

The Darent Federation of Schools

Acceptable Use of Technology Policy



Approved by:	Tom Hardwick	Date: September 2024
Last reviewed on:	October 2023	
Next review due by:	October 2025	

Acceptable Use of Technology Policy

Reference to the **Federation** throughout this policy refers to Sundridge & Brasted CE Primary School, Kemsing Primary School and all staff and pupils within these school communities. Reference to school refers to either Sundridge & Brasted CE Primary School or Kemsing Primary School.

Reference to the **Designated Safeguarding Lead (DSL)** refers to Tom Hardwick at Sundridge & Brasted CE Primary School and Emily Hill at Kemsing Primary School.

Reference to the **Deputy Designated Safeguarding Lead** refers to Becca Jackaman, Abbi Fordred, Colette Taylor-Hicks, Helen Prestage and Sue Purkiss.

Updated content for 2023-34

The core content within the Acceptable Use Policy (AUP) template for 2023-24 has been updated and remains much the same as 2022-23. Additional content or changes have been highlighted in yellow.

Additional content has been added to support schools and settings to clarify the systems in place in relation to appropriate filtering and monitoring. We recommend DSLs and leaders access the following national guidance and/or seek advice from the Education Safeguarding Service.

- [Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - DfE Guidance - GOV.UK \(www.gov.uk\)](#)
- [Appropriate Filtering and Monitoring Guidance - UK Safer Internet Centre](#)
- [Filtering and monitoring - Questions for governors, proprietors and trustees - UK Safer Internet Centre](#)
- [Filtering and Monitoring Webinars - SWGfL](#)

Disclaimer

Kent County Council make every effort to ensure that the information in this document is accurate and up to date. If errors are brought to our attention, we will correct them as soon as practicable. The copyright of these materials is held by Kent County Council. However, educational settings that work with pupils and young people are granted permission to use all or part of the materials for not-for-profit use, providing Kent County Council copyright is acknowledged and we are informed of its use.

Acceptable Use of Technology Policy

Pupil Acceptable Use of Technology Statements

Early Years and Key Stage 1 (0-6)

- I understand that the Federation's 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 and tablets.
- I always tell a member of staff if something online makes me feel upset, unhappy, or worried.
- I can visit www.thinkuknow.co.uk to learn more about keeping safe online.
- I know that if I do not follow the school rules:
 - I will need to discuss this with my class teacher, my parents and possibly Mr Hardwick or Mrs Taylor-Hicks.
- I have read and talked about these rules with my parents/carers.

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

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

Key Stage 2 (7-11)

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

Safe

- I will behave online the same way as I behave in the classroom.
- I only send messages which are polite and friendly.
- I will only post pictures or videos on the internet if they are safe and appropriate, and if I have permission.
- I only talk with, and open messages, from people I know.
- I will only click on links if I know they are safe.
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult.

Acceptable Use of Technology Policy

Learning

- I ask my teacher before using 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.

Trust

- I know that not everything or everyone online is honest or truthful.
- I will check content on various 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.

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 see 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 trusted adult at school as soon as possible.
- I know it is not my fault if I see, or someone sends me, something upsetting or unkind online.
- I always talk to an adult if I am not sure about something or if something happens online that makes me feel worried or frightened.
- I know that I can use the school worry boxes if I need to as well as the digital worry box on our website.

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 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 know that it is to be handed in to the office and then collected at the end of the school day.
- I have read and talked about these rules with my parents/carers.
- I can visit www.thinkuknow.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:

Acceptable Use of Technology Policy

- My teacher and my parents will discuss this and ensure that support is in place to teach me how to behave appropriately online. I know that this will mean that my use of the internet at home and at school will be monitored very carefully by adults.
- Mr Hardwick will be informed and he will also be checking that my use of the internet does not break school rules in future.

Alternative KS2 Statements (optional)

- I understand that the school's 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 accidentally 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.
- 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 a personal/smart device and/or mobile phone into school I know that it is to be handed in 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.

Acceptable Use of Technology Policy

Shortened KS2 version (for use on posters - optional)

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

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 internet unless I am directly supervised by an adult.

