St Matthew's High Brooms CE Primary School

Powder Mill Lane
Tunbridge Wells
Kent
TN4 9DY

Acceptable Use of Technology Policy

Headteacher: Claire Harris
Chair of Governors: Jayne Ingman

Ratified: September 2025
Next Review: September 2026

Policy written by: Based on Kent LESAS template Policy

Fulfilling God-given potential

Distinctive Christian Values-
Honesty, Kindness, Respect, Responsibility

Acceptable Use of Technology Policy 2025-26

Disclaimer

The Kent County Council LADO Education Safeguarding Advisory Service makes every effort to ensure that the information in our templates is accurate and up to date, however, ultimate responsibility for ensuring their individual policies are appropriate remains the responsibility of the school/college/setting leadership team. If errors are brought to our attention, we will correct them as soon as practicable.

Contents

Child/Pupil/Student Acceptable Use of Technology Sample Statements

Although statements for children/pupils/students are collected within key stages, it is recommended that settings amend and adapt them according to their own cohorts needs.

Settings should ensure their AUP includes age and ability appropriate information and expectations relating to the specific use and monitoring of school/setting provided devices and networks, services and/or systems, for example laptops, tablets and cloud computing, as well as use of learner owned devices such as mobile/smart phones, tablets and wearable technology.

The template statements and headers are suggestions only and some statements are duplicated; we encourage educational settings to work with their community to amend the statements so they can develop ownership and understanding of the expectations.

Early Years and Key Stage 1 (0-6)

- I understand that the school rules will help keep me safe and happy when I go online.
- I only go online when an adult is with me.
- I only click on online 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
- If I see something online which makes me feel upset, unhappy, or worried I 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 school rules, there will be consequences.
- I have read and talked about these rules with my parents/carers.

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

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

Key Stage 2 (7-11)

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

Safe

- I will be kind and respectful online, just like I am in school.
- I only send messages which are polite and friendly.
- I will only share pictures or videos online if they are safe, kind, and I have asked for permission first.
- I will only click on links if 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.

Learning

- My own personal devices/mobile phone are not to be used in school unless I receive specific instruction to do so from my teacher.
- I always ask permission from an adult before using the internet.
- I only use websites and search engines that my teacher has chosen or given me 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

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.
- 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 or upset, I will minimise the screen and tell an adult immediately.
- If I am aware of anyone being unsafe with technology, I will report it to an adult in school
- 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.

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 online 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 smart/mobile phone and/or other wearable technology into school then I will hand in to the office/class teacher and then collect it at the end of the school day.
- 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 or to see help.
- I know that if I do not follow the school rules then there will be sanctions.

Shortened KS2 version (for use on posters)

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

Learner Acceptable Use Policy Agreement Form

Pupils sign the Home/School Agreement which specifically mentions: safe internet use, following school rules and talking to adults when something is worrying them.

Parent/Carer Acceptable Use of Technology Policy

1. I know that my child will be provided with internet access and will use a range of IT systems in order to access the curriculum and be prepared for modern life whilst at St Matthew's.
2. I understand that the AUP applies to my child's use of St Matthew's devices and systems on site and at home, 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/student, could

have repercussions for the orderly running of the school, if a pupil/student is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school.

3. I am aware that use of mobile and smart technology, such as mobile phones by children, is not permitted at St Matthew's. Mobile phones are handed in to a nominated adult on arrival at school.
4. I understand that any use of St Matthew's devices and systems are appropriately filtered; https://www.wave9.co.uk/services/security/
5. I am aware that my child's use of St Matthew's provided devices and systems will be monitored for safety and security reasons, when used on and offsite. 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.
6. I understand that St Matthew's will take every reasonable precaution, including implementing appropriate monitoring and filtering systems as above, to ensure my child is safe when they use St Matthew's devices and systems, on and offsite. I however understand that St Matthew's 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.
7. I am aware 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.
8. I have read and discussed the Acceptable Use of Technology Policy (AUP) with my child.
9. I will support St Matthew's safeguarding policies and will ensure that I use appropriate parental controls, will appropriately supervise/monitor my child's use of the internet outside of St Matthew's and will discuss online safety with them when they access technology at home.
10. I know I can seek support from the St Matthew's about online safety, such as via the St Matthew's website (https://st-matthews-school.org/parents/e-safety), to help keep my child safe online at home.
11. I will support the St Matthew's approach to online safety. I will role model safe and positive online behaviour for my child by sharing images, text, and video online responsibly.
12. I, together with my child, will not deliberately upload or share any content that could upset, threaten the safety of or offend any member of the St Matthew's community, or content that could adversely affect the reputation of the school
13. I understand that a partnership approach to online safety is required. If St Matthew's has any concerns about either my or my child's behaviour or safety online, then I will be contacted.
14. I understand that if I or my child do not abide by the St Matthew's AUP, appropriate action will be taken. This could include sanctions being applied in line with the St Matthew's policies and if a criminal offence has been committed, the police being contacted.
15. I know that I can speak to the Designated Safeguarding Lead (Mrs C Pollard), my child's class teacher or the headteacher if I have any concerns about online safety.

Parent/Carer Acknowledgement Form

Parents/Carers sign the Home/School Agreement which specifically mentions: safe internet use, following school policies, online posting of pictures and use of social media.

Staff Acceptable Use of Technology Policy (AUP)

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use St Matthew's 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 Matthew's expectations regarding safe and responsible technology use and can manage the potential risks posed. The AUP will also help to ensure that St Matthew's 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 Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services, either provided to me by the St Matthew's or accessed by me as part of my role within St Matthew's, professionally and personally, both on and offsite. 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 Matthew's Acceptable Use of Technology Policy (AUP) should be read and followed in line with the St Matthew's Child Protection and Safeguarding policy, and staff code of conduct.

3. I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the St Matthew's ethos, St Matthew's staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Use of St Matthew's devices and systems

4. I will only use the equipment and internet services provided to me by St Matthew's for example St Matthew's provided laptops, tablets, mobile phones and internet access, when working with pupils. Personal devices may be used with permission from the Headteacher, eg on a school trip to update parents via ClassDojo.

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; this use 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 St Matthew's 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 St Matthew's systems.
    - I will protect the devices in my care from unapproved access or theft..

8. I will respect St Matthew's 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 St Matthew's 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 St Matthew's 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 St Matthew's Data Protection Officer and leadership team prior to use to ensure it is safe and legal.

12. I will not keep documents which contain St Matthew's 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 St Matthew's learning platform to upload any work documents and files in a password protected environment or St Matthew's approved/provided VPN.

13. I will not store any personal information on the St Matthew's IT system, including St Matthew's laptops or similar device issued to members of staff, that is unrelated to St Matthew's activities, such as personal photographs, files or financial information.

14. I will ensure that St Matthew's 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 the ICT Technician as soon as possible.

17. If I have lost any St Matthew's related documents or files, I will report this to the ICT Technician and St Matthew's Data Protection Officer (Satswana) as soon as possible.

18. Any images or videos of children/pupils/students will only be used as stated in the St Matthew's camera and image use policy (https://st-matthews-school.org/our-school/policies). I understand images of children/pupils/students must always be appropriate and should only be taken with St Matthew's provided equipment (staff are permitted with the Headteacher's permission to take photographs on personal devices on school trips if there is not a school device to use. Photographs will be deleted from personal devices once uploaded to the school system) and only be taken/published where children/pupils/students 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 Matthew's as detailed in child protection and online safety policies, 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 ICT technician in line with the St Matthew's child protection/online safety 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 child protection, online safety, 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, and 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.
    - 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 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/pupils/students 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) (Carolyn Pollard) or a deputy as part of planning online safety lessons or activities to ensure support is in place for any children/pupils/students 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 children/pupils/students 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 St Matthew's mobile and smart technology and social media policies which addresses use by children/pupils/students 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 behaviour policy/code of conduct and the St Matthew's mobile technology policy and the law.

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/online safety policy, staff code of conduct, social media policy and the law.

28. As outlined in the staff code of conduct and St Matthew's social media 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 children/pupils/students, staff, St Matthew's business or parents/carers on social media.

29. My electronic communications with current and past children/pupils/students 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 St Matthew's approved and/or provided communication channels and systems, such as a St Matthew's email address, user account or telephone number.
    - I will not share any personal contact information or details with children/pupils/students, 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 children/pupils/students and/or their parents/carers.
    - 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 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 and/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 St Matthew's into disrepute.

33. I will report and record any concerns about the welfare, safety or behaviour of children/pupils/students or parents/carers online to the DSL in line with the St Matthew's child protection policy.

34. I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher, in line with St Matthew's child protection policy and/or 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 St Matthew's or off site, I will raise them with the DSL and/or the headteacher.

36. I understand that the St Matthew's may exercise its right to monitor the use of its devices information systems to monitor policy compliance and to ensure the safety of children/pupils/students and staff. This includes monitoring all St Matthew's provided devices and St Matthew's systems and networks including St Matthew's provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via St Matthew's 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 St Matthew's believe that unauthorised and/or inappropriate use of St Matthew's devices, systems or networks is taking place, the St Matthew's may invoke its disciplinary procedures as outlined in the staff code of conduct.

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

39. I understand that if the St Matthew's suspects criminal offences have occurred, the police will be informed.

Staff Acknowledgement Form

Staff sign a safeguarding form which specifically mentions the school's AUP, which is recorded on the Central Record.

Visitor and Volunteer Acceptable Use of Technology Policy

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 Matthew's 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 St Matthew's or accessed by me as part of my role within St Matthew's, 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 Matthew's AUP should be read and followed in line with the St Matthew's 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 St Matthew's ethos, St Matthew's 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, 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 St Matthew's 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 children/pupils/students. Any images or videos of children/pupils/students will only be taken in line with the St Matthew's camera and image use policy.

Classroom practice

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

9. Where I deliver or support remote/online learning, I will comply with the St Matthew's remote/online learning AUP.

10. I will support and reinforce safe behaviour whenever technology is used on site, and I will promote online safety with the children/pupils/students in my care.

11. If I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material by any member of the St Matthew's community, I will report this to the DSL and IT Technician, in line with the St Matthew's child protection/online safety policy.

12. 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

13. In line with the St Matthew's mobile and smart technology policy.

Online communication, including the use of social media

14. 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/online safety/social media policy (https://st-matthews-school.org/our-school/policies).
    - I will not discuss or share data or information relating to children/pupils/students, staff, St Matthew's 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 St Matthew's code of conduct/behaviour policy and the law.

15. My electronic communications with children/pupils/students, 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 St Matthew's approved communication channels such as via a St Matthew's 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 and/or headteacher..

Policy compliance, breaches or concerns

16. If I have any queries or questions regarding safe and professional practice online either in St Matthew's or off site, I will raise them with the Designated Safeguarding Lead (Carolyn Pollard) and/or the headteacher.

17. I understand that the St Matthew's may exercise its right to monitor the use of its devices information systems to monitor policy compliance and to ensure the safety of children/pupils/students and staff. This includes monitoring all St Matthew's provided devices and St Matthew's systems and networks including St Matthew's provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via St Matthew's 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.

18. I will report and record concerns about the welfare, safety or behaviour of children/pupils/students or parents/carers online to the Designated Safeguarding Lead (Carolyn Pollard) in line with the St Matthew's child protection policy.

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

20. I understand that if the St Matthew's believes that unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour is taking place online, the St Matthew's may invoke its disciplinary procedures.

21. I understand that if the St Matthew's suspects criminal offences have occurred, the police will be informed.

I have read, understood and agreed to comply with St Matthew's High Brooms 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)…….....

Wi-Fi Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all members of the St Matthew's community are fully aware of the St Matthew's boundaries and requirements when using the St Matthew's 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 St Matthew's community are reminded that technology use should be consistent with our ethos, other appropriate policies, and the law.

1. The St Matthew's provides Wi-Fi for the St Matthew's community and allows access for education use only.

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

3. The use of technology falls under the Acceptable Use of Technology Policy (AUP), online safety policy and behaviour policy which all children/pupils/students /staff/visitors and volunteers must agree to and comply with.

4. The St Matthew's 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. St Matthew's 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 St Matthew's service is adequately secure, such as up-to-date anti-virus software, systems updates.

7. The St Matthew's wireless service is not secure, and the St Matthew's cannot guarantee the safety of traffic across it. Use of the St Matthew's 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 St Matthew's accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the St Matthew's 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 St Matthew's 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 St Matthew's security and filtering systems or download any unauthorised software or applications.

11. My use of St Matthew's Wi-Fi will be safe and responsible and will always be in accordance with the St Matthew's 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 St Matthew's into disrepute.

13. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead (Carolyn Pollard) as soon as possible.

14. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead (Carolyn Pollard) or the headteacher..

15. I understand that my use of the St Matthew's Wi-Fi may be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the St Matthew's suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the St Matthew's may terminate or restrict usage. If the St Matthew's 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 Matthew's High Brooms CE Primary School Wi-Fi Acceptable Use Policy.

Name ……..…...

Signed: ……..…….Date (DDMMYY)……...

St Matthew's Staff Remote/Online Learning AUP

The Remote/Online Learning Acceptable Use Policy (AUP) is in place to safeguarding all members of St Matthew's community when taking part in remote/online learning, for example following any full or partial St Matthew's closures.

Leadership oversight and approval

1. Remote/online learning will only take place using Microsoft 365 & ClassDojo.
    - Microsoft 365 & ClassDojo has been assessed and approved by the headteacher

2. Staff will only use St Matthew's 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 Carolyn Pollard, Designated Safeguarding Lead (DSL).
    - Staff will use work provided equipment where possible**,** for example, a St Matthew's laptop, tablet, or other mobile device.

3. Online contact with children/pupils/students **and/or** parents/carers will not take place outside of the operating times as defined by SLT:

4. All remote/online lessons will be formally timetabled; a member of SLT, DSL and/or head of department 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 & ClassDojo when delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy (https://st-matthews-school.org/our-school/policies).

7. All remote/online learning and any other online communication will take place in line with current St Matthew's confidentiality expectations https://st-matthews-school.org/our-school/policies.

8. All participants will be made aware that Microsoft 365 & ClassDojo records activity.
9. Staff will not record lessons or meetings using personal equipment unless agreed and risk assessed by SLT and in line with our data protection policy requirements.
10. Only members of the St Matthew's community will be given access to Microsoft 365 & ClassDojo

11. Access to Microsoft 365 & ClassDojo will be managed in line with current IT security expectations as outlined in Online Safety Policy.

Session management

12. Appropriate privacy and safety settings will be used to manage access and interactions.

13. Live 1:1 sessions will only take place with approval from the headteacher/a member of SLT.

14. A pre-agreed invitation/email detailing the session expectations will be sent to those invited to attend.
    - Access links should not be made public or shared by participants
    - Children/pupils/students and/or parents/carers should not forward or share access links.
    - If children/pupils/students or parents/carers believe a link should be shared with others, they will discuss this with the member of staff running the session first.
    - Children/pupils/students are encouraged to attend lessons in a shared/communal space or room with an open door and/or when appropriately supervised by a parent/carer or another appropriate adult.

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

Behaviour expectations

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

17. All participants are expected to behave in line with existing St Matthew's policies and expectations.

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

19. 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

20. Participants are encouraged to report concerns during remote and/or live-streamed sessions:

21. 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 Headteacher.

22. 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.

23. Any safeguarding concerns will be reported to Carolyn Pollard, Designated Safeguarding Lead, in line with our child protection policy.

I have read and understood the St Matthew's High Brooms 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.