Acceptable Use Policy

Status	Current
Agreed by the Governing Board	December 2023
Review Cycle	Annually
Next Review	December 2024

Lead Staff	Lloyd Marks
Chair of Governing Body	Alex Krutnik
Headteacher	Jane Hatwell

Child/Pupil/Student Acceptable Use of Technology Statements

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

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

Early Years and Key Stage 1 (0-6)

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

- Settings should include age-appropriate information and expectations relating to use of devices, for example tablets, cloud computing, learner owned devices such as mobile phones, tablets and wearable technology.
- 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.
- 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 have read and talked about these rules with my parents/carers.

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

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

Key Stage 2 (7-11)

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

Safe

- I will 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 ask my teacher before using my own personal smart devices at school.
- I always ask permission from an adult before using the internet.
- I only use websites and search engines that a member of staff 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.

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.
- 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.

Tell

- If I see anything online that I should not or that makes me feel worried or upset, I will minimise the page and tell an adult straight away.
- If I am aware of anyone being unsafe with technology, I will report it to a member of staff.
- 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.

Alternative KS2 Statements

(With thanks to Kingsnorth Primary School)

- I understand that the school Acceptable Use Policy will help keep me safe and happy online at home and at school.
- I know that I will be able to use the internet in school for a variety of reasons, if I use it responsibly. However, I understand that if I do not, I may not be allowed to use the internet at school.
- I know that being responsible means that I should not look for bad language, inappropriate images or violent or unsuitable games, and that if I accidently come across any of these, I should report it to a teacher or adult in school, or a parent or carer at home.
- I will treat my password like my toothbrush! This means I will not share it with anyone (even my best friend), and I will log off when I have finished using the computer or device.
- I will protect myself by not telling anyone I meet online my address, my telephone number, my school's 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 not bring in memory sticks/CDs from outside of school.
- 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.
- I will tell a teacher or other adult if someone online makes me feel uncomfortable or worried when I am online using games or other websites or apps.

Shortened KS2 version (for use on posters)

- I ask a member of staff 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.

Key Stage 3/4/5 (11-18)

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

- I know that school computers, tablets, laptops, and internet access has been provided to help me with my learning and that other use of technology may not be allowed. If I am not sure if something is allowed, I will ask a member of staff.
- I know that my use of school computers and devices, systems and on-site internet access will be monitored to keep me safe and ensure policy compliance.
- I will keep my password safe and private as my privacy, school work and safety must be protected.
- I will write emails and online messages carefully and politely as I know they could be forwarded or seen by someone I did not intend.
- I know that people I meet online may not be who they say they are. If someone online suggests meeting up then I will immediately talk to an adult and will always arrange to meet in a public place, with a trusted adult present.
- I know that bullying in any form (on and offline) is not tolerated and I know that technology should not be used for harassment.
- I 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.
- I understand that it may be a criminal offence or a breach of the school policy to download or share inappropriate pictures, videos, or other material online. I understand that it is against the law to take, save or send nude or semi-nude images or videos of anyone under the age of 18.
- I will protect my personal information online.
- I will not access or change other people files, accounts, or information.
- I will only upload appropriate pictures or videos of others online and when I have permission.
- I will only use personal devices in the school if I have permission from a member of staff.
- I will respect other people's information and copyright by giving a reference and asking permission before using images or text from online sources.
- I will always check that any information I use online is reliable and accurate.
- I will make sure that my internet use is safe and legal, and I am aware that online actions have offline consequences.
- I know it can be a criminal offence to gain unauthorised access to systems ('hacking'), make, supply or obtain malware or send threatening and offensive messages.
- I will only change the settings on the computer if a teacher/technician has allowed me to.
- I know that use of the school ICT system for personal financial gain, gambling, political purposes, or advertising is not allowed.

