

Acceptable Use of Technology Policy for The Federation of St Martin's and Seabrook CEP School's

September 2025

Vision Statement

As a community of learners we understand God loves us equally and unconditionally and wants us to live life in all its fullness. We instill love and respect for all the natural world and everything it encompasses. We value each unique individual's diversity of gifts and talents and celebrate all their hard work and achievements and champion each learner's journey to reach their God-given potential.

Contents

Using the AUP Templates: Guidance Notes	Error! Bookmark not defined.
Child/Pupil/Student Acceptable Use of Technology Sample Statements.....	3
Early Years and Key Stage 1 (0-6)	3
Key Stage 2 (7-11)	3
Children/Pupils/Students with Special Educational Needs and Disabilities (SEND)	5
Acceptable Use of Technology Sample Statements and Forms for Parents/Carers	8
Parent/Carer AUP Acknowledgement Form.....	8
Sample Parent/Carer Acceptable Use of Technology Policy (AUP)	10
Acceptable Use of Technology for Staff, Visitors and Volunteers Sample Statements	12
Staff Acceptable Use of Technology Policy (AUP).....	12
Visitor and Volunteer Acceptable Use of Technology Policy	19
Wi-Fi Acceptable Use Policy.....	22
Template Acceptable Use Policy (AUP) for Remote/Online Learning	24
Remote/Online Learning AUP Template - Staff Statements.....	24
Remote/Online Learning AUP Template – Pupil/Student Statements	27
Acknowledgements and Thanks	

Pupil Acceptable Use of Technology Statements

Early Years and Key Stage 1 (0-6)

- I understand that the school Acceptable Use Policy will help keep me safe and happy online.
- I only use the internet when an adult is with me.
- I only click on online links and buttons 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 messages online which are polite and friendly.
- I know the school can see what I am doing online when I use school computers/tablets and, including if I use them at home.
- I always tell an adult/teacher/member of staff if something online makes me feel upset, unhappy, or worried.
- I can visit www.ceopeducation.co.uk learn more about keeping safe online.
- I know that if I do not follow the school rules:
 - I will not be allowed to use the school technology for a fixed period
 - I will not be allowed to use the school technology without adult supervision
 - My parent/carers will be informed
 - I will miss some of my privileges
- I have read and talked about these rules with my parents/carers.
- 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.

Learning

- 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
- If I need to learn online at home, I will follow the same rules in this policy.
- I am not permitted to use my own personal smart devices and/or mobile phone at school.
- I always ask permission from an adult before using the internet.
- I only use websites and search engines that my teacher has chosen.
- I use school devices for school work unless I have permission otherwise.

- If I need to learn online at home, I will follow the school remote/online learning AUP.

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 I should not or if I see something online that makes me feel worried or upset, I will, minimise the screen, shut the laptop lid, turn off the screen and tell an adult immediately.
- If I am aware of anyone being unsafe with technology, I will report it to a teacher/adult at 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 monitored to help keep me safe, including 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 concerned about my or anyone else's safety or behaviour...
- If, for any reason, I need to bring a personal device, for example a smart/mobile phone and/or other wearable technology into school then I will hand it into the school office or the class teacher in the morning. It will be returned to me 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:
 - I will not be allowed to use the school technology for a fixed period
 - I will not be allowed to use the school technology without adult supervision
 - My parent/carers will be informed
 - I will miss some of my privileges

Pupils with Special Educational Needs and Disabilities (SEND)

Learners with SEND functioning at Levels P4 –P7

- I ask a grown-up if I want to use the computer.
- I make good choices on the computer.
- I use kind words on the internet.
- If I see anything that I do not like online, I tell a grown up.
- I know that if I do not follow the school rules then:
 - I will not be allowed to use the school technology for a fixed period
 - I will not be allowed to use the school technology without adult supervision
 - My parent/carers will be informed
 - I will miss some of my privileges

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

Safe

- I ask an adult if I want to use the internet.
- I keep my information private on the internet.
- I am careful if I share photos online.
- I know that if I do not follow the school rules then:
 - I will not be allowed to use the school technology for a fixed period
 - I will not be allowed to use the school technology without adult supervision
 - My parent/carers will be informed
 - I will miss some of my privileges

Meeting

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

Accepting

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

Reliable

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

Tell

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

Pupil Acceptable Use Policy Agreement Form

The Federation of St Martin's and Seabrook CEP School's Acceptable Use of Technology Policy – Pupil Agreement

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

I agree to follow the AUP when:

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

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

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

Parent/Carer's Name.....

Parent/Carer's Signature..... (If appropriate)

Date.....

Acceptable Use of Technology Statements and Forms for Parents/Carers

Parent/Carer AUP Acknowledgement Form

The Federation of St Martin's and Seabrook CEP School's Pupil Acceptable Use of Technology Policy Acknowledgment

1. I have read and discussed The Federation of St Martin's and Seabrook CEP School's pupil acceptable use of technology policy (AUP) with my child and understand that the AUP will help keep my child safe online.
2. I understand that the AUP applies to my child's use of school devices and systems on site and at home including and personal use where there are safeguarding and/or behaviour concerns. This may include if online behaviour poses a threat or causes harm to another pupil, could have repercussions for the orderly running of the school, if a pupil is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school.
3. I understand that any use of school devices and systems are appropriately filtered; this means staff will check browser history, monitor website visited and use our broadband filtering system to analyse sites visited
4. I am aware that my child's use of school provided devices and systems will be monitored for safety and security reasons, when used on and offsite. This includes staff will check browser history, monitor website visited and use our broadband filtering system to analyse sites visited. Monitoring approaches are in place to keep my child safe and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.
5. I understand that the school will take every reasonable precaution, including implementing appropriate monitoring and filtering systems as above, to ensure my child is safe when they use school devices and systems, on and offsite. I however understand that the school cannot ultimately be held responsible for filtering breaches that occur due to the dynamic nature of materials accessed online, or if my child is using a personal device, including mobile or smart technologies.
6. I am aware that the school mobile and smart technology policy states that my child cannot use personal devices, including mobile and smart technology on site. For example, mobile phones should be handed to the office/ class
7. I understand that my child needs a safe and appropriate place to access remote/online learning, for example, if the school is closed. I will ensure my child's access to remote/online learning is appropriately supervised and any use is in accordance with the

school/setting remote learning AUP.

8. I and my child are aware of the importance of safe online behaviour and will not deliberately upload or share any content that could upset, threaten the safety of or offend any member of the school community, or content that could adversely affect the reputation of the school.
9. I understand that the school will contact me if they have concerns about any possible breaches of the AUP or have any concerns about my child's safety online.
10. I will inform the school (for example speaking to a member of staff and/or the Designated Safeguarding Lead) or other relevant organisations if I have concerns over my child's or other members of the school community's safety online.
11. I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet, both in and out of school.
12. I understand my role and responsibility in supporting the school online safety approaches and safeguarding my child online. I will use parental controls, supervise access and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding.

Child's Name..... Child's Signature

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

Parent/Carer's Name.....

Parent/Carer's Signature.....

Date.....

Parent/Carer Acceptable Use of Technology Policy (AUP)

1. I know that my child will be provided with internet access and will use a range of IT systems including **iPad and laptops** in order to access the curriculum and be prepared for modern life whilst at The Federation of St Martin's and Seabrook CEP School.
2. I understand that the AUP applies to my child's use of school 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, could have repercussions for the orderly running of the school, if a pupil is identifiable as a member of the school/setting, or if the behaviour could adversely affect the reputation of the school/setting.
3. I am aware that use of mobile and smart technology, such as mobile phones by children, is not permitted at The Federation of St Martin's and Seabrook CEP School. **If my child brings a mobile phone into school this should be handed to the school office or class teacher on arrival. It will be returned at the end of the school day.**
4. I understand that any use of school devices and systems are appropriately filtered by Primary Technologies and a report is sent to the school on a regular basis.
5. I am aware that my child's use of school provided devices and systems will be monitored for safety and security reasons, when used on and offsite. 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 the school will take every reasonable precaution, including implementing appropriate monitoring and filtering systems as above, to ensure my child is safe when they use school devices and systems, on and offsite. I however understand that the school cannot ultimately be held responsible for filtering breaches that occur due to the dynamic nature of materials accessed online, or if my child is using a personal device, including mobile or smart technologies.
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 Federation of St Martin's and Seabrook CEP School pupil Acceptable Use of Technology Policy (AUP) with my child.
9. I will support school safeguarding policies and will ensure that I use appropriate parental controls, will appropriately supervise/monitor my child's use of the internet outside of school and will discuss online safety with them when they access technology at home.
10. I know I can seek support from the school about online safety, such as via the school website to help keep my child safe online at home.
11. 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.
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 school 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 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 Federation of St Martin's and Seabrook CEP School AUP, appropriate action will be taken. This could include sanctions being applied in line with the 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 Mrs L Carter, Senior Leadership Team, SENCO if I have any concerns about online safety.

I have read, understood and agree to comply with The Federation of St Martin's and Seabrook CEP School Parent/Carer Acceptable Use of Technology Policy.

Child's Name..... Child's Signature
(If appropriate)

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

Parent/Carer's Name.....

Parent/Carer's Signature.....

Date.....

Date

Acceptable Use of Technology for Staff, Visitors and Volunteers Statements

Staff Acceptable Use of Technology Policy (AUP)

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

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

Policy scope

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services, either provided to me by the school or accessed by me as part of my role within The Federation of St Martin's and Seabrook CEP School 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 The Federation of St Martin's and Seabrook CEP School Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school/setting child protection/online safety policy, staff code of conduct and remote/online learning AUP.
3. I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the school ethos, school staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Use of school devices and systems

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

5. I understand that any equipment and internet services provided by my workplace is intended for education purposes and/or professional use and should only be accessed by members of staff. Reasonable personal use of setting IT systems and/or devices by staff is not allowed.
6. Where I deliver or support remote/online learning, I will comply with the school remote/online learning AUP.

Data and system security

7. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.
 - I will use a 'strong' password to access school systems. A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system. Leaders should include any specific requirements, for example, how often passwords should be changed etc.
 - I will protect the devices in my care from unapproved access or theft. Detail how this should be achieved, for example not leaving devices visible or unsupervised in public places.
8. I will respect school system security and will not disclose my password or security information to others.
9. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the DSLs.
10. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the SLT.
11. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including UK GDPR in line with the school information security policies.
 - All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
 - Any data being removed from the school site, such as via email or on memory sticks or CDs, will be suitably protected. This may include data being encrypted by a method approved by the school.
12. I will not keep documents which contain school related sensitive or personal information, including images, files, videos, and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the school learning platform to upload any work documents and files in a password protected environment or school approved/provided VPN.

13. I will not store any personal information on the school IT system, including school laptops or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.
14. I will ensure that school owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
15. I will not attempt to bypass any filtering and/or security systems put in place by the school.
16. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the SLT as soon as possible.
17. Any data being shared online, such as via cloud systems or artificial intelligence tools (AI), will be suitably risk assessed and approved by the school. Data Protection Officer and leadership team prior to use to ensure it is safe and legal.
18. If I have lost any school related documents or files, I will report this to the Executive Headteacher Liz Carter and school Data Protection Officer Accordio as soon as possible.
19. Any images or videos of pupils will only be used as stated in the school camera and image use policy. I understand images of pupils must always be appropriate and should only be taken with school provided equipment and only be taken/published where pupils and/or parent/carers have given explicit written consent.

Classroom practice

20. I understand that it is part of my roles and responsibilities to ensure that appropriate filtering and monitoring is implemented by The Federation of St Martin's and Seabrook CEP School as detailed in Child Protection Policy, Online Safety Policy and as discussed with me as part of my induction and/or ongoing safeguarding and child protection staff training.
21. If there is failure in the filtering software or abuse of the filtering or monitoring systems, for example, I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material, I will report this to the DSL and IT provider **Primary technologies** in line with the school child protection/online safety policy.
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 child protection, data protection, and staff code of conduct/policy expectations.
- A risk assessment will be undertaken, and written approval will be sought from the senior leadership team prior to any use of AI tools, for example if used in the classroom, or to support lesson planning.
- A Data Protection Impact Assessment (DPIA) will always be completed prior to any use of AI tools that may be processing any personal, sensitive or confidential data and use will only occur following approval from the DPO.
- I am required to critically evaluate any AI-generated content for accuracy, bias, and appropriateness before sharing or using it in educational contexts.
- AI must not be used to replace professional judgement, especially in safeguarding, assessment, or decision-making involving pupils.
- Only approved AI platforms may be used with pupils. Pupils must be supervised when using AI tools, and I must ensure age-appropriate use and understanding prior to use.

Any misuse of AI will be responded to in line with relevant school policies, including but not limited to, anti-bullying, staff and pupil behaviour and child protection.

23.I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:

- exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used.
- creating a safe environment where pupils feel comfortable to report concerns and say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.
- involving the Designated Safeguarding Lead (DSL) Mrs L Carter, Mrs S James and Mr J Carter or a deputy Mrs J Hawkins, Mrs N Binks, Mrs L Ames, Miss P White, Mrs E Geering as part of planning online safety lessons or activities to ensure support is in place for any pupils who may be impacted by the content.
- Informing the DSL and/or leadership team if I am teaching topics which could create unusual activity on the filtering logs, or if I believe the filtering system is placing unreasonable restrictions on teaching, learning or administration.
- make informed decisions to ensure any online safety resources used with pupils is appropriate.

24.I will respect copyright and intellectual property rights and ensure my use of online platforms and tools is safe, legal and ethical; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, misuse, plagiarise, or distribute them.

Mobile devices and smart technology

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

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

27. 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

28. In line with the school mobile and smart technology policy, I understand that visitor use of mobile devices and smart technology, for example, mobile phones and personal devices are not permitted or are only permitted within specific areas such as the staff room, Executive Headteacher's office or when children are not present.

Online communication, including use of social media

29. 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.

30. As outlined in the staff code of conduct and school social media policy.

- a. 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.
- b. I will not discuss or share data or information relating to pupils, staff, school business or parents/carers on social media.

31. My electronic communications with current and past pupils and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.

- a. 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.

- b. I will not share any personal contact information or details with pupils, such as my personal email address or phone number.
- c. I will not add or accept friend requests or communications on personal social media with current or past pupils and/or their parents/carers.
- d. If I am approached online by a current or past pupils or parents/carers, I will not respond and will report the communication to my line manager and Mrs L Carter, Designated Safeguarding Lead (DSL).
- e. 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 Executive Headteacher.

Policy concerns

- 32. 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.
- 33. 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.
- 34. 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.
- 35. I will report and record any concerns about the welfare, safety or behaviour of pupils or parents/carers online to the DSL in line with the school child protection policy.
- 36. I will report concerns about the welfare, safety, or behaviour of staff online to the Executive Headteacher, in line with school child protection policy and the allegations against staff policy.

Policy Compliance and Breaches

- 37. If I have any queries or questions regarding safe and professional practise online, either in school or off site, I will raise them with the DSL or Executive Headteacher.
- 38. I understand that the school may exercise its right to monitor the use of its devices information systems to monitor policy compliance and to ensure the safety of pupils and staff. This includes monitoring all school provided devices and school systems and networks including school provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via school provided devices, systems and/or networks. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.
- 39. I understand that if the school believe that unauthorised and/or inappropriate use of school devices, systems or networks is taking place, the school may invoke its disciplinary procedures as outlined in the staff code of conduct.

40. I understand that if the school believe that unprofessional or inappropriate online activity, including behaviour which could bring the school into disrepute, is taking place online, the school may invoke its disciplinary procedures as outlined in the staff code of conduct.
41. 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 The Federation of St Martin's and Seabrook CEP School Staff Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of staff member:

Signed:

Date (DDMMYY).....

Visitor

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 The Federation of St Martin's and Seabrook CEP School 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, either provided to me by the school or accessed by me as part of my role within The Federation of St Martin's and Seabrook CEP School professionally and personally. This may include my use of devices such as laptops, mobile phones, tablets, digital cameras, as well as IT systems and networks, email, data and data storage, remote learning systems and communication technologies.
2. I understand that The Federation of St Martin's and Seabrook CEP School AUP should be read and followed in line with the school staff code of conduct.
3. I am aware that this AUP does not provide an exhaustive list; visitors and volunteers should ensure that all technology use is consistent with the school ethos, school staff 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 school into disrepute.

Data and image use

7. I will ensure that any access to personal data is kept in accordance with Data Protection legislation, including UK GDPR.
8. I understand that I am not allowed to take images or videos of pupils.

Classroom practice

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

10. I will support and reinforce safe behaviour whenever technology is used on site and I will promote online safety with the pupils in my care.
11. If I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material by any member of the school community, I will report this to the DSL in line with the school/setting child protection/online safety policy.
12. 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 mobile devices and smart technology

13. In line with the school mobile and smart technology policy, I understand that, **mobile phones and personal devices are not permitted. Leaders should ensure policies include specific details and expectations regarding visitors use of mobile technology; a template social media and mobile technology policy can be found on the school website.**

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.
 - I will not discuss or share data or information relating to pupils, staff, school business or parents/carers on social media.
 - I will ensure that my use of technology and the internet will not undermine my role, interfere with my duties and will be in accordance with the school code of conduct policy and the law.
15. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
 - All communication will take place via school approved communication channels such as via a school provided email address, account or telephone number.
 - Communication will not take place via personal devices or communication channels such as via my personal email, social networking account or mobile phone number.
 - Any pre-existing relationships or situations that may compromise my ability to comply with this will be discussed with the DSL Mrs L Carter.

Policy compliance, breaches or concerns

16. If I have any queries or questions regarding safe and professional practice online either in school or off site, I will raise them with the Designated Safeguarding Lead Mrs L Carter.

17. I understand that the school may exercise its right to monitor the use of its devices information systems to monitor policy compliance and to ensure the safety of pupils and staff. This includes monitoring all school provided devices and school systems and networks including school provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via school provided devices, systems and/or networks. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.
18. I will report and record concerns about the welfare, safety or behaviour of pupils or parents/carers online to the Designated Safeguarding Lead Mrs L Carter, in line with the schoolchild protection policy.
19. I will report concerns about the welfare, safety, or behaviour of staff online to the Executive Headteacher, in line with the allegations against staff policy.
20. I understand that if the school believes that unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour is taking place online, the school may invoke its disciplinary procedures.
21. 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 The Federation of St Martin's and Seabrook CEP 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 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. 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.
2. The use of technology falls under The Federation of St Martin's and Seabrook CEP School Acceptable Use of Technology Policy (AUP), online safety policy and behaviour policy (**any other relevant policies such as data security, child protection, online safety**) which all pupils/staff/visitors and volunteers must agree to and comply with.
3. 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.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.

9. I will not attempt to bypass any of the school security and filtering systems or download any unauthorised software or applications.
10. 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.
11. 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.
12. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead Mrs L Carter as soon as possible.
13. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead Mrs L Carter.
14. 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 The Federation of St Martin's and Seabrook CEP School Wi-Fi Acceptable Use Policy.

Name

Signed:Date (DDMMYY).....

Acceptable Use Policy (AUP) for Remote/Online Learning

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

Additional information and guides on specific platforms can be found at:

- LGfL: [Safeguarding Considerations for Remote Learning](#)
- SWGfL: [Which Video Conference platform is best?](#)

Further information and guidance for SLT and DSLs regarding remote learning:

- Local guidance:
 - Kelsi:
 - [Online Safety Guidance for the Full Opening of Schools](#)
 - The Education People: [Covid-19 Specific Safeguarding Guidance and Resources](#)
 - [‘Safer remote learning during Covid-19: Information for School Leaders and DSLs’](#)
- National guidance:
 - DfE: [‘Safeguarding and remote education during coronavirus \(COVID-19\)’](#)
 - SWGfL: [Safer Remote Learning](#)
 - NSPCC: [Undertaking remote teaching safely](#)
 - Safer Recruitment Consortium: [Guidance for safer working practice](#)

Remote/Online Learning AUP Template - Staff Statements

Supply staff or online tutors employed by the school should agree and follow your child protection policy, staff behaviour policy and associated AUPs.

The Federation of St Martin’s and Seabrook CEP School Staff Remote/Online Learning AUP

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

Leadership oversight and approval

1. Remote/online learning will only take place using Zoom.

- Zoom has been assessed and approved by the Executive Headteacher/a member of Senior Leadership Team (SLT).
2. Staff will only use school managed or specific, approved professional accounts with pupils and parents/carers.
 - Use of any personal accounts to communicate with pupils and/or parents/carers is not permitted.
 - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with Mrs L Carter, Designated Safeguarding Lead (DSL).
 - Staff will use work provided equipment where possible, for example, a school laptop, tablet, or other mobile device.
 3. Online contact with pupils and parents/carers will not take place outside of the operating times as defined by SLT:
 - School hours 8:40 to 3:15pm
 4. All remote/online lessons will be formally timetabled; a member of SLT, DSL is able to drop in at any time.
 5. Live-streamed remote/online learning sessions will only be held with approval and agreement from the Executive Headteacher/a member of SLT.

