St James' CE Primary School
Early Years and Key Stage 1 Acceptable Use of Technology Policy 2026

- 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 only click on things online when I know what they do. If I am not sure, I ask an adult first.
- 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 and tablets including when I am using Microsoft 365 when I am 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 parents/carers will be told
    - I may not be able to use technology and the internet in the future
- I have read and talked about these rules with my parents/carers.

St James' CE Primary School
Key Stage 2 Acceptable Use of Technology Policy 2026

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 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 a trusted adult says they are safe.
- I know that people online might not be who they say they are. I will only chat with people I know or who a trusted adult says are safe.
- If someone online asks to meet me, I will tell a trusted adult straight away.
- I will protect myself by not telling anyone I meet online my address, my telephone number, my school name or by sending a picture of myself without permission from a teacher or other adult.
- I will always be myself and not pretend to be anyone or anything I am not. I know that posting anonymous messages or pretending to be someone else is not allowed.

Learning (including remote/online learning)

- I always ask permission from an adult before using the internet.
- I only use websites, tools and/or 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. I understand that:
    - remote learning will only take place using Microsoft 365 and during usual school times.
    - My use of Microsoft 365 is monitored to help keep me safe. If my teacher is recording a session, they will have permission from Mr Tutt or Miss Hayward and my parents/carers. The recording will be kept safely and securely and only seen by St James' staff.
- Only members of St James' CE Primary School community can access Microsoft 365.
    - I will only use my school provided email accounts to access remote learning.
    - I will use privacy settings as set up by the school.
    - I will not share my login/password with others.
    - I will not share any access links to remote learning sessions with others.

- When taking part in remote learning I will behave as I would in the classroom. This includes:

- Using appropriate language.
- Not taking or recording images/content without agreement from the teacher and those featured.
- Being polite and friendly at all times.

- When taking part in live sessions I will:
  - Mute my video and microphone. My teacher will control if/when my video and/or microphone are unmuted.
  - Wear appropriate clothing e.g. my school uniform.
  - Ensure backgrounds of videos are neutral and personal information/content is not visible.
  - Use appropriate alternative backgrounds if my teacher gives permission.
  - Attend lessons in a suitable shared/communal space or room and supervised by a parent/carer or another appropriate adult.

Trust

- 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 trusted adult.
- I always credit the person or source that created any work, images, or text I use.
- I will use Artificial Intelligence (AI) tools safely and sensibly. I won't use them to cheat, copy other people's work, or say anything unkind. I know that AI tools can sometimes make mistakes. I will only use them when a teacher or trusted adult says it's okay.

Responsible

- I keep my personal information safe and private online.
- I will keep my passwords safe and will not share them and I will log off when I have finished using a computer or device.
- 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.
- I will use all devices and technology in a sensible way that does not damage equipment, including when moving around school. I will not plug/unplug devices without adult supervision.
- I will not use or try to use personal email, social networking sites or instant messaging whilst in school.
- I know that being responsible means that I should not look for bad language, inappropriate images or violent or unsuitable games, and that if I accidently come across any of these, I should report it to a teacher or adult in school, or a parent or carer at home.

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 owned devices and networks are checked/monitored to help keep me safe, even if I use them at home. This means someone at the school may be able to see

and/or check my activity when I use school devices and/or networks if they are worried about my or anyone else's safety or behaviour.

- If, for any reason, I need to bring a personal device, like a mobile phone and/or other wearable technology into school I know that it is to be switched off, handed in to my teacher and then collected at the end of the school day. I know that I need a letter from Mr Tutt or Miss Hayward before this is allowed. I will not use my mobile phone or smart device whilst at school unless I have permission from Mr Tutt or Miss Hayward.
- I know that smart devices are only allowed in some very occasional circumstances e.g. for medical needs, which are agreed in writing by Mr Tutt or Miss Hayward
- 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.
- I know that if I do not follow the school rules then:
    - My parents will be informed
    - I may not be allowed access to technology and the internet in the future
    - I may lose some of my playtime

Tell

- If I see anything online that I should not or that makes me feel worried or upset, I will use a screen cover tool or minimise the page, turn off the monitor (if able) and tell an adult straight away.
- If I am aware of anyone being unsafe with technology, I will report it to a teacher, parent/carer or trusted adult immediately.
- I know it is not my fault if I see something upsetting or unkind online.
- If I'm not sure about something online or it makes me feel worried or scared, I will talk to a trusted adult.
- If I get unpleasant, rude, or bullying emails or messages, I will report them to a teacher or other adult. I will not delete them straight away, but instead, keep them so I can show them to the person I am reporting it to.