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

Safe

- I ask a grown up if I want to use the computer.
- I do not tell strangers my name on the internet.
- I know that if I do not follow the school rules then:
I will not be allowed to use the internet unless I am being directly supervised by an adult.

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.

Acceptable Use of Technology Policy

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's IT systems in a professional, lawful, and ethical manner. To ensure that members of staff understand their professional responsibilities when using technology and provide appropriate curriculum opportunities for pupils, they are asked to read and sign the staff Acceptable Use of Technology Policy (AUP).

Our AUP is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally, however the AUP will help ensure that all staff understand the Federation's 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 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's Acceptable Use of Technology Policy (AUP) should be read and followed in line with the Child Protection Policy and Staff Code of Conduct.
3. I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the school ethos, school code of conduct and safeguarding policies, national and local education and child protection guidance, and the law.

Use of Federation devices and systems

4. I will only use the equipment and internet services provided to me by the Federation for example school provided laptops, tablets, mobile phones and internet access, when working with pupils.
5. I understand that any equipment and internet services provided by my workplace is intended for education purposes and/or professional use and should only be accessed by members of staff. Reasonable personal use of setting IT systems and/or devices by staff is allowed; this use is at the school's discretion and can be revoked at any time. Occasional personal use of the settings devices can be beneficial to the development of staff IT skills and can enable staff to maintain a positive work-life balance. This is at the school's discretion and can be revoked at any time.

Acceptable Use of Technology Policy

Data and system security

6. 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.
7. I will respect the school's system security and will not disclose my password or security information to others.
8. 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 Carbon Cloud.
9. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from Carbon Cloud
10. 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.
11. I will not keep documents which contain school related sensitive or personal information, including images, files, videos, and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the school learning platform to upload any work documents and files in a password protected environment or school approved/ VPN.
12. I will not store any personal information on the school's IT system, including school laptops or similar device issued to members of staff, that is unrelated to school activities, such as personal photographs, files or financial information.
13. I will ensure that school owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
14. I will not attempt to bypass any filtering and/or security systems put in place by the school.
15. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to Carbon Cloud as soon as possible.
16. If I have lost any school related documents or files, I will report this to Carbon Cloud and the school's Data Protection Officer (Helen Prestage or Tom Hardwick) as soon as possible.

Acceptable Use of Technology Policy

17. Any images or videos of pupils will only be used as stated in the school's Photographic 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

18. I understand that it is part of my roles and responsibilities to ensure that appropriate filtering and monitoring is implemented by the Federation as detailed in the Child Protection Policy and as discussed with me as part of my induction and/or ongoing safeguarding and child protection staff training.
19. 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 Carbon Cloud, in line with the school's Child Protection Policy.
20. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed in Child Protection Policy and the AUP.
21. 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 or a deputy 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.
22. 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.

Mobile devices and smart technology

23. 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 law.

Acceptable Use of Technology Policy

Online communication, including use of social media

24. I will ensure that my use of communication technology, including use of social media is compatible with my professional role, does not interfere with my work duties and takes place in line with the Child Protection Policy, Staff Code of Conduct, and the law.
25. As outlined in the Staff Code of Conduct:
 - I will take appropriate steps to protect myself and my reputation, and the reputation of the school, online when using communication technology, including the use of social media.
 - I will not discuss or share data or information relating to pupils, staff, school business or parents/carers on social media.
26. My electronic communications with current and past pupils and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.
 - I will ensure that all electronic communications take place in a professional manner via school approved and/or provided communication channels and systems, such as a school email address, user account or telephone number.
 - I will not share any personal contact information or details with pupils, such as my personal email address or phone number.
 - I will not add or accept friend requests or communications on personal social media with current or past pupils and/or their parents/carers.
 - If I am approached online by a current or past pupils or parents/carers, I will not respond and will report the communication to the DSL.
 - Any pre-existing relationships or situations that compromise my ability to comply with the AUP or other relevant policies will be discussed with the DSL.

