying online content.
- I know I must only open online messages that are safe. If I am unsure, I will not open it without speaking to an adult first.
- I know that people online are strangers, and they may not always be who they say they are.
- If someone online suggests meeting up, I will always talk to an adult straight away.
- I will not use technology to be unkind to people.
- I will keep information about me and my passwords private.
- I always talk to an adult if I see something which makes me feel worried.

Sissinghurst CE (VA) Primary School
Acceptable Use of Technology Policy – Pupil Agreement

I, with my parents/carers, have read and understood the school Acceptable Use of Technology Policy (AUP) and remote learning AUP.

I agree to follow the AUP when:

1. I use school devices and Google Classroom both at school and at home.
2. I use my own equipment out of the school, including communicating with other members of the school or when accessing Google Classrooms

Name..... Signed.....

Class..... Date.....

Parent/Carer's Name.....

Parent/Carer's Signature.....

Date.....

Parent/Carer AUP Acknowledgement Form

Sissinghurst CE (VA) Primary School Pupil Acceptable Use of Technology Policy Acknowledgment

1. I have read and discussed Sissinghurst CE (VA) Primary School pupil acceptable use of technology policy (AUP) expectations with my child in a way that is appropriate to their age, understanding and needs.
2. I understand that the AUP explains how my child is expected to use technology safely, kindly, lawfully and responsibly, including when using: School laptops, Chrome books, tablets, ipads and Google Classroom and personal devices or services where their use affects the safety or wellbeing of a child or another person, disrupts the safe or effective operation of the school, or raises a safeguarding or behaviour concern.
3. I understand that access to online content through school devices and systems is appropriately filtered and that use of school-provided devices, accounts and systems may be monitored, including when they are used away from the setting.
4. I understand that filtering and monitoring arrangements help to keep children safe, protect systems and support compliance with relevant policies, but cannot remove every online risk. Monitoring will be proportionate and undertaken in accordance with data protection, privacy and human rights requirements.
5. I am aware of the school's expectations concerning mobile phones and smart devices and will support my child to follow them. If my child may need an exception or reasonable adjustment because of a disability, medical condition, communication need or other individual circumstance, I will discuss this with the school so that appropriate arrangements can be considered, agreed and recorded. I will support any individual arrangements agreed for my child. If I need to contact my child during the school day, I will use the school office or another agreed contact route, unless an alternative arrangement has been agreed.
6. I will support my child to understand and follow the school's expectations for technology use, including social media, mobile phones, online communication, images and recordings and, where relevant, artificial intelligence tools.
7. I will model safe, positive and respectful online behaviour and support my child not to create, post or share content that identifies, targets, threatens, bullies, harasses or risks causing harm to a child, family, member of staff or another member of the school community.
8. If I have a concern or complaint, I am encouraged to use the school's established communication, safeguarding or complaints routes, as appropriate, so that it can be properly considered.
9. I will report concerns about my child's online safety, or online concerns that may affect the safety or wellbeing of another member of the school community, to an appropriate member of staff. This may include class teacher, the Designated Safeguarding Lead or Headteacher. Where necessary, I may also report the concern to another relevant organisation.
10. If the school has concerns about my child's online safety or behaviour, I understand that these will be considered fairly and proportionately in line with relevant safeguarding, behaviour and other procedures. The school will communicate with me where it is appropriate and safe to do so.
11. I understand my role in helping my child to use technology safely. As appropriate to my child's age, understanding and needs, I will consider the use of parental controls, provide suitable supervision and support, and encourage safe and responsible use of the internet and other technology at home.
12. I know that I can speak to the Designated Safeguarding Lead, Sharmila Desai, Deputy Headteacher if I have any concerns or need support or information about online safety.

I acknowledge that I have received and read the Pupil Acceptable Use of Technology Policy and have discussed its expectations with my child.

Child's Name..... Child's Signature (*if appropriate*)

Class..... Date.....

Parent/Carer's Name.....

Parent/Carer's Signature..... Date.....