Data Protection and Security

6. Any personal data used by staff and captured by Zoom when delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy.
7. All remote/online learning and any other online communication will take place in line with current school confidentiality expectations as outlined in the Confidentiality Policy.
 - Taking platform safety/security issues as appropriate into account.
8. All participants will be made aware that Zoom records activity.
9. Only members of the The Federation of St Martin's and Seabrook CEP School community will be given access to Zoom.
10. Access to Zoom will be managed in line with current IT security expectations as outlined in policy name.
 - using strong passwords, logging off or locking devices when not in use etc.

Session management

11. Staff will record the length, time, date, and attendance of any sessions held.

12. Appropriate privacy and safety settings will be used to manage access and interactions. This includes:
- Detail specifics according to the system being used, for example, language filters, disabling/limiting chat, staff not permitting children/young people to share screens, keeping meeting IDs private, use of waiting rooms/lobbies or equivalent.
13. When live streaming with pupil:
- contact will be made via pupils school provided email accounts and/or logins.
 - contact will be made via a parents/carers account.
 - staff will mute/disable pupils videos and microphones., for example, video/microphones should be muted
 - at least 2 members of staff will be present.
 - If this is not possible, SLT approval will be sought.
14. Live 1:1 sessions will only take place with approval from the Executive Headteacher/a member of SLT. Live 1:1 sessions with pupils are not recommended unless they are approved by SLT, a parent/carer is present in the room if possible and the session is auditable.
15. A pre-agreed invitation/email detailing the session expectations will be sent to those invited to attend.
- pupils and/or parents/carers should not forward or share access links.
 - If pupils or parents/carers believe a link should be shared with others, they will discuss this with the member of staff running the session first.
 - Pupils 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.
16. Alternative approaches and/or access will be provided to those who do not have access.

Behaviour expectations

17. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.
18. All 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.
 - Setting decisions about if other attendees can or cannot record events for their own use, and if so, any expectations or restrictions about onward sharing.
19. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.

20. When sharing videos and/or live streaming, participants are required to:

- wear appropriate dress.
- ensure backgrounds of videos are neutral (blurred if possible).
- ensure that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds.

21. Educational resources will be used or shared in line with our existing teaching and learning policies, taking licensing and copyright into account.

Policy Breaches and Reporting Concerns

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

- All pupils, reporting concerns to the member of staff running the session, telling a parent/carer etc.

23. If inappropriate language or behaviour takes place, participants involved will be removed by staff, the session may be terminated, and concerns will be reported to Mrs Liz Carter, Executive Headteacher.

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

25. Sanctions for deliberate misuse may include, for example, restricting/removing use, contacting police if a criminal offence has been committed.

26. Any safeguarding concerns will be reported to Mrs L Carter, Designated Safeguarding Lead, in line with our child protection policy.

I have read and understood The Federation of St Martin's and Seabrook CEP School Acceptable Use Policy (AUP) for remote/online learning.

Staff Member Name:

Date.....

Remote/Online Learning AUP Template – Pupil Statements

The Federation of St Martin's and Seabrook CEP School Pupil Remote/Online Learning AUP

1. I understand that:
 - these expectations are in place to help keep me safe when I am learning at home using Zoom,
 - I should read and talk about these rules with my parents/carers.
 - remote/online learning will only take place using Zoom and during usual school times.
 - my use of Zoom is monitored to help keep me safe.
2. Only members of the The Federation of St Martin's and Seabrook CEP School community can access Zoom.
 - I will only use my school provided email accounts and/or login to access remote learning.
 - I will use privacy settings as agreed with my teacher/set up the school.
 - I will not share my login/password with others.
 - I will not share any access links to remote learning sessions with others.
3. When taking part in remote/online learning I will behave as I would in the classroom. This includes
 - Using appropriate language.
 - Not taking or recording images/content without agreement from the teacher and/or those featured.
4. When taking part in live sessions I will:
 - mute my video and microphone. Pupils' video/microphones should be muted throughout
 - 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 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/online learning, I will:
 - Reporting concerns to the member of staff running the session, tell a parent/carer etc.

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

I have read and understood The Federation of St Martin's and Seabrook CEP School Pupil Acceptable Use Policy (AUP) for remote learning.

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

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

Parent/Carer's Name..... *(If appropriate)*

Parent/Carer's Signature..... *(If appropriate)*

Date.....