Acceptable Use of Technology Policy

Ratified by Full Governing Body Governor: October 2026

Draft Prepared	October 2026
Date Agreed	October 2026
Signed by Headteacher	N.Hirst
Signed (Chair of Governors)	K.Bell
Date Policy to be Reviewed	October 2028
VERSION CONTROL: Updated to adhere to the most recent KCSIE and EYFS Statutory Framework.	

This document provides a framework to enable us to ensure that all of our children, regardless of background or circumstances, fulfil their potential within our Christian community. The school Christian Values of Respect, Friendship, Perseverance, Forgiveness, Compassion and Trust are applied when following this policy, and we will use this guidance to ensure that our children will be fully prepared for the future, with high self-esteem and having forged strong and respectful relationships with other people.

We want our children to be fully prepared for God's ever changing world.

Acceptable Use of Technology Policy (AUP)

The content and structure of this policy reflects the relevant guidance in Keeping Children Safe in Education and the Early Years Foundation Stage statutory framework. This AUP should be read alongside our Mobile Phone and Smart Device policy, Social Media policy, Staff Code of Conduct, Child Protection policy, Data Protection and Freedom of Information policy and Remote Learning Policy.

Filtering and Monitoring

Filtering and monitoring should be understood as part of the setting's wider safeguarding arrangements, rather than solely as a technical function. The filtering and monitoring provision is reviewed annually, and staff know how to report safeguarding or technical concerns with regard to filtering and monitoring.

Our approach to filtering and monitoring is:

- Age and ability appropriate
- Proportionate to our unique context
- Helps protect our children and staff from illegal, inappropriate and harmful content without unreasonably restricting teaching, learning and/or access to appropriate support.

Filtering and monitoring arrangements apply to Ashford St Mary's-provided devices, networks, cloud-based services, apps, mobile devices and any approved use of artificial intelligence tools. Where monitoring identifies potential safeguarding, behavioural, data protection or technical concerns, these are responded to in line with our existing child protection, behaviour, staff conduct and data protection policies and procedures.

- Meeting digital and technology standards in schools and colleges - Filtering and monitoring: core standard - GOV.UK
- Appropriate Filtering and Monitoring Guidance - UK Safer Internet Centre
- Filtering and monitoring - Questions for governors, proprietors and trustees - UK Safer Internet Centre
- Filtering and Monitoring Webinars - SWGfL

Mobile Phones and smart devices: screen use

For the purposes of this policy, mobile phones and smart technology may include smartphones, smart watches, tablets, wearable technology, devices with cameras, recording or communication functions, and any other device capable of accessing the internet, sending or receiving messages, capturing images, audio or video, or using apps and online services.

This AUP reflects our Mobile Phone and Smart Devices Policy and the Department for Education's "Mobile phones in schools" guidance, which states that schools should be mobile phone-free environments by default and should prohibit pupil use of mobile phones and similar smart technology throughout the school day, including lessons, time between lessons, breaktimes and lunchtime. Any exceptions or reasonable adjustments need to be agreed by the Headteacher, risk assessed, communicated and recorded.

Smart technology and mobile devices at Ashford St Mary's are used to support learning, development, communication and/or care needs. It is therefore planned, purposeful, age appropriate and supervised. Screen use should not replace face-to-face interaction, play, physical activity, rest, care routines or real-world exploration. This aligns with the EYFS 2026 framework and DfE guidance.

Staff should model safe, responsible and professional use of technology, and any use of personal or setting-provided devices must not compromise supervision, safeguarding, confidentiality, data protection, professional boundaries or the learning environment.

Where staff are permitted to use personal devices on site, our Mobile Phone and Smart Devices policy details the clear expectations about where, when and how devices may be used, including expectations for storage, notifications, camera use, recording functions, wearable technology and communication with children and their family.

Use of Artificial Intelligence (AI)

Children - at school using a school device

Our children are **unable** to **interact** with AI at school. Ashford St Mary's Primary School is 1 of the 32,000 schools and colleges who use Google Education throughout the school. Since the beginning of 2026 all 'answers' to all Google 'searches' give a Google Gemini (AI model) overview of the answer. This is, and has been, the case for anyone in the world using Google on any device. The 'AI overview' feature cannot be 'turned off'. It is, and has been, the choice of the user* whether or not they interact with Google Gemini (AI) further on the subject of their initial question or search. **Children under the age of 13 who use Google Education whilst at school DO NOT have the choice to interact with Google Gemini (AI) or not - it is deactivated by Google for users of this age.*

Google Education complies with ***Keeping Children Safe in Education and Data Protection law***. Our filtering and monitoring system immediately recognises any search of an inappropriate nature and alerts members of our senior leadership team immediately.

Staff

Generative artificial intelligence (AI) tools can support teaching, learning, communication and administrative tasks when used safely, lawfully and appropriately. Any use of AI tools should adhere to data protection laws and safeguarding expectations, and be limited to tools that comply with the **Department for Education (DfE) Generative AI Product Safety Standards and Expectations**. AI tools such as **'TeachmateAi'** and **'SLTai'**, are compliant with DfE Guidance because they feature UK/EU data storage, UK GDPR and DPA 2018 compliance and a policy of not using inputted data to train AI models.

Staff should be aware that AI can produce inaccurate or biased content. Proofreading and fact checking against approved and reputable curriculum planning resources is essential before using any other resources to plan and deliver lessons. At Ashford St Mary's Primary School, AI tools must not replace professional judgement, safeguarding decision-making, assessment decisions or direct support for children from staff.

The following links may also provide further information:

- Generative artificial intelligence (AI) in education - GOV.UK
- Using AI in education settings: support materials - GOV.UK
- Generative Artificial intelligence (AI) and data protection in schools - Guidance - GOV.UK
- Artificial Intelligence and Online Safety | SWGfL
- Using artificial intelligence (AI) safely | Internet Matters
- A Safeguarding First Approach to adopting Gen-AI in schools | LGFL

Acceptable use of Social Media

At the time of publication, national policy and legislation relating to children's use of social media and online services continues to develop. We therefore, will not present proposed changes as current legal requirements until they are in force. We will monitor national DfE guidance to ensure that our social media, mobile technology and acceptable use policies remain accurate and up to date. Please see our separate Social Media policy 2026 for the most up-to-date information.

It is our expectation that the parents/carers and other adults' online behaviour and communications about Ashford St Mary's Primary School is consistent with our School Christian values. Our complaints procedure and our response to other concerns that parents/carers may have is done so as quickly as possible. If you have a concern, come and speak to us. Posting on social media will never help solve a problem.

We will have regard to the DfE's guidance, *Preventing and tackling bullying and harassment of school staff* and the LESAS *Responding to Complaints, Bullying and Harassment on Social Media*. Both of which set out the expectations for preventing and responding to bullying, harassment and intimidation of school staff, including online. We will respond fairly, calmly and proportionately to concerns shared online, while ensuring that legitimate criticism, complaints and safeguarding reports can still be raised through appropriate routes.

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

- I understand that the Ashford St Mary's Primary School Acceptable Use Policy will help keep me safe and happy when I go online.
- I only go online when an adult is with me.
- I check with an adult 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 that Ashford St Mary's Primary School can see what I am doing online when I use school computers, tablets, Google Drive, Google Classroom and any learning apps, when I am at home.
- I know that if I do not follow our school values whilst online that a consequence will be given
- I can visit www.thinkuknow.co.uk and https://www.ceopeducation.co.uk/ and https://www.bbc.co.uk/bitesize/topics/zfcvhbk/articles/zkcj92p to learn more about keeping safe online.

Key Stage 2 (Age 7-11)

I understand that the Ashford St Mary's Primary 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 when I am in school.
- I will only share pictures or videos online if they are safe, kind and I have asked permission.
- 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 to online.
- If someone online asks to meet me, I WILL TELL A SAFE ADULT IMMEDIATELY.

Learning

- I follow the Ashford St Mary's Primary School rules about mobile phones and smart device/technology
- I always ask permission from an adult before going online
- 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 school learning Acceptable Use Policy.

True

- I know that some things or people online might not be honest or truthful.
- If I'm unsure if something online is true, I will check 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 not put personal information about me or anyone else into AI tools.
- I will not use AI to make fake images, sounds, 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 makes me feel worried, upset, or frightened, I will minimise the screen and tell an adult immediately
- If I am aware of anyone being unkind or unsafe with technology, I will report it to an adult at home and/or at school.
- 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 Ashford St Mary's Primary 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 owned devices and networks are checked/monitored to help keep me safe, even if I use them at home. This means someone at school may be able to see and/or check my online activity when I use a school device or network e.g. Google Classroom if they are worried about my or anyone else's safety or behaviour.
- If I bring a mobile phone or other device to school, I will follow the rules. I know that it has to be turned off and put in the Mobile Device Box in my classroom and then collected at the end of the school day. I will not use it during the school day unless a member of staff has agreed to this.
- 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 these rules that:
    - Adults in school will investigate and give a consequence

Shortened KS2 version (for use on posters)

- I ask a teacher 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.
- I know my use of school devices and systems can be monitored.

Learners with SEND functioning at Levels P4 –P7

(Based on Childnet's SMART Rules)

- I only use phones, tablets or computers when a grown-up says it is okay.
- I make good choices on the computer.
- I use kind words on the internet.
- I tell a grown-up if I see or hear something online that upsets me.

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 a phone, tablet or computer.
- I do not tell strangers my name on the internet.
- I know that if I do not follow the rules there will be a consequence.

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 online that worries me, 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 use phones, tablets or computers when an adult says it is okay.
- I keep my information private on the internet.
- I ask an adult before I take or share a photo, video or message.
- I know that if I do not follow the rules there will be a consequence.

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.

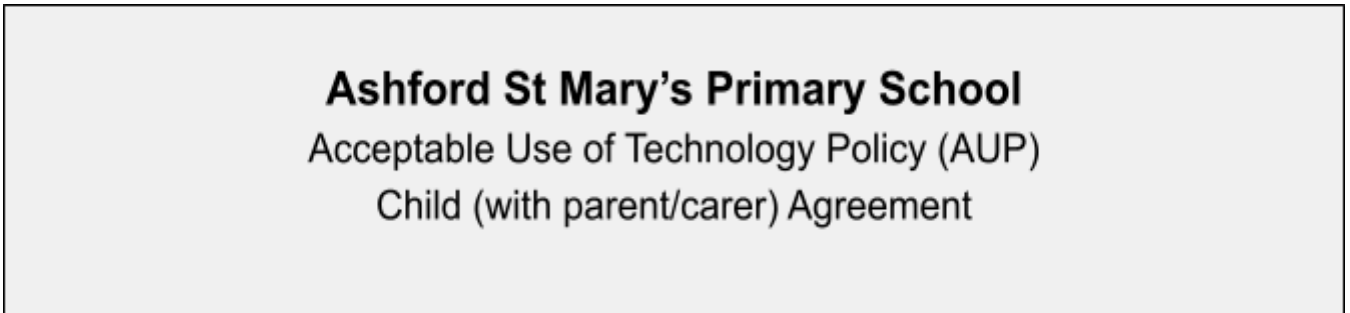
Reliable

- 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 worries or upsets me, I will tell an adult at home or school.

Ashford St Mary's Acceptable Use of Technology Policy - Child Agreement



Ashford St Mary's Acceptable Use of technology Policy Acknowledgement

Parent/Carer agrees that:

1. I have received and read the Ashford St Mary's Primary School Acceptable Use of Technology Policy (AUP) and have discussed its 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-provided devices, accounts, systems and internet access;
    - school-provided technology away from the setting;
    - 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. The school has provided information about its filtering and monitoring arrangements at the start of this policy.

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/phase leader/SLT], 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 seek online safety information or support from the school by contacting the Family Liaison Officer.

I acknowledge that I have received and read the Ashford St Mary's Primary School Acceptable Use of Technology Policy and have discussed its expectations with my child.

Child's name: .....

Class: .....

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 staff are expected to use technology in a professional, lawful, ethical and responsible manner.

This Staff Acceptable Use of Technology Policy (AUP) sets out our expectations for safe technology use, professional conduct, safeguarding, data protection and system security. It is not intended to unduly limit appropriate teaching, learning or professional use of technology, but to help protect children, staff, systems and the wider school community from accidental or deliberate misuse.

All staff are asked to read, understand and sign this AUP.

Policy scope

1. I understand that this policy applies to my use of technology systems and services provided by the school or accessed by me as part of my role, both on and offsite. It also applies to personal use of technology where this is linked to my role, involves the school community, uses school systems or information, could affect safeguarding, professional boundaries, confidentiality or data protection, or could reasonably impact on my professional role or the reputation of the school.

2. I understand that the Acceptable Use of Technology Policy (AUP) for Ashford St Mary's Primary should be read and followed in line with our school policies for: child protection, online safety, behaviour policy, code of conduct and remote learning.

3. I am aware that all staff should ensure that technology use is consistent with the school ethos, staff 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 use school-provided or approved equipment, systems and internet services when working with children, unless otherwise formally agreed by leaders.

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. Personal use of setting IT systems and/or devices by staff is not allowed.

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.***
    - I will protect the devices in my care from unapproved access or theft.

8. 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 the IT System Manager (Lee) and/or the Headteacher.

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

10. I will ensure that any personal data is kept in accordance with the 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.

11. 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.

12. 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.

13. 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.

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

15. 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 System Manager (Lee) and Headteacher as soon as possible.

16. If I have lost any school related documents or files, I will report this to the ICT System Manager (Lee) and the Headteacher.

17. Any images or videos of children will only be used for school. I understand images of children must always be appropriate and should only be taken with school provided equipment and only be taken/published where parent/carers have given explicit written consent.

Classroom practice

18. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces. I understand my role and responsibilities in relation to filtering and monitoring, as explained in safeguarding training and relevant policies: Child Protection, AUP, Mobile Phone.

    - ***Teachers need to position themselves (static or moving round the room) in such a way that they can see most of the screens most of the time.***

19. 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, in line with the school child protection policy.
20. I will adhere to our 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.
- 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 our policies for: child protection, behaviour, anti-bullying, staff conduct and data protection.

22. I will promote online safety with the children/pupils/students 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 children feel comfortable to report concerns and say what they feel, without fear of getting into trouble and/or being judged for talking about something which happened to them online.
    - involving the Designated Safeguarding Lead (DSL) or a deputy Designated Safeguarding Lead as part of planning online safety lessons or activities to ensure support is in place for any children 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.
    - making informed decisions to ensure any online safety resources used with children is appropriate.

23. 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

24. 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, the Mobile Phone and Smart Device Policy and the law.

25. 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 headteacher.

26. 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. Use must not compromise supervision, safeguarding, confidentiality, professional boundaries, data protection or the learning environment.

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 and the law.

28. As outlined in Section 27 of the Code of Conduct 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.

29. I will not discuss or share data or information relating to children, staff, school business or parents/carers on social media.

30. My electronic communications with current and former 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 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 SLT.

- I will not share any personal contact information or details with children, such as my personal 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 or accept friend requests or communications on personal social media with current or past pupils and/or their parents/carers, where this is linked to my role, the school, or could blur professional boundaries.
- If I am approached online by a current or past children/pupils/students or parents/carers, I will not respond and will report the communication to my 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 Headteacher.
- Where digital communication with children and/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

31. 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.

32. 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.

33. 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.

34. 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.

35. 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 our child protection policy, staff code of conduct,and/or managing allegations against staff policy.

Policy Compliance and Breaches

36. 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 headteacher.

37. 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.

38. I understand that if the school believes that unauthorised and/or inappropriate use of school systems, devices or networks is taking place, the school may invoke its disciplinary procedures as outlined in the staff code of conduct.

39. 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 headteacher so it can be recorded and managed transparently.

40. 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 without delay, even if it appears minor, accidental or unlikely to meet the harm threshold.

41. 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.

42. 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.

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

44. 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 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 the Ashford St Mary's 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/Volunteer Acceptable Use of Technology Policy (AUP)

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 systems, or when acting in a role connected to the school. This AUP helps 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, or accessed by me as part of my role, visit or activity with Ashford St Mary's 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 our other relevant policies, including the staff code of conduct, child protection policy, visitor/volunteer procedures, 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. 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 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 in line with the child protection policy to:

    - The headteacher if it is regarding a member of staff or another visitor or volunteer
    - A Designated Safeguarding Lead (DSL) if it is a child

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 devices and smart technology

15. In line with the school's 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 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 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 child protection 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 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 Ashford St Mary's 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).....

Acceptable Use Policy - WiFi

This section of the policy is in regard to WiFi-internet access by guest users.

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, relevant policies, and the law.

1. The school provides guest Wi-Fi for the school community and allows access for school use only, for example, for members of the school governing body to access the agenda whilst in the school building.
2. Use of the Wi-Fi falls under Ashford St Mary's 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. Everyone 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. 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 the 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/setting] 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 the school data protection and safeguarding procedures.

9. Staff using school Wi-Fi on personal devices remain subject to the staff behaviour policy/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 headteacher.
    - If I have any queries about safe behaviour online, I will speak to a DSL

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 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 Ashford St Mary's Wi-Fi Acceptable Use Policy.

Name ……

Signed: ……

Date (DDMMYY)……..