- I understand that the school internet filter is there to protect me, and I will not try to bypass it.
- I know that if the school suspect that I am behaving inappropriately with technology, then enhanced monitoring approaches may be used, such as checking and/or confiscating personal technologies.
- If I am aware of anyone trying to misuse technology, I will report it to a member of staff.
- I will speak to an adult I trust if something happens to either myself or another student which makes me feel worried, scared, or uncomfortable.
- I will visit [www.thinkuknow.co.uk,](www.thinkuknow.co.uk) www.childnet.com and www.childline.org.uk to find out more about keeping safe online.
- I have read and talked about these rules with my parents/carers.

Alternative KS3/4 Statements

Learning

- I know that school computers, devices and internet access has been provided to help me with my learning and that other use of technology may not be allowed. If I am not sure if something is allowed, I will ask a member of staff.
- I will only use a personal device in school if I have permission from a teacher.

Safe
- I will make sure that my internet use is safe and legal, and I am aware that online actions have offline consequences.
- I know that my use of school devices and systems will be monitored, to protect me and to ensure I comply with the acceptable use policy.
- I know that people online are not always who they say they are and that I must always talk to an adult before meeting any online contacts.

Private
- I will keep my passwords private.
- I know I must always check my privacy settings are safe and private.
- I will think before a share personal information and seek advice from an adult.
- I will keep my password safe and private as my privacy, school work and safety must be protected.

Responsible

- I will not access or change other people files, accounts, or information.
- I will only upload appropriate pictures or videos of others online and when I have permission.
- I know I must respect the school systems and equipment and if I cannot be responsible then I will lose the right to use them.

- I will write emails and online messages carefully and politely as I know they could be forwarded or seen by someone I did not intend.
- I will only change the settings on the computer if a teacher/technician has allowed me to.
- I know that use of the school ICT system for personal financial gain, gambling, political purposes, or advertising is not allowed.
- I understand that the school internet filter is there to protect me, and I will not try to bypass it.
- I know that if the school suspect that I am behaving inappropriately with technology, then enhanced monitoring approaches may be used, such as checking and/or confiscating personal technologies.

Kind

- I know that bullying in any form (on and offline) is not tolerated; technology should not be used for any form or abuse or harassment.
- I will not upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.
- I will always think before I post as text, photos or videos can become public and impossible to delete.
- I will not use technology to be unkind to people.

Legal

- I know cybercrime can be a criminal offence, for example gaining unauthorised access to systems ('hacking') and making, supplying or obtaining malware.
- I know it can be a criminal offence to send threatening and offensive messages.
- I will respect other people's information and copyright by giving a reference and asking permission before using images or text from online sources.
- I understand that it may be a criminal offence or breach of the school policy to download or share inappropriate pictures, videos, or other material online.

Reliable

- I will always check that any information I use online is reliable and accurate.
- I know that people I meet online may not be who they say they are. If someone online suggests meeting up then I will immediately talk to an adult and will always arrange to meet in a public place, with a trusted adult present.

Report

- If I am aware of anyone trying to misuse technology, I will report it to a member of staff.
- I will speak to an adult I trust if something happens to either myself or another student which makes me feel worried, scared, or uncomfortable.
- I will visit www.thinkuknow.co.uk, www.childnet.com and www.childline.org.uk to find out more about keeping safe online.
- I have read and talked about these expectations with my parents/carers.

Shortened KS3/4 Version (for use on posters)

Responsible

- I know I must respect the school systems and equipment and if I cannot be responsible then I will lose the right to use them.
- I know that online content might not always be true.
- I know my online actions have offline consequences.
- I will always think before I post as text, photos or videos can become public, and impossible to delete once shared online.
- I will not use technology to be unkind to people.

Private

- I will keep my password and personal information private.
- I know I must always check my privacy settings are safe and private.

Legal

- I know that my internet use is monitored to protect me and ensure I comply with the school acceptable use policy.
- I am aware that copyright laws exist, and I need to ask permission before using other people's content and acknowledge any sources I use.
- I know cybercrime, such as hacking accounts or systems or sending abusive, threatening or offensive messages can be a criminal offence.