Acceptable Use of Technology for Staff, Visitors and Volunteers

Staff Acceptable Use of Technology Policy (AUP)

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Sissinghurst CE (VA) Primary School IT systems in a professional, lawful, and ethical manner. To ensure that members of staff understand their professional responsibilities when using technology and provide appropriate curriculum opportunities for pupils, they are asked to read and sign the staff Acceptable Use of Technology Policy (AUP).

Our AUP is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally, however the AUP will help ensure that all staff understand the school expectations regarding safe and responsible technology use and can manage the potential risks posed. The AUP will also help to ensure that school systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

Policy scope

1. I understand that this AUP applies to my use of technology systems and services provided to me or accessed as part of my role within Sissinghurst CE (VA) Primary School both professionally and personally. This may include use of laptops, Chrome books, mobile phones, tablets, digital cameras, and email as well as IT networks, data and data storage, remote learning and online and offline communication technologies.
2. I understand that Sissinghurst CE (VA) Primary School Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school child protection including online safety policy, staff code of conduct and remote/online learning AUP.
3. I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the school ethos, school code of conduct and safeguarding policies, national and local education and child protection guidance, and the law.

Use of school devices and systems

4. I will only use the equipment and internet services provided to me by the school for example school provided laptops, tablets, mobile phones, and internet access, when working with pupils.
5. I understand that any equipment and internet services provided by my workplace is intended for education purposes and/or professional use and should only be accessed by members of staff. Reasonable personal use is permitted but must not interfere with my work duties, system security, safeguarding, confidentiality or professional boundaries. This permission is at the school's discretion and may be withdrawn at any time.

Data and system security

6. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.
 - I will follow the school's requirements for secure passwords, authentication and account access. I will keep authentication information secure and will not share passwords, verification codes or access credentials with others.
 - I will protect the devices in my care from unapproved access or theft by being mindful about where I leave my devices and not leaving them unsupervised in public places.
7. I will take care before opening links or attachments, including those apparently sent by a known contact. I will check unexpected or suspicious messages through an appropriate route and report suspected phishing or malicious content to Perry Everard.
8. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT Technician – Perry Everard.

9. I will ensure that any personal data is kept in accordance with data protection legislation, in line with the school information security policies.
- All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
 - Any data being removed from the school site, such as via email or on memory sticks or CDs, will be suitably protected. This may include data being encrypted by a method approved by the school.
 - I will only process or share personal data through school-approved systems and services and in line with the setting's data protection and information-security procedures. Any proposed new or changed use of cloud services, AI tools or other online systems involving personal data will be risk assessed and approved through the setting's agreed process before use. Where required, a Data Protection Impact Assessment will be completed.
10. I will not keep documents which contain school related sensitive or personal information, including images, files, videos, and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the school learning platform to upload any work documents and files in a password protected environment or school VPN.
11. I will not store any personal information on the school IT system, including school laptops or similar device issued to members of staff, that is unrelated to school activities, such as personal photographs, files or financial information.
12. I will ensure that school owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
13. I will not attempt to bypass any filtering and/or security systems put in place by the school.
14. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the ICT Support Provider Perry Everard and the Headteacher as soon as possible.
15. If I have lost any school related documents or files, I will report this to the ICT Support Provider Perry Everard and school Data Protection Officer SATSWANA via the Headteacher as soon as possible.
16. I will follow the school image use policy when taking, using, storing or sharing images or recordings of children. Images and recordings must always be appropriate and must only be taken using school-provided or approved equipment. I will not use personal devices, including personal mobile phones, cameras, tablets, smart watches or other wearable technology, to take images or recordings of children. Images and recordings will only be taken, used or shared in line with the school image use policy, safeguarding expectations, data protection requirements and consent/lawful basis arrangements.

Classroom practice

17. I understand my role and responsibilities in relation to filtering and monitoring, as explained through induction, safeguarding training and relevant school policies.
18. If I become aware of a filtering or monitoring failure, or witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material, I will report this to the DSL and IT provider/staff, in line with the school child protection policy.
19. I will follow school expectations for safe technology use in classrooms, remote/online learning and other working spaces, including the use of approved platforms, search tools and AI tools. The school agreed AI system is Microsoft Copilot.

20. I will follow the setting's agreed approach to screen use. Any use of screens, devices, apps or online content will be planned, purposeful, age appropriate and supervised, and will not replace face-to-face interaction, play, physical activity, rest, care routines or real-world exploration.
21. I am aware that generative artificial intelligence (AI) tools may have many uses which could benefit our school community. However, I recognise that AI tools can also pose risks, including, but not limited to, bullying and harassment, abuse and exploitation (including child sexual abuse), privacy and data protection risks, plagiarism and cheating, and inaccurate, harmful and/or biased material. Additionally, their use can pose moral, ethical and legal concerns if not carefully managed. As such, I understand that:
- AI tools must only be used responsibly, ethically and where the tool, purpose and use have been approved by leaders. Any new, unapproved or changed use of AI tools will be risk assessed and approved before use, in line with child protection, data protection and professional conduct expectations.
 - I understand that AI-generated content must be checked for accuracy, bias, appropriateness, copyright and safeguarding implications before it is used or shared.
 - I will not enter personal, sensitive, confidential, safeguarding, assessment or special category information, or images of children, staff or other identifiable individuals, into any AI tool unless the tool has been approved for that purpose, the use has been risk assessed, consent has been obtained where required, and the DPO/leadership team has confirmed that the processing is lawful and appropriate.
 - I will not add or use AI note takers, transcription tools, recording bots or automated meeting summary tools in any meeting, lesson, supervision, training or professional discussion unless this has been agreed in advance by leadership. Where approved, I will ensure that participants are made aware and their use is transparent, proportionate and in line with safeguarding, confidentiality, consent, data protection and information governance expectations.
 - I will not use AI to make decisions about children, families or staff, including decisions relating to safeguarding, behaviour, SEND, assessment, attendance, admissions, recruitment, allegations or pastoral support, without appropriate professional oversight and in line with setting policy.
 - Only approved AI platforms may be used with children. Children must be supervised when using AI tools, and I must ensure age-appropriate use and understanding prior to use.

I will report any concern involving AI misuse, including deepfake or manipulated content, impersonation, harmful AI-generated material, AI-facilitated bullying or harassment, or AI-generated nude/semi-nude imagery, in line with the school child protection, behaviour, anti-bullying, staff conduct and data protection procedures.

Mobile devices and smart technology

22. I will ensure that my use of mobile phones and smart devices is compatible with my professional role, does not interfere with my duties, and takes place in line with the staff behaviour policy/code of conduct, mobile phone policy and the law.
23. I will model safe and professional use of mobile phones and smart devices and will support the school's expectations for children.
24. Where mobile phones or smart devices are used for professional purposes, such as authentication, learning activities, recording rewards or sanctions, or other agreed tasks, I will use school-provided devices where available. Where staff are permitted to use personal devices for professional purposes, this must be formally agreed by the school and managed in line with school policy.
25. Any use of a personal mobile phone or smart device for professional purposes, or in exceptional circumstances, must be transparent, necessary, proportionate and approved by the headteacher or other designated leader. Use must not compromise supervision, safeguarding, confidentiality, professional boundaries, data protection or the learning environment.

Online communication, including use of social media

26. I will ensure that my use of communication technology, including social media, is compatible with my professional role, does not interfere with my work duties, and takes place in line with the child protection policy, staff behaviour policy/code of conduct, social media policy and the law.
27. I will protect myself, my professional reputation and the reputation of the school online. I will not discuss or share data or information relating to children, staff, school business or parents/carers on social media.
28. My electronic communications with current and former children and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.
- I will ensure that all electronic communications take place in a professional manner via school-provided communication channels and systems, such as a school email address, user account or telephone number.
 - I will not use personal accounts, personal profiles, personal phone numbers, private messaging apps, gaming accounts or other personal communication channels to contact or communicate with **children** or their families, unless this has been formally approved, risk assessed and recorded by leaders.
 - I will not share any personal contact information or details with children, such as my personal address, email address or phone number.
 - I will not share personal information about my private life with children online, through messaging, social media, gaming platforms, apps or other digital communication channels. I will maintain appropriate professional boundaries in all digital communication.
 - I will not add, follow, accept or respond to friend requests, direct messages or other personal online communication from current or former children, or their parents/carers, where this is linked to my role, the school, or could blur professional boundaries. Any attempted contact will be reported to my line manager and/or the DSL.
 - Any pre-existing links, relationships or situations that affect how I apply the AUP or other relevant policies will be discussed with the DSL and/or headteacher. This is to help safeguard children, staff and the wider school community by ensuring professional boundaries, safeguarding expectations and communication arrangements are clear.
 - Where digital communication with children or families is required, I will follow the school's expectations about when communication should take place, including any agreed arrangements for out-of-hours contact, emergency communication or role-specific responsibilities.

Policy concerns

29. I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, terrorist material or adult pornography covered by the Obscene Publications Act.
30. I will not access, create, transmit, display, publish, forward, discuss, send, share or show any material or content that may be harmful, inappropriate, adult, offensive, unprofessional, or likely to harass, cause offence, inconvenience or needless anxiety to any other person. This applies when using school systems, school devices, personal devices, personal accounts, messaging apps, online platforms, social media or shared spaces. It includes content shared in staff rooms, offices, online groups or other staff communication spaces, where this takes place on school premises, during working time, or in any context linked to my role.
31. I will not engage in online or digital behaviour linked to my role that compromises safeguarding, professional boundaries, confidentiality, data protection, public confidence in my professional conduct or my ability to carry out my role.
32. I will report and record any concerns about the welfare, safety or behaviour of children or parents/carers online to the DSL in line with the school child protection policy.
33. I will report concerns about the welfare, safety, conduct, or behaviour of staff, including online, digital, device-related or technology-linked concerns, to the headteacher, in line with the school child protection policy, staff behaviour policy/code of conduct, low-level concerns procedures and/or allegations against staff policy.

Policy compliance and breaches

34. If I have any queries or questions regarding safe and professional practice online, either in school or off-site, I will raise them with the DSL and/or the headteacher.
35. I understand that the school may exercise its right to monitor the use of its devices and information systems to check policy compliance and help ensure the safety of children and staff.
- This includes monitoring all school-provided devices and school systems and networks including school-provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via school-provided devices, systems and/or networks.
 - This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.
 - Staff will be informed about the nature, purpose and extent of monitoring through this AUP, relevant policies, privacy information and/or staff guidance.
36. I understand that if the school believes that unauthorised and/or inappropriate use of school devices, systems or networks is taking place, the school may invoke its disciplinary procedures as outlined in the staff handbook /code of conduct.
37. If I find myself in a situation where my online contact, device use, recording, image use or AI use could be misinterpreted, I will report this promptly to the DSL and / or headteacher so it can be recorded and managed transparently.
38. Any breach or concern involving online contact, device use, images, recordings, social media, AI use, confidentiality, data protection or professional boundaries must be reported to the headteacher and/or DSL without delay, even if it appears minor, accidental or unlikely to meet the harm threshold.
39. I understand that if the school believes that unprofessional or inappropriate online or technology-related activity may have compromised safeguarding, professional boundaries, confidentiality, data protection, public confidence in professional conduct or my ability to carry out my role, the concern will be considered fairly, proportionately and confidentially, in line with relevant safeguarding, staff behaviour, low-level concerns, allegations, data protection and disciplinary procedures. Where the concern may meet the harm threshold, advice will be sought and/or a referral made to the Local Authority Designated Officer (LADO) in line with local allegations procedures. Where it does not meet this threshold, it will still be recorded and responded to appropriately.
40. Where a concern involves personal data, confidential information, safeguarding information, images, recordings, AI tools, transcription tools or unauthorised sharing, the DPO/data protection lead will be informed promptly so that any data protection, information governance or reporting requirements can be considered.
41. I understand that if the school suspects criminal offences have occurred, the police will be informed where appropriate.
42. I understand that this AUP cannot cover every possible situation. If I am unsure whether any use of technology, online communication, image use, recording, personal device use, social media, AI tool or digital contact is appropriate, I will seek advice from the DSL and/or headteacher before taking action. I will act in a way that safeguards children, protects professional boundaries, and is open to scrutiny.

I have read, understood and agreed to comply with Sissinghurst CE (VA) Primary School Staff Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of staff member:

Signed:

Date (DDMMYY).....

Visitor and Volunteer Acceptable Use of Technology Policy

As a professional organisation with responsibility for safeguarding, it is important that visitors and volunteers understand our expectations for safe, lawful and responsible technology use while on site, when using [school/setting] systems, or when acting in a role connected to the [school/setting]. This AUP helps [school/setting name] explain expectations around safeguarding, professional conduct, data protection, image use, mobile phones, online communication and reporting concerns.

Policy scope

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems, services, devices or information provided by the [school/setting], or accessed by me as part of my role, visit or activity with Sissinghurst Primary School. It also applies to personal devices or accounts where their use takes place on site, involves the school community, is linked to my role or visit, or could affect safeguarding, confidentiality, data protection, professional boundaries or the reputation of the school.
2. I understand that this AUP should be read and followed in line with relevant school policies, including the staff behaviour policy/code of conduct, child protection policy, visitor/volunteer procedures, image use policy and mobile phone/smart device policy.
3. I am aware that this AUP does not provide an exhaustive list; visitors and volunteers should ensure that all technology use is consistent with the school ethos, school staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.
4. I will not upload, download or access any materials which are illegal, including but not limited to child sexual abuse material, criminally racist material, terrorist material or adult pornography covered by the Obscene Publications Act.
5. I will not access, create, transmit, display, publish, forward, discuss, send, share or show any material or content that may be harmful, inappropriate, adult, offensive, unprofessional, or likely to harass, cause offence, inconvenience or needless anxiety to any other person. This applies when using school systems, school devices, personal devices, personal accounts, messaging apps, online platforms, social media or shared spaces, where this takes place on school premises, during my visit/volunteering activity, or in any context linked to my role.
6. I will not engage in any online activity, digital communication or behaviour that could compromise safeguarding, professional boundaries or the reputation of the school.

Data and image use

7. Where I have access to personal data, confidential information, safeguarding information, school systems, records or devices, I will only access, use or share this information where it is necessary for my agreed role, visit or activity and in line with data protection legislation and school procedures. I will not copy, download, photograph, record, forward or share information unless this has been authorised.
8. I will not take, use, store or share images or recordings of children during lessons, visits, trips, events, performances, activities or celebrations unless this has been specifically authorised by the school and is in line with the school image use policy. Where authorised, images or recordings must only be taken, used, stored or shared using school approved equipment, accounts and systems, unless leaders have made a specific, risk-assessed decision otherwise. I will not take images or recordings of children for personal use or share them on personal devices, personal accounts, social media, messaging apps or online groups.

Classroom practice

9. I am aware of the expectations regarding safe use of technology in the classroom and other working spaces, including appropriate supervision of children.

10. Where I deliver or support remote/online learning, I will comply with the school remote/online learning AUP.
11. Where I am supporting children, I will reinforce safe and appropriate technology use and will follow staff instructions and school policies.
12. If I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material by any member of the school community, I will report this to a Designated Safeguarding Lead (DSL) and Headteacher, in line with the school child protection policy.
13. I will respect copyright and intellectual property rights and ensure my use of online platforms and tools is safe, legal and ethical; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, misuse, plagiarise, or distribute them.
14. I will not record, transcribe, livestream, use AI note-taking tools, recording bots or automated meeting summary tools during any meeting, visit, lesson, activity or professional discussion unless this has been specifically authorised by the [school](#) and is in line with safeguarding, confidentiality, consent and data protection expectations.

Use of mobile phones and smart devices

15. In line with the school mobile phone and smart device policy, I will model safe and appropriate use of mobile phones and smart devices while on site. I will not use my own mobile phone or smart device in front of children unless this has been agreed by the school and is directly linked to my role, visit or volunteering activity. I will follow the school's expectations about where and when mobile phones and smart devices may be used or stored.

Online communication, including the use of social media

16. I will ensure that my online conduct, reputation and use of technology are compatible with my role within the school. This includes my use of email, text, social media, social networking, gaming and any other personal devices or websites.
17. Any electronic communication with children, parents/carers or staff as part of my role, visit or volunteering activity will take place within clear professional boundaries and be transparent and open to scrutiny.
 - Communication will take place using school approved channels, such as a school-provided email address, account, platform or telephone number.
 - I will not use personal devices, personal email, personal social media, private messaging apps, gaming accounts or personal phone numbers to contact children or their families unless this has been formally approved, risk assessed and recorded by leaders.
 - Any pre-existing relationships, links or situations that may affect how I apply this AUP will be discussed with the DSL and/or headteacher.
18. I will respect confidentiality and will not post, comment on, discuss or share information online about children, staff, families, incidents, activities or anything I become aware of through my role, visit or volunteering activity. This includes comments, images, videos, recordings or information shared on personal social media, messaging apps, online groups or community forums.

Policy compliance, breaches or concerns

19. If I have any queries or questions regarding safe and professional practice online either in school or off site, I will raise them with the Designated Safeguarding Lead – Sharmila Desai and/or the headteacher.
20. I understand that the school may exercise its right to monitor the use of its devices and information systems to check policy compliance and help ensure the safety of children and staff.
 - This includes monitoring all school-provided devices and school systems and networks, including school-provided internet access, whether used on or offsite, and may include the interception of messages and emails sent or received via school-provided devices, systems and/or networks.

- This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

21. I will report and record any concerns about the welfare, safety or behaviour of children or parents/carers online to the DSL, in line with the school child protection policy.
22. I will report concerns about the welfare, safety, conduct or behaviour of staff, including online, digital, device-related, image-related or technology-linked concerns, to the headteacher, in line with the school child protection policy, staff behaviour/code of conduct, low-level concerns procedures and/or allegations against staff policy.
23. I understand that if the school believes that illegal, unauthorised or inappropriate use, unacceptable behaviour, or a breach of this AUP has taken place, action may be taken in line with relevant safeguarding, behaviour, complaints, volunteer, contractor, visitor, data protection, low-level concerns or allegations procedures, as appropriate. This may include ending or restricting access to the site, systems or activities, informing an employer/agency/organisation, seeking advice from the LADO, informing the DPO/data protection lead, or contacting the police where appropriate.
24. Any breach or concern involving online contact, device use, images, recordings, social media, AI use, confidentiality, data protection or professional boundaries must be reported to the DSL or headteacher without delay, even if it appears minor, accidental or unlikely to meet the harm threshold.
25. Where a concern involves personal data, confidential information, safeguarding information, images, recordings, AI tools, transcription tools or unauthorised sharing, the Data Protection Officer (DPO) will be informed promptly so that any data protection, information governance or reporting requirements can be considered.
26. I understand that this AUP cannot cover every possible situation. If I am unsure whether any use of technology, online communication, image use, recording, personal device use, social media, AI tool or digital contact is appropriate, I will seek advice from the DSL and/or headteacher.

I have read, understood and agreed to comply with Sissinghurst CE (VA) Primary School visitor/volunteer Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of visitor/volunteer:

Signed:

Date (DDMMYY).....

Wi-Fi Acceptable Use Policy

As a professional organisation with responsibility for safeguarding children, all users must understand the boundaries and expectations when using the school Wi-Fi. Users are expected to use Wi-Fi safely, lawfully and responsibly, and to take reasonable steps to protect devices, data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

This is not an exhaustive list. All users are reminded that technology use should be consistent with the school ethos, relevant policies and the law.

1. The school provides Wi-Fi for educational use only.
2. Use of the Wi-Fi falls under Sissinghurst Primary School Acceptable Use of Technology Policy (AUP), the child protection policy, behaviour policy/code of conduct, data protection/security policies and any other relevant policies. All children, staff, visitors and volunteers using the Wi-Fi must comply with these expectations.
3. The school reserves the right to limit, restrict, withdraw or manage Wi-Fi access where necessary to maintain safeguarding, security, network reliability or fair use of network resources.
4. Sissinghurst Primary School owned information systems, including Wi-Fi, must be used lawfully. I understand that the Computer Misuse Act 1990 makes it a criminal offence to gain unauthorised access to computer material, gain unauthorised access with intent to commit or facilitate further offences, or modify computer material without authorisation.
5. I will take reasonable steps to ensure that any personal device connected to school Wi-Fi is appropriately secure, for example by using security updates, antivirus protection where appropriate, and secure passwords/PINs.
6. I will respect system security and will not share passwords, Wi-Fi access details or security information. I will not attempt to bypass school security, filtering or monitoring systems, or download unauthorised software, applications or files.
7. I will not use school Wi-Fi to access, create or share illegal or harmful content, compromise another person's safety or privacy, interfere with systems, or breach relevant school policies.
8. I will not use school Wi-Fi to access, store, send or share confidential, personal or safeguarding information unless this has been specifically authorised and is in line with school data protection and safeguarding procedures.
9. Staff using school Wi-Fi on personal devices remain subject to the staff code of conduct, Staff AUP, mobile phone/smart device policy, data protection expectations, and relevant safeguarding and disciplinary procedures.
10. The school takes reasonable and proportionate steps to manage the security of its Wi-Fi service. However, no wireless or internet service can be guaranteed to be free from all risk. Where personal devices are permitted to connect to the school Wi-Fi, users do so at their own discretion and are expected to keep their devices secure. Any concerns about Wi-Fi security, filtering, monitoring or device safety should be reported to the DSL or identified technical contact.
11. I will report any online safety concerns, filtering breaches, security concerns, or access to inappropriate materials to the Designated Safeguarding Lead – Sharmila Desai or identified technical contact as soon as possible. If I have any queries about safe behaviour online, I will speak to the DSL, identified technical contact or headteacher.
12. I understand that activity carried out through school Wi-Fi may be monitored and recorded to check policy compliance, protect systems and help keep users safe, including where the Wi-Fi is accessed using a personal device. This does not mean that the school can monitor other activity or information held on the personal device. Monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.
13. If the school suspects that unauthorised or inappropriate use, unacceptable behaviour, a data protection concern, a safeguarding concern or criminal activity may have taken place, access may be restricted or withdrawn and the concern may be managed in line with relevant [school/setting] procedures. Where appropriate, this may include informing the DSL, Data Protection Officer, headteacher/manager, employer/organisation, LADO or police.

**I have read, understood and agreed to comply with Sissinghurst CE (VA) Primary School
Wi-Fi Acceptable Use Policy. Please get the code from the Office.**

Name

Signed:Date (DDMMYY).....

Acceptable Use Policy (AUP) for Remote/Online Learning

KCSIE states “Schools and colleges are likely to be in regular contact with parents and carers. Those communications should be used to reinforce the importance of children being safe online and parents and carers are likely to find it helpful to understand what systems schools and colleges use to filter and monitor online use. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will be asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online”.

This policy specifically addresses safer practice when running formal remote/online learning, including live streamed sessions, but can also apply to other online communication, such as remote/online parent meetings or pastoral activities.

Remote/Online Learning AUP Template - Staff Statements

Sissinghurst CE (VA) Primary School Staff Remote/Online Learning AUP

The Remote/Online Learning Acceptable Use Policy (AUP) is in place to safeguard all members of Sissinghurst CE (VA) Primary School community when taking part in remote/online learning, for example following any full or partial school closures.

Leadership oversight and approval

1. Remote/online learning will only take place using **Google Classroom**
 - **Google Classroom** has been assessed and approved by the **SLT**.
2. Staff will only use **school** managed **or** specific, approved professional accounts with pupils **and/or** parents/carers.
 - Use of any personal accounts to communicate with pupils and/or parents/carers is not permitted.
 - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with **Sharmila Desai**, Designated Safeguarding Lead (DSL).
 - Staff will use work provided equipment where possible **e.g. a school laptop, tablet, ipad or other mobile device**.
3. Online contact with pupils **and/or** parents/carers will not take place outside of the operating times as defined by SLT:

Weekdays 8:30am – 4pm (NB. later times are permitted for agreed parent consultation evenings held virtually although the TEAMS platform would most likely be used for this if needed, staff should ensure the school office has a copy of the timetable for parent consultation meetings held virtually)
4. All remote/online lessons will be formally timetabled; **a member of SLT** is able to drop in at any time.
5. Live-streamed remote/online learning sessions will only be held with approval and agreement from **a member of SLT**.

Data Protection and Security

6. All remote/online learning and any other online communication will take place in line with current **school** confidentiality expectations as outlined in **our code of conduct**.
7. All participants will be made aware if Google Classrooms is being used to record activity and consent will be taken from all participants.
8. Staff will not record lessons or meetings using personal equipment.
9. Only members of the school community will be given access to the school **Google Classroom**.
10. Access to **Google Classroom** will be managed in line with current IT security expectations and it is expected that all staff will use strong password and will log off securely.
11. AI note takers, transcription tools, recording bots or automated meeting summaries must not be used in remote/online learning, meetings or training unless this has been approved in advance by leaders and is managed in line with safeguarding, consent, confidentiality and data protection requirements.

Session management

12. Staff will record the length, time, date, and attendance of any live sessions held.
13. Appropriate privacy and safety settings will be used to manage access and interactions. This includes:
 - **limiting chat functions,**
 - **not permitting children to share screens**
 - **children cannot access the Google chat without a teacher being present.**
14. When live streaming in a Google Meet with children:
 - contact will be made via children's **school** provided Google accounts **and** logins.
 - staff will **mute** children's microphones until children are invited to talk.
 - at least 2 members of staff will be present, If this is not possible, SLT approval will be sought.
15. Live 1:1 sessions will only take place with approval from the **headteacher and with a parent / appropriate adult present with the child.**
16. A pre-agreed **invitation** detailing the session expectations will be sent to those invited to attend.
 - Access links should not be made public or shared by participants.
 - Children and parents/carers should not forward or share access links.
 - If children or parents/carers believe a link should be shared with others, they will discuss this with the member of staff running the session first
 - Children are encouraged to attend lessons in a shared/communal space or room with an open door and/or when appropriately supervised by a parent/carer or another appropriate adult.
17. Alternative approaches **and/or** access will be provided to those who do not have access.

Behaviour expectations

18. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.
19. All participants are expected to behave in line with existing **school** policies and expectations. This includes
 - Appropriate language will be used by all attendees.
 - Staff will not take or record images for their own personal use.
 - Parents cannot record events for their own use.
 - Consideration will be made to the location of remote learning sessions to protect the privacy of all.
20. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.
21. When sharing videos and/or live streaming, participants are required to:
 - **wear appropriate dress.**
 - **ensure backgrounds of videos are neutral (blurred if possible).**
 - **ensure that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds.**
22. Educational resources will be used or shared in line with our existing teaching and learning policies, taking licensing and copyright into account.

Policy Breaches and Reporting Concerns

23. Participants are encouraged to report concerns during remote **and/or** live-streamed sessions. Children and parents can speak to their class teacher or any DSL or the Headteacher about any concerns.
24. If inappropriate language or behaviour takes place, participants involved will be removed by staff, the session may be terminated, and concerns will be reported to **the Headteacher**

25. Inappropriate online behaviour will be responded to in line with existing policies such as acceptable use of policies, allegations against staff, anti-bullying and behaviour.
26. Sanctions for deliberate misuse may include **but are not limited to: restricting/removing use, contacting police if a criminal offence has been committed.**
27. Any safeguarding concerns will be reported to **Sharmila Desai**, Designated Safeguarding Lead, in line with our child protection policy.

I have read and understood Sissinghurst CE (VA) Primary School Acceptable Use Policy (AUP) for remote/online learning.

Staff Member Name:

Date.....