Acceptable Use Policy (AUP) for Remote/Online Learning - Staff

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

Leadership oversight and approval

1. Remote/online learning will only take place using **Google Classroom**.
    - **Google** has been assessed and approved by **the headteacher/a member of Senior Leadership Team (SLT)**.

2. Staff will only use school managed or specific, approved professional accounts with children/pupils/students and/or parents/carers.
    - Use of any personal accounts to communicate with children/pupils/students and/or parents/carers is not permitted.
        - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with name, Designated Safeguarding Lead (DSL).
    - Staff will only use school-provided equipment where possible e.g. a school laptop or tablet.

3. Remote online teaching of children/pupils/students and contact with their parents/carers will not take place outside of the school day.
    - School day = 0845 - 1515

4. All remote/online lessons will be formally timetabled; a member of the leadership team or a 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 Google Classroom when delivering remote learning will be processed and stored with appropriate consent and in accordance with data protection legislation.

7. All remote learning and any other online communication will take place in line with current school confidentiality expectations as outlined in the confidentiality policy

8. Staff will not record lessons or meetings using personal equipment in line with our data protection policy requirements.

9. Only members of the Ashford St Mary's community will be given access to the remote learning that we provide.

10. Access to remote via Google Classroom will be managed in line with current IT security expectations outlined in this policy i.e. *strong passwords that are kept private, locking devices when not in use*.

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 sessions held. Normal Register e.g. Arbor.

13. Appropriate privacy and safety settings will be used to manage access and interactions. This includes but not limited to:
    - e.g. language filters, disabling/limiting chat, staff not permitting children/young people to share screens, keeping meeting IDs private, use of waiting rooms/lobbies or equivalent.

14. When live streaming (teaching) with children: contact will be made via children's school provided email accounts and/or logins.

15. Live 1:1 sessions will only take place with approval from the headteacher.

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

Behaviour expectations

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

18. All pupils/children/students are expected to behave in line with existing school policies and expectations.

19. When sharing videos and/or live streaming, pupils/children/students are required to:
    - wear appropriate dress.
    - ensure backgrounds of videos are not blurred or disguised
    - ensure that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds.

20. Children are encouraged to attend online learning 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.

21. 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

22. Participants are encouraged to report concerns during remote and/or live-streamed sessions:
    - Children report concern about other children to teacher
    - Parents report concerns to the teacher or Headteacher if the concern is a concern about the teacher.

23. 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 Phase Leader.

24. 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 for learning policies.

25. Sanctions for deliberate misuse may include (but are not limited to) e.g. restricting/removing use, exclusion and contacting police if a criminal offence has been committed.

26. Any safeguarding concerns will be reported to our Designated Safeguarding Lead(s), in line with our child protection policy.

Acceptable Use Policy for Remote/Online Learning - Pupil

1. I understand that:
   - These expectations are in place to help keep me safe when I am learning at home using Google e.g. Microsoft Teams, Google Meet etc.
   - I should read and talk about these rules with my parents/carers.
   - remote/online learning will only take place using a school approved system and during usual school times.
   - My use of Google classroom, Microsoft teams and Google Meet is monitored to help keep me safe.

2. Only members of the Ashford St Mary's community can access our Google education suite.
   - I will only use my school provided email accounts and/or login 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.

3. When taking part in remote/online learning I will behave as I would in the classroom.

4. When taking part in live sessions I will:
   - attend lessons where possible in a shared/communal space or room with an open door and/or when I can be supervised by a parent/carer or another appropriate adult.
   - mute my microphone.
   - wear appropriate clothing
   - ensure personal information/content is not visible.
   - I will not use alternative backgrounds or blur my background
   - attend the session in full.

5. If I am concerned about anything that takes place during remote/online learning, I will:
   - reporting concerns to the member of staff running the session

OR

   - tell a parent/carer

6. I understand that inappropriate online behaviour or concerns about my or others safety during remote/online learning will be taken seriously. This could include:
   - restricting/removing access, informing parents/carers, exclusion, contacting police if a criminal offence has been committed.

I have read and understood the Ashford St Mary's Primary School Acceptable Use Policy (AUP) for remote learning.

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

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

Parent/Carer's Name.....

Parent/Carer's Signature.....

Date.....

This policy has been produced with help and guidance from LADO Education Safeguarding Advisory Service.

Additional guidance from 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, Loose Primary School, Peter Banbury, Kent Police, Kent Schools Personnel Service (SPS), Kent Legal Services and Kent Libraries and Archives.