Report

- I know that people online are not always who they say they are and that I must always talk to an adult before meeting any online contacts.
- If anything happens online which makes me feel worried or uncomfortable then I will speak to an adult I trust and visit www.thinkuknow.co.uk.

Children/Pupils/Students 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.

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.

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

Accepting
- I do not open messages or emails from strangers.

Reliable
- I make good choices on the computer.

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

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

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.

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 member of staff.

Pupil/Student Acceptable Use Policy Agreement Form

If age appropriate to use, Settings should attach a copy of an age-appropriate AUP to this form. Settings may need to provide pupils/students and parents/carers with updated versions of the AUP as their children progress through the setting.

Stone Bay School Acceptable Use of Technology Policy
Student Agreement

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

I agree to follow the AUP when:

I use school devices and systems, both on site and at home.

Name……………………………………………… Signed…………………………………….….…

Class……………………………………………… Date……………………………………………

Parent/Carer's Name……………………………………………….………..........

Parent/Carer's Signature…………………………………………………………

Date……………………………………………………………………………………

Parent/Carer AUP Acknowledgement Form

Stone Bay School Student Acceptable Use of Technology Policy Acknowledgment

1. I have read and discussed Stone Bay School's student 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, 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 student, could have repercussions for the orderly running of the school, if a student is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school.

3. I am aware that any use of school devices and systems are appropriately filtered and may be monitored for safety and security reason 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.

4. I am aware that the school mobile and smart technology policy states that my child cannot use personal device and mobile and smart technology on site.

5. I understand that my child needs a safe and appropriate place to access remote/online learning, for example, if the school is closed in response to Covid-19. I will ensure my child's access to remote/online learning is appropriately supervised and any use is in accordance with the school remote learning AUP.

6. I understand that the school will take every reasonable precaution, including implementing appropriate monitoring and filtering systems, to ensure my child is safe when they use school devices and systems. I understand that the school cannot ultimately be held responsible for the nature and content of materials accessed online or if my child is using personal mobile or smart technologies.

7. 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.

8. 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.

9. 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.

10. 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.

11. I understand my role and responsibility in supporting the schools 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 ………………………………….. (*if appropriate*)

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 in order to access the curriculum and be prepared for modern life whilst at Stone Bay 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 student, could have repercussions for the orderly running of the school, if a student is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school.

3. I am aware that use of mobile and smart technology, such as mobile phones by children, is not permitted at Stone Bay School.

4. I understand that my child needs a safe and appropriate place to access remote/online learning, for example if the school is closed in response to Covid-19. I will ensure my child's access to remote/online learning is appropriately supervised and any use is in accordance with the school remote/online learning AUP.

5. I am aware that any use of school devices and systems are appropriately filtered and may be monitored for safety and security reason 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, to ensure my child is safe when they use school devices and systems. I understand that the school cannot ultimately be held responsible for the nature and content of materials accessed online or if my child is using personal 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 Stone Bay School's student 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 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 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

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 Stone Bay School's 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, my child's class teacher, head of year or the headteacher if I have any concerns about online safety.

I have read, understood and agree to comply with Stone Bay School's 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....................................

Acceptable Use of Technology for Staff, Visitors and Volunteers

Staff Acceptable Use of Technology Policy (AUP)

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Stone Bay School'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 students, 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 Stone Bay School'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 AUP applies to my use of technology systems and services provided to me or accessed as part of my role within Stone Bay 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 Stone Bay School's Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school's child protection policy, staff behaviour policy 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 students.

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.
   o   I will use a 'strong' password to access school systems.
   o   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 Technician.

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

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.
   o   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.
   o   Any data being removed from the school site, such as via email suitably protected. This may include data being encrypted by a method approved by the school.
   o   Sensitive data covered under GDPR will not be stored on memory sticks, other portable USB devices or CD's.

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.

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 IT Technician as soon as possible.

17.   If I have lost any school related documents or files, I will report this to the IT Technician and school Data Protection Officer as soon as possible.

18.   Any images or videos of students will only be used as stated in the school camera and image use policy. I understand images of students must always be appropriate and should only be taken with school provided equipment and only be taken/published where students 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.