St James' CE 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).

I agree to follow the AUP when:

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

Name……. Signed…….……...….

Class…….…… Date…….

Parent/Carer's Name……...…….....

Parent/Carer's Signature…….…….

Date……

Pupils with Special Educational Needs and Disabilities (SEND)

Please note, these are sample statements to be adapted for the needs of individual children.

Learners with SEND functioning at Levels P4 –P7

- I ask a grown-up if I want to use the computer.
- I make good choices on the computer.
- I use kind words on the internet.
- If I see anything that I do not like online, I tell a grown up.
- I know that if I do not follow the school rules then:
    - My parents will be informed
    - I may not be allowed access to technology and the internet in the future
    - I may lose some of my playtime

Learners with SEND functioning at Levels P7-L1 (Based on Childnet's SMART Rules)

Safe

- I ask a grown up if I want to use the computer.
- I do not tell strangers my name on the internet.
- I know that if I do not follow the school rules then:
    - My parents will be informed
    - I may not be allowed access to technology and the internet in the future
    - I may lose some of my playtime

Meeting

- I tell a grown-up if I want to talk on the internet.

Accepting

- I do not open messages or emails from strangers.

Reliable

- I make good choices on the computer.

Tell

- I use kind words on the internet.
- If I see anything that I do not like online, I will tell a grown up.

Learners with SEND functioning at Levels L2-4 (Based on Childnet's SMART Rules)

Safe

- I ask an adult if I want to use the internet.
- I keep my information private on the internet.
- I am careful if I share photos online.
- I know that if I do not follow the school rules then:
  - My parents will be informed
  - I may not be allowed access to technology and the internet in the future
  - I may lose some of my playtime

Meeting

- I tell an adult if I want to talk to people on the internet.
- If I meet someone online, I talk to an adult.

Accepting

- I do not open messages from strangers.
- I check web links to make sure they are safe.

Reliable

- I make good choices on the internet.
- I check the information I see online.

Tell

- I use kind words on the internet.
- If someone is mean online, then I will not reply. I will save the message and show an adult.
- If I see anything online that I do not like, I will tell a teacher.

St James' CE Primary School
Parent/Carer Acceptable Use of Technology Policy Acknowledgement 2026

1. I have read and discussed St James' CE Primary School pupil acceptable use of technology policy (AUP) with my child and understand that the AUP will help keep my child safe online.

2. I understand that the AUP applies to my child's use of school devices and systems on site and at home including school Microsoft 365 accounts, and personal use where there are safeguarding and/or behaviour concerns. This may include if online behaviour poses a threat or causes harm to another pupil, could have repercussions for the orderly running of the school, if a pupil is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school.

3. I understand that any use of school devices and systems are appropriately filtered; this means that the school's internet provider blocks access to sites which could promote or include harmful and/or inappropriate behaviour or material.

4. I am aware that my child's use of school provided devices and systems will be monitored for safety and security reasons, when used on and offsite. This includes physical monitoring via supervision, and monitoring internet and web access. Monitoring approaches are in place to keep my child safe and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

5. I understand that the school will take every reasonable precaution, including implementing appropriate monitoring and filtering systems as above, to ensure my child is safe when they use school devices and systems, on and offsite. I however understand that the school cannot ultimately be held responsible for filtering breaches that occur due to the dynamic nature of materials accessed online, or if my child is using a personal device, including mobile or smart technologies.

6. I am aware that the school mobile and smart technology policy states that my child cannot use personal device and mobile and smart technology on site. If, for any reason, my child needs to bring a personal/smart device or mobile phone into school I will seek written permission from Mr Tutt or Miss Hayward. If given permission to bring a mobile phone or smart device to school, they know that it is to be switched off, handed in to their teacher and then collected at the end of the school day.

7. I understand that my child needs a safe and appropriate place to access remote/online learning, for example, if the school is closed. I will ensure my child's access to remote/online learning is appropriately supervised and any use is in accordance with the school remote learning AUP.

8. I, and my child are aware of the importance of safe online behaviour and will not deliberately upload or share any content that could upset, threaten the safety of or offend any member of the school community, or content that could adversely affect the reputation of the school.

9. I understand that the school will contact me if they have concerns about any possible breaches of the AUP or have any concerns about my child's safety online.

10. I will inform the school (for example speaking to a member of staff and/or the Designated Safeguarding Lead) or other relevant organisations if I have concerns over my child's or other members of the school community's safety online.