Policy concerns

27. 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.
28. 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.
29. 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.
30. 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's Child Protection Policy.
31. I will report concerns about the welfare, safety, or behaviour of staff online to the DSL in line with School's Child Protection Policy and the Whistle Blowing policy.

Acceptable Use of Technology Policy

Policy Compliance and Breaches

- 32. 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 DSL.
- 33. 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.
- 34. I understand that if the school believes 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.
- 35. 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.
- 36. 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's 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

Acceptable Use of Technology Policy

Visitor and Volunteer Acceptable Use of Technology Policy

As a professional organisation with responsibility for safeguarding, it is important that all members of the community, including visitors and volunteers, are aware of our behaviour expectations and their professional responsibilities when using technology. This AUP will help the Federation to ensure that all visitors and volunteers understand the Federation's expectations regarding safe and responsible technology use.

Policy scope

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services, either provided to me by the school or accessed by me as part of my role within the Federation, 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's AUP should be read and followed in line with the School's Staff Code of Conduct.
3. I am aware that this AUP does not provide an exhaustive list; visitors and volunteers should ensure that all technology use is consistent with the 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.

Acceptable Use of Technology Policy

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. Where I deliver or support remote/online learning, I will comply with the school's remote/online learning AUP.
11. 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.
12. If I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material by any member of the school community, I will report this to the DSL in line with the school's Child Protection Policy.
13. 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

14. In line with the school's mobile and smart technology policy, I understand that mobile phones and personal devices are not permitted to be used whilst in the same vicinity as pupils.

Online communication, including the use of social media

15. I will ensure that my online reputation and use of technology and is compatible with my role within the school. This includes my use of email, text, social media, social networking, gaming and any other personal devices or websites.
 - I will take appropriate steps to protect myself online as outlined in the Child Protection 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's Staff Code of Conduct Policy and the law.
16. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
 - All communication will take place via school approved communication channels such as via a school provided email address, account or telephone number.
 - Communication will not take place via personal devices or communication channels such as via my personal email, social networking account or mobile phone number.
 - Any pre-existing relationships or situations that may compromise my ability to comply with this will be discussed with the DSL.

Acceptable Use of Technology Policy

Policy compliance, breaches or concerns

17. If I have any queries or questions regarding safe and professional practice online either in school or off site, I will raise them with the DSL.
18. I understand that the school may exercise its right to monitor the use of its devices information systems to monitor policy compliance and to ensure the safety of pupils and staff. This includes monitoring all school provided devices and school systems and networks including school provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via school provided devices, systems and/or networks. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.
19. I will report and record concerns about the welfare, safety or behaviour of pupils or parents/carers online to the Designated Safeguarding Lead in line with the school's Child Protection Policy.
20. I will report concerns about the welfare, safety, or behaviour of staff online to the Headteacher, Tom Hardwick, in line with the allegations against staff policy.
21. I understand that if the school believes that unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour is taking place online, the school may invoke its disciplinary procedures.
22. I understand that if the school suspects criminal offences have occurred, the police will be informed.

I have read, understood and agreed to comply with the Federation's 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

Acceptable Use of Technology Policy

Wi-Fi Acceptable Use Policy

As a professional organisation with responsibility for pupils' 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 the Federation's Acceptable Use of Technology Policy (AUP) and Child Protection Policy which all pupils/staff/visitors and volunteers must agree to and comply with.
4. The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.
5. School owned information systems, including Wi-Fi, must be used lawfully; I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
6. I will take all practical steps necessary to make sure that any equipment connected to the school service is adequately secure, such as up-to-date anti-virus software, systems updates.
7. The school's wireless service is not secure, and the school cannot guarantee the safety of traffic across it. Use of the school's wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. I confirm that I knowingly assume such risk.
8. The school accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the school's wireless service 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.

Acceptable Use of Technology Policy

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's Wi-Fi will be safe and responsible and will always be in accordance with the school's AUP and the law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.
12. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.
13. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead as soon as possible.
14. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead.
15. I understand that my use of the school's 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's Wi-Fi Acceptable Use Policy.

Name

Signed:

Date: