



Greatstone Primary School

Acceptable Use of Technology Policy

Policy lead:	Jaclyn Kay
Date:	February 2022
Review Frequency:	Annually
Review Date:	February 2023
References:	<p>Kent County Council's Online Safety Guidance and Information for Education Settings: www.kelsi.org.uk/child-protection-and-safeguarding/e-safety</p> <p>Kent County Council Education Safeguards Team Content: www.kelsi.org.uk/child-protection-and-safeguarding</p> <p>These statements have been produced by The Education People Education Safeguarding Service.</p> <p>Additional thanks to members of the Kent Education Online Safety Strategy Group, the UK Safer Internet Centre, South West Grid for Learning (SWGfL), London Grid for Learning (LGfL), South East Grid for Learning (SEGfL), Childnet, CEOP, The Judd School, Kingsnorth Primary School, Loose Primary School, Peter Banbury, Kent Police, Kent Schools Personnel Service (SPS), Kent Legal Services and Kent Libraries and Archives, for providing comments, feedback and support on previous versions.</p>
Governor Agreement:	9 th February 2022
To be read in conjunction with	<p>Safeguarding and Child Protection Policy</p> <p>Online Safety Policy</p> <p>Behaviour Policy</p>

Contents

Learner Acceptable Use of Technology Statements

Early Years and Key Stage 1 (0-6) *Page 3*

Key Stage 2 (7-11) *Pages 3 and 4*

Learners with SEND *Page 5*

Learner Acceptable Use Policy Agreement Form *Page 6*

Learners use of Mobile and Smart Technology *Page 7*

Year 5 and 6 Mobile and Smart Technology Permission *Pages 8*

Acceptable Use of Technology Statements/Forms for Parents/Carers

Parent/Carer Acceptable Use of Technology Policy *Pages 9*

Parent/Carer Agreement *Page 10*

Acceptable Use of Technology for Staff, Visitors, Volunteers & Governors

Staff Acceptable Use of Technology Policy *Pages 11-15*

Visitor, Volunteer & Governors Acceptable Use of Technology Policy *Pages 16 -18*

Wi-Fi Acceptable Use Policy *Pages 19 - 20*

Learner Acceptable Use of Technology Statements.

Early Years and Key Stage 1 (0-6 years old)

I understand that the Greatstone Primary 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 links and buttons online when I know what they do.
- 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 devices, including when I am at home.
- I always tell an adult 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 rules, internet privileges will be removed.
- I have read and talked about these rules with my parents/carers.

Key Stage 2 (7-11years old)

I understand that the Greatstone Primary School 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.

Learning

- 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 Greatstone Primary School remote learning AUP.

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.

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 systems are monitored to help keep me safe, including when I use them at home.
- 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.
- I know that if I do not follow the school rules then internet privileges will be removed.

Tell

- If I see anything online that I should not or that makes me feel worried or upset, I shut the laptop lid or turn off the screen and tell an adult straight away.
- If I am aware of anyone being unsafe with technology, I will report it to a teacher.
- I know it is not my fault if I see, or someone sends me, something bad 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 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.

Learners with Special Educational Needs and Disabilities (SEND)

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:
 - *My behaviour plan or whole school policy will be referred to.*

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.

Learner Acceptable Use Policy Agreement Form

Greatstone Primary School Acceptable Use of Technology Policy – Learner 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.....

Date.....

Learners use of mobile and smart technology

Aim and Purpose

Parents should discourage pupils from bringing mobile phones to school on the grounds that they are valuable and may be lost or stolen. However, we recognise that in Years Five and Six mobile phones may have a part to play in securing pupils' personal safety before and after school and on journeys to and from school. If a pupil needs to contact his/her parents/guardians they will be allowed to use a school phone. If parents need to contact children urgently they should phone the school office and a message will be relayed promptly. Under no circumstances will pupils be allowed to take mobile phones on school excursions. Parents of Year Five and Six pupils will need to complete the permission form. The school accepts no responsibility for any loss or damage whilst the device is on school premises.

Procedures

- Learners will be educated regarding the safe and appropriate use of mobile and smart technology, including mobile phones and personal devices, and will be made aware of behaviour expectations and consequences for policy breaches.
- Safe and appropriate use of mobile and smart technology will be taught to learners as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources. Further information is contained within our child protection and relevant specific curriculum policies.
- Mobile phones and personal devices must not be taken into classrooms, educational visits or residential. They must be handed into the school office. The phone must be switched off when entering the school ground and only switched back on again when leaving the school grounds. Learners found in possession of a mobile phone will have it confiscated and their parent/carer will be asked to collect it at the end of the day.
- Any concerns regarding learners use of mobile technology or policy breaches will be dealt with in accordance with our existing policies, including anti-bullying, child protection and behaviour.
 - Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our child protection, behaviour or anti-bullying policy.
 - Learners' mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/carer. Content may be deleted or requested to be deleted if it contravenes our policies.
 - Mobile phones and devices that have been confiscated will be held in a secure place and released to parents/carers at the end of the day.
 - Concerns regarding policy breaches by learners will be shared with parents/carers as appropriate.
 - Where there is a concern that a child is at risk of harm, we will contact respond in line with our child protection policy.
 - If there is suspicion that material on a learner's personal device or mobile phone may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

I have read, understood and agree to comply with the Greatstone Primary School Mobile and Smart Technology Procedures

Child's Name.....

Mobile Phone Number

Reason for phone being in school

.....
.....
.....

I give permission for my son/daughter to bring the above-mentioned phone into the school office. The phone will be switched off when entering the school grounds and will only be turned back on when leaving the school grounds. The school accepts no responsibility for any loss or damage whilst the device is on school premises.

Parent/Carer's Name.....

Parent/Carer's Signature..... Date.....

Parent/Carer Acceptable Use of Technology Policy

1. I know that my child will be provided with internet access and will use a range of IT systems in order to access the curriculum and be prepared for modern life whilst at Greatstone Primary School
2. I am aware that learners use of mobile and smart technology, is not permitted at Greatstone Primary School
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 in response to Covid-19. I will ensure my child's access to remote learning is appropriately supervised and any use is in accordance with the school remote learning AUP.
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 Greatstone Primary School 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 <https://greatstoneschool.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 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.
13. I understand that if I or my child do not abide by the Greatstone Primary 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.
14. I know that I can speak to the Designated Safeguarding Lead (Jaclyn Kay), my child's class teacher or the Head of School if I have any concerns about online safety.

I have read, understood and agree to comply with the Greatstone Primary School Parent/Carer Acceptable Use of Technology Policy.

Child's Name.....

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

Parent/Carer's Name.....

Parent/Carer's Signature..... Date.....

Acceptable Use of Technology for Staff, Visitors and Volunteers Statements

Staff Acceptable Use of Technology Policy

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Greatstone Primary 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 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 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 Greatstone Primary School 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 Greatstone Primary School Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school staff code of conduct and remote 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 learners.
5. I understand that any equipment and internet services provided by my workplace is intended for education purposes and professional use and should only be accessed by members of staff. Reasonable personal use of setting IT systems and devices by staff is allowed.
6. Where I deliver or support remote learning, I will comply with the school remote 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.
 - I will protect the devices in my care from unapproved access or theft.
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 IT system manager.
10. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT system manager.
11. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including 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 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 Provider as soon as possible.

17. If I have lost any school related documents or files, I will report this to the ICT Support Provider/ and school Data Protection Officer Fiona Roberts as soon as possible.

18. Any images or videos of learners will only be used as stated in the image use policy. I understand images of learners must always be appropriate and should only be taken with school provided equipment and only be taken/published where learners and/or parent/carers have given explicit written consent.

Classroom Practice

19. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed in the child protection, online safety and remote learning AUP.

20. I have read and understood the school mobile technology 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 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) Jaclyn Kay or a deputy Matt Rawling, Fiona Roberts and Nadia Leech 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 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.

23. 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

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

Staff are advised to:

- Keep mobile phones and personal devices in a safe and secure place (in a bag, cupboard or drawer) during lesson time.

- Keep personal mobile phones and devices switched off or set to 'silent' mode during lesson times.
- Not use personal devices during teaching periods unless permission has been given by the Head of School, such as in emergency circumstances. .
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence using a personal device or mobile phone, the police will be contacted and the LADO (Local Authority Designated Officer) will be informed in line with our allegations policy.

Online Communication, including Use of Social Media

25. 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 our code of conduct policy and the law.

- I will take appropriate steps to protect myself and my reputation online when using communication technology, including the use of social media.
- I will not discuss or share data or information relating to learners, staff, school business or parents/carers on social media.

26. 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.
- If I am approached online by a current or past learner or parents/carer, I will not respond and will report the communication to my Designated Safeguarding Lead (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 is 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 concerns about the welfare, safety or behaviour of learners or parents/carers to the DSL in line with the school child protection policy.

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

Policy Compliance and Breaches

32. 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.

33. I understand that the school may exercise its right to monitor the use of its 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.

34. 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.

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 code of conduct policy.

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 Greatstone Primary School Staff Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of staff member:

Signed:

Date (DDMMYY).....

Visitor, Volunteer (& Governors) 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 Greatstone 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 provided to me or accessed as part of my role within Greatstone Primary School, 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 systems and communication technologies.
2. I understand that Greatstone Primary 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 behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Data and Image Use

4. I will ensure that any access to personal data is kept in accordance with Data Protection legislation, including GDPR.
5. I understand that I am allowed to take images or videos of learners. Any images or videos of learners will only be taken in line with the image use policy.

Classroom Practice

6. I am aware of the expectations regarding safe use of technology in the classroom and other working spaces, including appropriate supervision of learners.
7. Where I deliver or support remote learning, I will comply with the school remote learning AUP.
8. 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.
9. I will immediately report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the Designated Safeguarding Lead (DSL) (Jaclyn Kay) in line with the school child protection policy.

10. 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

11. In line with the school mobile technology policy, I understand that mobile phones and personal devices are only permitted within specific areas where children are not present or are only permitted for specific purposes e.g. as part of multi-agency working arrangements.

Online Communication, including the Use of Social Media

12. 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 online safety policy.
- I will not discuss or share data or information relating to learners, staff, school/setting 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.

13. 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 (Jaclyn Kay)

Policy Compliance, Breaches or Concerns

14. 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 (Jaclyn Kay)

15. 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.

16. 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.

17. 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.

18. I understand that the school may exercise its right to monitor the use of school information systems, including internet access and the interception of emails, to monitor policy compliance and to ensure the safety of learners, staff and visitors/volunteers. 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 learners or parents/carers to the Designated Safeguarding Lead (Jaclyn Kay) in line with the school child protection policy.

20. I will report concerns about the welfare, safety, or behaviour of staff to the Head of School, 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 Greatstone Primary School visitor/volunteer/Governor 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 the 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 Greatstone Primary School Acceptable Use of Technology Policy (AUP), online safety policy and behaviour 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 (Jaclyn Kay) as soon as possible.
14. If I have any queries or questions regarding safe behaviour online, I will discuss them with the Head of School.
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 Greatstone Primary School Wi-Fi acceptable Use Policy.

Name

Signed:Date (DDMMYY).....