11. I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet, both in and out of school.

12. I understand my role and responsibility in supporting the school's online safety approaches and safeguarding my child online. I will use parental controls, supervise access and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding.

Child's Name…….

Class……..…… Date……..…….

Parent/Carer's Name…….....

Parent/Carer's Signature…….. Date…….

St James' CE Primary School
Staff Acceptable Use of Technology Policy 2026

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use St James' CE 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 St James' CE Primary 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 St James' CE Primary School both professionally and personally, both on and offsite. This may include use of laptops, 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 St James' CE Primary School Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school child protection policy, staff code of conduct and remote 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 staff behaviour 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 of setting IT systems and/or devices by staff is allowed however this should be outside of teaching hours and not in the presence of pupils. This use is at the school's discretion and can be revoked at any time.

6. Where I deliver or support remote/online learning, I will comply with the school remote/online learning AUP.

Data and system security

7. 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 use a 'strong' password to access school systems. A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system. Passwords should be regularly changed.
    - I will protect the devices in my care from unapproved access or theft for example by not leaving devices visible or unsupervised in public places.

8. I will respect school system security and will not disclose my password or security information to others.

9. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the IT system manager.

10. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT system manager.

11. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including UK GDPR 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.

- Any data being shared online, such as via cloud systems or artificial intelligence tools (AI), will be suitably risk assessed and approved by the school Data Protection Officer and leadership team prior to use to ensure it is safe and legal.

12. 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 my school Microsoft 365 account to upload any work documents and files in a password protected environment or school approved/provided VPN.

13. 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.

14. 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.

15. I will not attempt to bypass any filtering and/or security systems put in place by the school.

16. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to a Computing Lead (Adele Smith/Jez Stevens) or IT Technician as soon as possible.

17. If I have lost any school related documents or files, I will report this to the Computing Lead (Jez Stevens) or IT Technician and school Data Protection Officer (Satswana) as soon as possible.

18. Any images or videos of pupils will only be used as stated in the school camera and image use policy which can be found on our school website. I understand images of pupils must always be appropriate and should only be taken with school provided equipment and only be taken/published where pupils and/or parent/carers have given explicit written consent.

Classroom practice

19. I understand that it is part of my roles and responsibilities to ensure that appropriate filtering and monitoring is implemented by St James' CE Primary School as detailed in child protection policy, and as discussed with me as part of my induction and/or ongoing safeguarding and child protection staff training.

20. If there is failure in the filtering software or abuse of the filtering or monitoring systems, for example, I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material, I will report this to the DSL and IT technician, in line with the school child protection policy.

21. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed in the school's child protection policy, remote learning AUP

22. I am aware that generative artificial intelligence (AI) tools may have many uses which could benefit our school community. However, I also 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, its use can pose moral, ethical and legal concerns if not carefully managed. As such, I understand that:
    - AI tools are only to be used responsibly and ethically, and in line with our school Child Protection, data protection, behaviour and Staff Code of Conduct policy expectations.
    - A risk assessment will be undertaken, and written approval will be sought from the senior leadership team prior to any use of AI tools, for example if used in the classroom, or to support lesson planning in line with the school's AI Policies.
    - A Data Protection Impact Assessment (DPIA) will always be completed prior to any use of AI tools that may be processing any personal, sensitive or confidential data and use will only occur following approval from the DPO.
    - I am required to critically evaluate any AI-generated content for accuracy, bias, and appropriateness before sharing or using it in educational contexts.
    - AI must not be used to replace professional judgement, especially in safeguarding, assessment, or decision-making involving pupils.
    - Only approved AI platforms may be used with pupils. Pupils must be supervised when using AI tools, and I must ensure age-appropriate use and understanding prior to use.
    - Any misuse of AI will be responded to in line with relevant school policies, including but not limited to, anti-bullying, staff and pupil behaviour and child protection.

23. I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:
    - exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used.
    - creating a safe environment where pupils feel comfortable to report concerns and say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.
    - involving the Designated Safeguarding Lead (DSL) (Sarah Greenfield) or a deputy (Penny Wardell, Lucy Hayward, John Tutt, Kate Jones or Lucy Coward) as part of planning online safety lessons or activities to ensure support is in place for any pupils who may be impacted by the content.
    - Informing the DSL and/or leadership team if I am teaching topics which could create unusual activity on the filtering logs, or if I believe the filtering system is placing unreasonable restrictions on teaching, learning or administration.
    - make informed decisions to ensure any online safety resources used with pupils is appropriate.

24. 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.

Mobile devices and smart technology

25. I have read and understood the school mobile and smart technology and social media policies which addresses use by pupils and staff.

26. I will ensure that my use of mobile devices and smart technology is compatible with my professional role, does not interfere with my work duties and takes place in line with the staff code of conduct, child protection policy, mobile and smart technology policy and social media policy.

Online communication, including use of social media

27. I will ensure that my use of communication technology, including use of 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 code of conduct, social media policy and the law.

28. As outlined in the staff code of conduct and social media section of the school online safety policy:
    - I will take appropriate steps to protect myself and my reputation, and the reputation of the school, online when using communication technology, including the use of social media.
    - I will not discuss or share data or information relating to pupils, staff, school business or parents/carers on social media.

29. My electronic communications with current and past pupils 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 approved and/or provided communication channels and systems, such as a school email address, user account or telephone number.
    - I will not share any personal contact information or details with pupils, such as my personal email address or phone number.
    - I will not add or accept friend requests or communications on personal social media with current or past pupils and/or their parents/carers.
    - If I am approached online by a current or past pupils or parents/carers, I will not respond and will report the communication to my line manager and (Lucy Hayward) Designated Safeguarding Lead (DSL).
    - Any pre-existing relationships or situations that compromise my ability to comply with the AUP or other relevant policies will be discussed with the DSL or headteacher.

Policy concerns

30. I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.

31. I will not attempt to access, create, transmit, display, publish or forward any material or content online that may be harmful, inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.

32. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school into disrepute.

33. I will report and record any concerns about the welfare, safety or behaviour of pupils or parents/carers online to the DSL in line with the school child protection and online safety policies.

34. I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher, in line with school child protection policy and the allegations against staff policy.

Policy Compliance and Breaches

35. If I have any queries or questions regarding safe and professional practise online, either in school or off site, I will raise them with the DSL or the headteacher.

36. I understand that the school may exercise its right to monitor the use of its devices information systems to monitor policy compliance and to ensure the safety of pupils 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.

37. I understand that if the school believe 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 code of conduct.

38. I understand that if the school believe that unprofessional or inappropriate online activity, including behaviour which could bring the school into disrepute, is taking place online, the school may invoke its disciplinary procedures as outlined in the staff code of conduct.

39. I understand that if the school suspects criminal offences have occurred, the police will be informed.

I have read, understood and agreed to comply with St James' CE 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: ……

St James' CE Primary School
Visitor and Volunteer Acceptable Use of Technology Policy 2026

As a professional organisation with responsibility for safeguarding, it is important that all members of the community, including visitors and volunteers, are aware of our behaviour expectations and their professional responsibilities when using technology.

This AUP will help St James' CE Primary School ensure that all visitors and volunteers understand the school's expectations regarding safe and responsible technology use.

Policy scope

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services, either provided to me by the school or accessed by me as part of my role within St James' CE Primary School, professionally and personally. This may include my use of devices such as laptops, mobile phones, tablets, digital cameras, as well as IT systems and networks, email data and data storage, remote learning systems and communication technologies.

2. I understand that St James' CE Primary School AUP should be read and followed in line with the school staff code of conduct.

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 code of conduct 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, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.

5. I will not attempt to access, create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.

6. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school into disrepute.

Data and image use

7. I will ensure that any access to personal data is kept in accordance with Data Protection legislation, including UK GDPR.

8. I understand that I am not allowed to take images or videos of pupils without permission from the headteacher or deputy headteacher. If permission is granted, any images or videos of pupils will only be taken in line with the school image use policy which can be found on the school website.

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 pupils, and evaluation of websites, tools and apps before use in the classroom or recommending for home learning. For more information see Section 7.1 of our school Online Safety Policy which can be found on the school website.

10. Where I deliver or support remote/online learning, I will comply with the school remote/online learning AUP.

11. I will support staff in reinforcing safe behaviour whenever technology is used on site and I will promote online safety with the pupils in my care.

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 DSL and IT technician, 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.

Use of mobile devices and smart technology

14. In line with the mobile and smart technology sections of the school child protection policy, I understand that...
    - Mobile phones and personal/smart devices are only permitted to be used in the school office waiting area, unless permission is granted by a member of the Senior Leadership Team for use for a specific purpose, for example as part of multi-agency working arrangements.
    - Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use mobile and smart technology in accordance with our staff acceptable use of technology policy and other associated policies including child protection, image use and online safety.

Online communication, including the use of social media

15. I will ensure that my online reputation and use of technology and is 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.

- I will take appropriate steps to protect myself online as outlined in the child protection and online safety policy, which can be found on our school website.
- I will not discuss or share data or information relating to pupils, staff, school business or parents/carers on social media.
- I will ensure that my use of technology and the internet will not undermine my role, interfere with my duties and will be in accordance with the school code of conduct policy and the law.

16. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
    - All communication will take place via school approved communication channels such as via a school provided email address, account or telephone number.
    - Communication will not take place via personal devices or communication channels such as via my personal email, social networking account or mobile phone number.
    - Any pre-existing relationships or situations that may compromise my ability to comply with this will be discussed with the DSL (Sarah Greenfield) or deputy DSL (Lucy Hayward, John Tutt, Penny Wardell, Kate Jones or Lucy Coward).

Policy compliance, breaches or concerns

17. 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 (Sarah Greenfield), deputy DSL (Lucy Hayward, John Tutt, Penny Wardell, Lucy Coward or Kate Jones) or the headteacher.

18. I understand that the school may exercise its right to monitor the use of its devices information systems to monitor policy compliance and to ensure the safety of pupils 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.

19. I will report and record concerns about the welfare, safety or behaviour of pupils or parents/carers online to the Designated Safeguarding Lead (Sarah Greenfield) or deputy DSL (Lucy Hayward, John Tutt, Penny Wardell, Kate Jones or Lucy Coward) in line with the school child protection policy.

20. I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher, in line with the allegations against staff policy.

21. I understand that if the school believes that unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour is taking place online, the school may invoke its disciplinary procedures.

22. I understand that if the school suspects criminal offences have occurred, the police will be informed.

I have read, understood and agreed to comply with St James' CE 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)……

St James' CE Primary School
Wi-Fi Acceptable Use of Technology Policy 2026

As a professional organisation with responsibility for children's safeguarding it is important that all members of the school community are fully aware of the school boundaries and requirements when using the school Wi-Fi systems and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

This is not an exhaustive list, and all members of the school community are reminded that technology use should be consistent with our ethos, other appropriate policies, and the law.

1. The school provides Wi-Fi for the school community and allows access for education use only. Visitors and volunteers will only be given access for specific purposes (agreed by SLT), should not use the school Wifi for any other purpose, should not save the Wifi password to a non-school device and should log out once the purpose is served.

2. I am aware that the school will not be liable for any damages or claims of any kind arising from the use of the wireless service. The school takes no responsibility for the security, safety, theft, insurance, and ownership of any device used within the school premises that is not the property of the school.

3. The use of technology falls under St James' CE Primary Acceptable Use of Technology Policy (AUP), child protection policy and behaviour policy which all pupils /staff/visitors and volunteers must agree to and comply with.

4. The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.

5. School owned information systems, including Wi-Fi, must be used lawfully; 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.

6. I will take all practical steps necessary to make sure that any equipment connected to the school service is adequately secure, such as up-to-date anti-virus software, systems updates.

7. The school wireless service is not secure, and the school cannot guarantee the safety of traffic across it. Use of the school wireless service is done at my own risk. By using this

service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. I confirm that I knowingly assume such risk.

8. The school accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the school wireless service's connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.
9. I will respect system security; I will not disclose any password or security information that is given to me. To prevent unauthorised access, I will not leave any information system unattended without first logging out or locking my login as appropriate.
10. I will not attempt to bypass any of the school security and filtering systems or download any unauthorised software or applications.
11. My use of school Wi-Fi will be safe and responsible and will always be in accordance with the school AUP and the law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.
12. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.
13. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead (Sarah Greenfield) or deputy DSL (Lucy Hayward, John Tutt, Penny Wardell, Kate Jones or Lucy Coward) as soon as possible.
14. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead (Sarah Greenfield) or deputy DSL (Lucy Hayward, John Tutt, Penny Wardell, Kate Jones or Lucy Coward).
15. I understand that my use of the school Wi-Fi may be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the school suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school may terminate or restrict usage. If the school suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agreed to comply with St James' CE Primary School Wi-Fi Acceptable Use Policy.

Name ……..…...

Signed: …….....Date (DDMMYY)……..

St James' CE Primary School
Staff Remote/Online Learning Acceptable Use of Technology Policy 2026

The Remote/Online Learning Acceptable Use Policy (AUP) is in place to safeguarding all members of school St James' CE 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 using Microsoft 365.
    - Microsoft 365 has been assessed and approved by the SLT team.

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 Lucy Hayward, Deputy Headteacher/Deputy DSL, John Tutt, Headteacher/Deputy DSL or Sarah Greenfield (Assistant Headteacher/Lead DSL).
    - Staff will use work provided equipment where possible e.g. a school laptop or tablet.

3. Online contact with pupils and/or parents/carers will not take place outside of the operating times as defined by SLT:
    - Monday – Friday 8am – 5pm
4. All remote/online sessions will be formally timetabled; a member of SLT or DSL is able to drop in at any time.
5. Live streamed remote/online learning sessions will only be held with approval and agreement from the headteacher/a member of SLT.

Data Protection and Security

6. Any personal data used by staff and captured by Microsoft 365 when delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy, which can be found on our school website.

7. Email communication with multiple parents will be sent via Arbor so that email addresses and/or names are not disclosed to other recipients.

8. All remote/online learning and any other online communication will take place in line with current school confidentiality expectations as outlined in the staff code of conduct policy.
9. All participants will be made aware that Microsoft 365 can record activity. Before any recordings are made, consent will be obtained from SLT and parents/carers. The recording will be saved in the Remote Learning folder on StaffPublic which is only accessed by staff and recordings will be deleted after 30 days.
10. Staff will not record lessons or meetings using personal equipment under any circumstance.
11. Only members of the St James' CE Primary School community will be given access to Microsoft 365.
12. Access to Microsoft 365 will be managed in line with current IT security expectations as outlined in our Online Safety Policy and Staff Acceptable Use Policy

Session management

13. Staff will record the length, time, date, and attendance of any sessions held. This will be recorded through Microsoft 365 Teams or on the Remote Learning Record document and stored in the Remote Learning Folder on StaffPublic.

14. Appropriate privacy and safety settings will be used to manage access and interactions. This includes:
    - language filters,
    - disabling chat where possible and monitoring where not,
    - staff not permitting learners to share screens,
    - keeping meeting IDs private,
    - use of waiting rooms/lobbies or equivalent.

15. When live streaming with pupils:
    - contact will be made via pupils **school** provided email accounts **and/or** logins.
    - staff will **mute** pupils videos and microphones unless pupil participation is required.
    - at least 2 members of staff will be present or SLT will be able to 'drop in' unannounced to any session

16. Live 1 to 1 sessions will only take place with approval from the headteacher/a member of SLT. If these are permitted, a parent/carer must give consent, be present in the room if possible (however, this may not be appropriate if providing counselling or safeguarding support) and the session must be auditable either by making a recording or by a member of the SLT team being present.

17. A pre-agreed email, which has been approved by the SLT, detailing the session expectations will be sent to those invited to attend.
    - Access links should not be made public or shared by participants.
    - Pupils and/or parents/carers should not forward or share access links.

- Pupils are encouraged to attend lessons in a shared/communal space or room with an open door and when appropriately supervised by a parent/carer or another appropriate adult.

18. Alternative approaches and/or access will be provided to those who do not have access.

Behaviour expectations

19. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.

20. 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.
    - Other attendees cannot record events for their own use.

21. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.

22. 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.

23. 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

24. Participants are encouraged to report concerns during remote **and/or** live-streamed sessions:
    - Pupils should report concerns to the member of staff running the session or tell a parent/carer/trusted adult.

25. 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 a member of the SLT team.

26. Inappropriate online behaviour will be responded to in line with existing policies such as acceptable use of technology, allegations against staff, anti-bullying and behaviour.

27. Sanctions for deliberate misuse may include contacting parents, restricting/removing use, and/or contacting police if a criminal offence has been committed.

28. Any safeguarding concerns will be reported to our Designated Safeguarding Lead (Sarah Greenfield) or deputy DSL (Lucy Hayward, John Tutt, Penny Wardell, Kate Jones or Lucy Coward) in line with our child protection policy.

I have read and understood the St James' CE Primary School Acceptable Use Policy (AUP) for remote/online learning.

Staff Member Name: ……

Date……

Acknowledgements and Thanks

This document has been produced by LADO Education Safeguarding Advisory Service.

Additional thanks to members of the Kent Education Online Safety Strategy Group, the UK Safer Internet Centre, South West Grid for Learning (SWGfL), London Grid for Learning (LGfL), South East Grid for Learning (SEGfL), Childnet, CEOP, The Judd School, Kingsnorth Primary School, Loose Primary School, Peter Banbury, Kent Police, Kent Schools Personnel Service (SPS), Kent Legal Services and Kent Libraries and Archives, for providing comments, feedback and support on previous versions.