Acceptable Use of Technology Policy for Educational Settings

February 2026

At St Peter's we believe that all our Christian values stem from Love. The Love that God has for us, that we have for God and that we show each other.

Approved by:	Full Governing Body	**Date:** 20.5.2026
Last reviewed:	May 2026 (Based on KCC Model September 2025-26)	
Next review due by:	March 2028	

Contents

As A St Peter's Pupil:

I understand that the St. Peter-in-Thanet 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 permission first.
- I will only click on links if a trusted adult says they are safe.
- I only talk with and open messages from people I know.
- I know that people I meet online may not always 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 suggests meeting up, I will immediately talk to an adult.

Learning

- I ask my teacher before using my own personal devices at school.
- I always ask permission from an adult before using the internet.
- I only use websites and search engines that my teacher has given me permission to use. (e.g. Purple Mash, TTRS, Word Hippo)
- I use school devices for schoolwork unless I have permission otherwise.
- If I need to learn online at home, I will follow St Peter's remote learning guidelines.

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 content on other sources like other websites, books or with 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 say anything unkind. I know that AI tools can sometimes make mistakes. I will only use them when a 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.

Understand

- I understand that the school internet filter is there to protect me, and I will not try to bypass it.

- I know that all school devices and networks are checked to help keep me safe, including when I use them at home. This means that St. Peter-in-Thanet Junior School may be able to see and check my online activity when I use St. Peter-in-Thanet Junior School's devices and networks if they are worried about my or anyone else's safety or behaviour.
- If, for any reason, I need to bring in a personal device such as a mobile phone into St. Peter-in-Thanet Junior School, then I will put my phone in a zip bag in a cardboard box and it will be taken to the school office for safe keeping until the end of the school day. If I bring in a tablet (iPad) to aid with my learning, I will put them in a prearranged safe container in my classroom until I need to use it. I will wait/ask for an adult's permission before taking it out of the container.
- I have read and talked about these rules with my parents/carers.
- I can visit www.ceopeducation.co.uk and www.childline.org.uk to learn more about being safe online.
- I know that if I do not follow the school rules then there will be consequences from school and my parents.

Tell

- If I see something online that makes me feel worried or upset, I will close the laptop screen (lock the tablet if working on this instead) and tell an adult immediately.
- If I am aware of anyone being unsafe with technology, I will report it to a trusted adult.
- 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.
- I understand that the school Acceptable Use Policy will help keep me safe and happy online at home and at school.
- I know that I will be able to use the internet in school for a variety of reasons, if I use it responsibly. However, I understand that if I do not, I may not be allowed to use the internet at school.
- I know that being responsible means that I should not look for bad language, inappropriate images or violent or unsuitable games, and that if I accidently come across any of these I should report it to a teacher or adult in school or a parent or carer at home.
- I will treat my password like my toothbrush! This means I will not share it with anyone (even my best friend), and I will log off when I have finished using the computer or device.
- I will protect myself by not telling anyone I meet online my address, my telephone number, my school name or by sending a picture of myself without permission from a teacher or other adult.
- I will not arrange to meet anyone I have met online alone in person without talking to a trusted adult.
- If I get unpleasant, rude, or bullying emails or messages, I will report them to a teacher or other adult. I will not delete them straight away, but instead, keep them so I can show them to the person I am reporting it to.
- I will always be myself and not pretend to be anyone or anything I am not. I know that posting anonymous messages or pretending to be someone else is not allowed.

- I will always check before I download software or data from the internet. I know that information on the internet may not be reliable and it sometimes needs checking.
- If I bring in memory sticks / CDs from outside of school, I will always give them to my teacher so they can be checked for viruses and content before opening them.
- I will be polite and sensible when I message people online and I know that sending a message is the same as having a conversation with someone. I will not be rude or hurt someone's feelings online.
- I know that I am not allowed on personal email, social networking sites or instant messaging in school.
- If, for any reason, I need to bring my mobile phone into school I know that it is to be handed in to the class collection box which then goes to the office and then collected at the end of the school day.
- I know that all school devices/computers and systems are monitored, including when I am using them at home.
- I will tell a teacher or other adult if someone online makes me feel uncomfortable or worried when I am online using games or other websites or apps.

Shortened KS2 version (for use on posters in class)

- I ask an adult 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 devices and systems in school can be monitored

Pupils with Special Educational Needs and Disabilities (SEND)

Learners with SEND functioning at Levels P7-L1

(Based on Childnet's SMART Rules: www.childnet.com)

Safe

- I ask a grown up if I want to use the computer
- I do not tell strangers my name on the internet
- I know that if I do not follow the school rules then there will be consequences

Meeting

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

Accepting

- I do not open messages or emails from strangers

Reliable

- I make good choices on the computer

Tell

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

Learners with SEND functioning at Levels L2-4 (Based on Childnet's SMART Rules: www.childnet.com)

Safe

- I ask an adult if I want to use the internet
- I keep my information private on the internet
- I am careful if I share photos online
- I know that if I do not follow the school rules then there will be consequences

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 with an adult to make sure web links to make sure they are safe

Reliable

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

Tell

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

St Peter's Learner Acceptable Use Policy Agreement Form

St. Peter-in-Thanet Acceptable Use of Technology Policy – Learner Agreement

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

I agree to follow the AUP when:

1. I use school devices and systems, both on site and at home.
2. I use my own devices in school when allowed, including mobile phones, internet access and other new technologies in a responsible way at all times.
3. I use my own equipment out of the school, including communicating with other members of the school or when accessing school systems.
4. I know that network and internet access may be monitored.

Name……. Signed…….

Class…… Date……..

Parent/Carers Name…….....

Parent/Carers Signature…….

Date…….

Acceptable Use of Technology Forms for Parents/Carers

Parent/Carer AUP Acknowledgement

St. Peter-in-Thanet Learner Acceptable Use of Technology Policy Acknowledgment

1. I know that my child will be provided with internet access and will use a range of IT systems including Purple Mash and Zoom in order to access the curriculum and be prepared for modern life whilst at St. Peter-in-Thanet.

2. I am aware that learners' use of mobile technology and devices, such as mobile phones, is not permitted at St. Peter-in-Thanet. All mobile phones must be handed in to the class collection box at the beginning of the day. The box is then stored in a secure place in the school office. The phone box is then collected from the office at the end of the day and taken back to class for collection.

3. I am aware that any internet and technology use using school equipment may be monitored for safety and security reasons, to safeguard both my child and the school systems. This monitoring will take place in accordance with data protection (including GDPR) and human rights legislation.

4. I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that learners are safe when they use the school internet and systems. I understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

5. I understand that my child needs a safe and appropriate place to access remote learning if school is closed. I will ensure my child's access to remote learning is appropriately supervised. When accessing zoom calls, I will ensure they are an appropriate location (e.g. not in bed) and that they are suitably dressed. This does not mean they have to be in school uniform.

6. 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.

7. I have read and discussed the St. Peter-in-Thanet Learner Acceptable Use of Technology Policy (AUP) with my child.

8. I will support school safeguarding policies and will ensure that I appropriately monitor my child's use of the internet outside of school and discuss online safety with them when they access technology at home.

9. I know I can seek support from the school about online safety, such as via the school website (www.stpetersthanet.co.uk), to help keep my child safe online at home.

10. I will support the school approach to online safety. I will role model safe and positive online behaviour for my child by sharing images, text, and video online responsibly.

11. I, together with my child, will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.

12. I will not use technology to make visual or sound recordings of children or staff unless permission has been expressly granted.

13. I understand that a partnership approach to online safety is required. If the school 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. Peter-in-Thanet AUP, appropriate action will be taken. This could include sanctions being applied in line with other school 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 Jo Goodson, my child's teacher or the head teacher if I have any concerns about online safety.

I have read, understood and agree to comply with the St. Peter-in-Thanet Parent or Carer Acceptable Use of Technology Policy.

Child's Name…… Class……

Parent/Carers Name…….....

Parent/Carers Signature…….

Date…….

Staff Acceptable Use of Technology Policy

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use St. Peter-in-Thanet 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 learners, 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. Peter-in-Thanet expectations regarding safe and responsible technology use, and can manage the potential risks posed. The AUP will also help to ensure that school systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

Policy Scope

1. I understand that this AUP applies to my use of technology systems and services provided to me or accessed as part of my role within St. Peter-in-Thanet both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras, and email as well as IT networks, data and data storage, remote learning and online and offline communication technologies**.**

2. I understand that St. Peter-in-Thanet Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school staff code of conduct policy.

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

Use of School Devices and Systems

4. I will only use the equipment and internet services provided to me by the school, for example school provided laptops, tablets and internet access, when working with learners.

5. I understand that any equipment and internet services provided by my workplace is intended for educational use and should only be accessed by members of staff. Personal use of school IT systems and/or devices by staff is not allowed.

6. Where I deliver or support remote learning, I will comply with the school remote learning guidance as set out in this 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.
    - I will protect the devices in my care from unapproved access or theft and will not leave them unsupervised in public places.
8. I will respect school system security and will not disclose my password or security information to others.

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

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

11. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with the school information security policies.
    - All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
    - Any data being removed from the school site, such as via email or on memory sticks or CDs, will be suitably protected. This may include data being encrypted by a method approved by the school.

12. I will not keep documents which contain school related sensitive or personal information, including images, files, videos, and emails, on any personal devices, such as laptops and digital cameras. Where possible, I will use the school learning platform to upload any work documents and files in a password protected environment or school provided VPN

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

14. I will ensure that school owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

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

16. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the ICT Support Team (Think Big) as soon as possible.

17. If I have lost any school related documents or files, I will report this immediately to SLT and the Data Protection Manager, Alan Martin, Data Protection Advice Ltd, Tel 07402489691 as soon as possible.

18. Any images of learners must always be appropriate and should only be taken with school provided equipment and taken/published where learners and their parent/carer have given explicit consent.

Classroom Practice

19. I am aware of the expectations relating to safe technology use in the classroom and safe remote learning, as listed in our Child Protection and Online Safety policies.
20. I have read and understood the school mobile technology and social media policy as set out in the Online Safety Policy.
21. I will promote online safety with the learners 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 learners feel comfortable to 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) (Jo Goodson) as part of planning online safety lessons or activities to ensure support is in place for any learners who may be impacted by the content.
    - make informed decisions to ensure any online safety resources used with learners is appropriate.
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, e.g. 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's child protection, data protection and professional 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 children.
- Only approved AI platforms may be used with children. Children must be supervised when using AI tools, and I must ensure age-appropriate use and understanding prior to use.
- Any misuse of AI will be responded to in line with relevant school policies, including but not limited to, anti-bullying, staff and student behaviour and child protection.

For explicit instructions on how AI should be used in school, including examples, please see Appendix 1.

23. I will report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the DSL in line with the school child protection policies.

24. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, or distribute or use them.

Use of Social Media and Mobile Technology

25. I have read and understood the school policy which covers expectations regarding staff use of mobile technology and social media (Online Safety Policy).

26. I will ensure that my online reputation and use of IT and information systems are compatible with my professional role and in line with the staff code of conduct, when using school and personal systems. This includes my use of email, text, social media and any other personal devices or mobile technology.
    - I will take appropriate steps to protect myself online when using social media as outlined in the Staff Code of Conduct and Online Safety policies.
    - I am aware of the school expectations with regards to use of personal devices and mobile technology, including mobile phones as outlined in the Online Safety and Staff Code of Conduct policies.
    - I will not discuss or share data or information relating to learners, staff, school business or parents/carers on social media.
    - I will ensure that my use of technology and the internet does not undermine my professional role or interfere with my work duties and is in accordance with the school code of conduct and the law.

27. My electronic communications with current and past learners and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.
    - I will ensure that all electronic communications take place in a professional manner via school approved and/or provided communication channels and systems, such as a school email address, user account or telephone number.

- I will not share any personal contact information or details with learners, 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 learners and/or parents/carers. Should I feel this is necessary for the purpose of childcare arrangements etc. I will inform the Senior Leadership Team.
- If I am approached online by a learner or parents/carer, I will not respond and will report the communication to SLT and the Designated Safeguarding Lead (DSL).
- Any pre-existing relationships or situations that compromise my ability to comply with the AUP will be discussed with the DSL and Headteacher.

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

29. 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.

30. 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.

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

Policy Compliance

32. I understand that the school may exercise its right to monitor the use of information systems, including internet access and the interception of emails, to monitor policy compliance and to ensure the safety of learners and staff. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

Policy Breaches or Concerns

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

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

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

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

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

I have read, understood and agreed to comply with St. Peter-in-Thanet Staff Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of staff member: ……

Signed: ……

Date (DDMMYY)……...

Visitor and Volunteer Acceptable Use of Technology Policy

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

This AUP will help St. Peter-in-Thanet ensure that all visitors and volunteers understand the school 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 provided to me or accessed as part of my role within St. Peter-in-Thanet both professionally and personally. This may include use of laptops, tablets, digital cameras, and email as well as IT networks, data and data storage, remote learning systems and communication technologies**.**

2. I understand that the St. Peter-in-Thanet AUP should be read and followed in line with the school staff code of conduct.

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

Classroom Practice

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

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

6. I will immediately report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the Designated Safeguarding Lead (DSL) (Jo Goodson) in line with the school child protection policy.

7. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text, or music is protected, I will not copy, share, or distribute or use it.

Use of Social Media and Mobile Technology

8. I have read and understood the school policy which covers expectations regarding staff use of social media and mobile technology.

9. I will ensure that my online reputation and use of technology 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 online safety policy.
    - I will not discuss or share data or information relating to learners, staff, school business or parents/carers on social media.
    - I will ensure that my use of technology and the internet will not undermine my role, interfere with my duties and will be in accordance with the school code of conduct policy and the law.

10. I will not use my own devices to take any images or recordings of staff or pupils whilst in the school unless permission has been expressly granted.

11. My electronic communications with learners, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
    - All communication will take place via school approved communication channels such as via a school provided email address, account or telephone number.
    - Communication will not take place via personal devices or communication channels such as via my personal email, social networking account or mobile phone number.
    - Any pre-existing relationships or situations that may compromise this will be discussed with the DSL (Jo Goodson) and Headteacher.

12. If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with the Designated Safeguarding Lead (Jo Goodson) and the Headteacher.

13. 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.

14. 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.

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

Policy Compliance, Breaches or Concerns

16. I will report and record concerns about the welfare, safety or behaviour of learners or parents/carers to the Designated Safeguarding Lead (Jo Goodson) in line with the school child protection policy.

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

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

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

I have read, understood and agreed to comply with St. Peter-in-Thanet 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 school community are fully aware of the school boundaries and requirements when using the school Wi-Fi systems, and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

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

1. The school provides Wi-Fi for the school community and allows access for education use only.

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

3. The use of technology falls under St. Peter-in-Thanet Acceptable Use of Technology Policy (AUP), online safety policy, child protection policy and staff code of conduct policy which all learners/staff/visitors and volunteers must agree to and comply with.

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

5. School owned information systems, including Wi-Fi, must be used lawfully; I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

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

7. The school wireless service is not secure, and the school cannot guarantee the safety of traffic across it. Use of the school wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. I confirm that I knowingly assume such risk.

8. The school accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the school wireless service's connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.

9. I will respect system security; I will not disclose any password or security information that is given to me. To prevent unauthorised access, I will not leave any information system unattended without first logging out or locking my login as appropriate.

10. I will not attempt to bypass any of the school security and filtering systems or download any unauthorised software or applications.

11. My use of school Wi-Fi will be safe and responsible and will always be in accordance with the school AUP and the law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.

12. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.

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

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

15. I understand that my use of the school Wi-Fi may be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the school suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school may terminate or restrict usage. If the school suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agreed to comply with St. Peter-in-Thanet Wi-Fi Acceptable Use Policy.

Name ……...

Signed: ……..Date (DDMMYY)……

St Peter-in-Thanet Staff Remote Learning AUP

The Remote Learning Acceptable Use Policy (AUP) is in place to safeguard all members of St. Peter-in-Thanet School community when taking part in remote learning following any full or partial school closures.

Leadership Oversight and Approval

1. Remote learning will only take place using Purple Mash or other school approved programmes such as Fast Phonics and Engaging Eyes.
    - Purple Mash has been assessed and approved by the Headteacher and members of the Senior Leadership Team (SLT).
2. Staff will only use school managed or specific, approved professional accounts with learners and parents/carers.
    - Use of any personal accounts to communicate with learners and/or parents/carers is not permitted.
        - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with Jo Goodson, Designated Safeguarding Lead (DSL).
    - Staff will use work provided equipment where possible e.g. a school laptop, tablet, or other mobile device.
3. Online contact with learners and parents/carers should not take place outside of the operating times as defined by SLT, which are broadly defined as a typical working day
4. Live streamed remote learning sessions will only be held with approval and agreement from the Headteacher.

Data Protection and Security

5. All remote learning and any other online communication will take place in line with current school confidentiality expectations as outlined in the AUP policy.
6. Staff will not record lessons or meetings using personal equipment.
7. Only members of St. Peter-in-Thanet community will be given access systems to such as Purple Mash or Zoom.
8. Access to **SIMS and Abor** will be managed in line with current IT security expectations as outlined earlier in the AUP, namely through using strong passwords, logging off or locking devices when not in use.

Session Management

Staff will record the attendance of any sessions held and share this with SLT.

9. Appropriate privacy and safety settings will be used to manage access and interactions. Children will be reminded of their AUP agreement outlined earlier.
10. Live 1 to 1 sessions will only take place with approval from the Headteacher or a member of SLT. A parent or carer should be present in the room whilst session is taking place.
11. A pre-agreed email detailing the session expectations will be sent to those invited to attend.
    - Access links should not be made public or shared by participants.
    - Learners and/or parents/carers should not forward or share access links.
    - If learners/parents/carers believe a link should be shared with others, they will discuss this with the member of staff running the session first.

- Learners 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.

12. Access will be provided to those who do not have access via a school loan of a device.

Behaviour Expectations

13. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.
14. All participants are expected to behave in line with existing school policies and expectations. This includes:
    - Appropriate language will be used by all attendees.
    - Staff will not take or record images for their own personal use.
15. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.
16. When sharing videos and/or live streaming, participants are required to:
    - wear appropriate dress.
    - ensure backgrounds of videos are neutral.
    - ensure that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds.
17. 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

18. Participants are encouraged to report any concerns to a member or staff or telling a parent/carer during remote or live streamed sessions.
19. 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 Jo Goodson (DSL).
20. 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.
21. Sanctions for deliberate misuse may include: restricting/removing use, contacting police if a criminal offence has been committed.
22. Any safeguarding concerns will be reported to Jo Goodson, Designated Safeguarding Lead, in line with our child protection policy.

I have read and understood the St. Peter-in-Thanet Acceptable Use Policy (AUP) for remote learning.

Staff Member Name: ……..…….

Date…….

St. Peter-in-Thanet Learner Remote Learning AUP

I understand that:

- these expectations are in place to help keep me safe when I am learning at home using Purple Mash.
- I should read and talk about these rules with my parents/carers.
- remote learning will only take place using Purple Mash during usual school times.
    - My use of Purple Mash is monitored to help keep me safe.

2. Only members of the St. Peter-in-Thanet community can access Purple Mash.
    - I will only use my school provided email accounts or login to access remote learning.
    - I will use privacy settings as agreed.
    - 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 learning I will behave as I would in the classroom. This includes:
    - Using appropriate language.
    - Not taking or recording images/content.

4. When taking part in live sessions I will:
    - Mute my video and microphone until asked to speak.
    - wear appropriate clothing and be in a suitable location.
    - ensure backgrounds of videos are neutral and personal information/content is not visible.
    - Use appropriate alternative backgrounds.
    - Attend the session in full. If for any reason I cannot attend a session in full, I will let my teacher know.
    - attend lessons/zoom meetings in a shared/communal space or room with an open door and/or where possible when I can be supervised by a parent/carer or another appropriate adult.

5. If I am concerned about anything that takes place during remote learning, I will:
    - report concerns to the member of staff running the session, tell my parent/carer.

6. I understand that inappropriate online behaviour or concerns about my safety during remote learning will be taken seriously. This could include informing my parents/carers

I have read and understood the St. Peter-in-Thanet Acceptable Use Policy (AUP) for remote learning.

Name…… Signed…….

Class…… Date…….

Parent/Carers Name…….....

Parent/Carers Signature…….

Appendix 1: Use of Artificial Intelligence (AI) by Staff

The school recognises that Artificial Intelligence (AI) tools can support staff efficiency, creativity, and professional practice when used appropriately, ethically, and securely. AI tools may be used only for professional purposes and only within the limits set out below.

This guidance applies to all staff, including teachers, support staff, administrators, trainees, volunteers, and external professionals working on behalf of the school.

Acceptable Uses of AI for Work Purposes

Staff may use AI tools to support their work in the following ways, provided no personal or sensitive data is entered.

Teaching, Learning and Curriculum Support

- Drafting lesson ideas, lesson outlines, or teaching activities.
- Generating examples, model texts, or explanations for curriculum topics.
- Adapting lesson content for different ages or abilities without referencing real pupils.
- Creating quiz questions, discussion prompts, or retrieval practice activities.
- Generating generic worksheets, task ideas, or classroom activities.

Planning and Professional Tasks

- Supporting medium- or long-term planning frameworks.
- Drafting policies, procedures, or guidance documents.
- Improving clarity, structure, or tone of professional writing.
- Generating ideas for assemblies, displays, or enrichment activities.
- Summarising publicly available research or guidance documents.

Communication and Administration

- Drafting template letters or emails such as generic parent communications.
- Rewording text to be more formal, accessible, or concise.
- Supporting proofreading and spelling or grammar checks.
- Generating generic scripts or agendas for meetings or presentations.

Staff Development and Training

- Supporting CPD planning ideas.
- Creating hypothetical scenarios for training discussions.
- Summarising educational concepts or pedagogical approaches.

Important Clarification

The examples above are not exhaustive. If a member of staff wishes to use AI for a purpose not listed and is unsure whether it is appropriate, they must seek guidance from a member of Senior Leadership Team or Computing Lead before using the tool.

Unacceptable Uses of AI

Under no circumstances may AI be used in the following ways.

Personal, Sensitive, or Identifiable Information
Staff must not input, upload, copy, paste, or describe pupil names, staff names, parent or carer information, safeguarding details, medical information, SEN information, behaviour records, assessment data linked to real pupils, or any information that could reasonably identify an individual.

This applies even if the AI tool claims to be secure, the data is anonymised, the account is paid for, or the information is already known to the user.

Safeguarding and Confidential Matters
AI must never be used for safeguarding concerns, behaviour incidents involving named pupils, pastoral notes, or case discussions.

Assessment and Professional Judgement
AI must not mark or assess pupil work as a replacement for teacher judgement, generate pupil reports using real pupil information, or be presented as the author of professional judgements or decisions.

Why Personal Information Must Never Be Entered into AI

Entering personal or sensitive data into AI systems presents serious legal, ethical, and safeguarding risks. AI tools may store or process information outside the school's control, potentially breaching data protection legislation. Once information is entered, it cannot be retrieved or deleted by the school.

There is also a safeguarding risk, as personal information could be exposed, misused, or re-identified. AI tools do not understand school context, safeguarding thresholds, or professional boundaries, and outputs may be inaccurate or inappropriate.

Responsibility and Accountability

Staff are responsible for ensuring AI use aligns with this Acceptable Use Policy, checking the accuracy and suitability of AI-generated content, and maintaining professional judgement at all times. AI should be used as a support tool and not a replacement for professional expertise.

Failure to follow this guidance may be treated as a breach of the Acceptable Use Policy.

Remember, what AI generates is not necessarily the truth. AI pulls together what is on the internet about the subject requested by the user. The truth and what is on the internet are not necessarily the same. This is why it is imperative that we do not let AI replace our judgement as professionals and humans.