20.   I will promote online safety with the students in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:
    o   exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used.
    o   creating a safe environment where students feel comfortable to report concerns and say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.
    o   involving the Designated Safeguarding Lead (DSL) or a deputy as part of planning online safety lessons or activities to ensure support is in place for any students who may be impacted by the content.
    o   make informed decisions to ensure any online safety resources used with students is appropriate.

21.   I will report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the DSL.

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 behaviour policy and the school mobile technology policy and the law.

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 behaviour policy, social media policy and the law.

25.   As outlined in the staff behaviour policy:
   o   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.
   o   I will not discuss or share data or information relating to students, staff, school business or parents/carers on social media.

26.   My electronic communications with current and past students and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.
   o   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, Class Dojo or telephone number.
   o   I will not share any personal contact information or details with students, such as my personal email address or phone number.
   o   I will not add or accept friend requests or communications on personal social media with current or past students and/or their parents/carers.
   o   If I am approached online by a current or past students or parents/carers, I will not respond and will report the communication to my line manager and Designated Safeguarding Lead (DSL).
   o   Any pre-existing relationships or situations that compromise my ability to comply with the AUP or other relevant policies will be discussed with the DSL and/or headteacher.

Policy concerns

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 students or parents/carers online to the DSL in line with the school child protection policy.

31. I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher, in line with school child protection policy and/or 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 and/or the headteacher.

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 messages/emails on our systems, to monitor policy compliance and to ensure the safety of students 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 staff behaviour policy.

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 behaviour 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 Stone Bay School'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 (DDMMYY)..

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 Stone Bay School ensure that all visitors and volunteers understand the schools 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 Stone Bay 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 Stone Bay School's AUP should be read and followed in line with the school staff behaviour policy.

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.

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 not allowed to take images or videos students.

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 students.

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

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

9. 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

10. I understand that I am not allowed to use personal mobile phones on site.

Online communication, including the use of social media

11. 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.
    o   I will take appropriate steps to protect myself online.
    o   I will not discuss or share data or information relating to students, staff, school business or parents/carers on social media.
    o   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 behaviour policy and the law.

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

Policy compliance, breaches or concerns

13. 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 and/or the headteacher.

14. 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.

15. 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.

16. 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.

17. 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/messages on school systems, to monitor policy compliance and to ensure the safety of students, staff and

visitors/volunteers. 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 students or parents/carers online to the Designated Safeguarding Lead in line with the school child protection policy.

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

20. I understand that if the 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 Stone Bay School'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
(DDMMYY)..
....

Wi-Fi Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all members of the school community are fully aware of the school boundaries and requirements when using the school Wi-Fi systems and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

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

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

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 Stone Bay School's Acceptable Use of Technology Policy (AUP), online safety policy and behaviour policy which all students /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 as soon as possible.

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

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

I have read, understood and agreed to comply with Stone Bay School's Wi-Fi Acceptable Use Policy.

Name ....

Signed: ....Date (DDMMYY).........................

Acceptable Use Policy (AUP) for Remote/Online Learning

Remote/Online Learning AUP - Staff Statements

Stone Bay School Staff Remote/Online Learning AUP

The Remote/Online Learning Acceptable Use Policy (AUP) is in place to safeguard all members of the Stone Bay school 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 Office 365, Google and Class Dojo.
   - These systems have been assessed and approved by the headteacher/a member of Senior Leadership Team (SLT).

2. Staff will only use school managed or specific, approved professional accounts with students and parents/carers.
   - Use of any personal accounts to communicate with students or parents/carers is not permitted.
     - o Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the Designated Safeguarding Lead (DSL).
   - Staff will use work provided equipment where possible e.g. a school laptop, tablet, or other mobile device.

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

4. All remote/online lessons will be formally timetabled; a member of SLT, DSL and/or head of department is able to drop in at any time.

5. Live-streamed remote/online learning sessions will only be held with approval and agreement from the headteacher/a member of SLT.

Data Protection and Security

6. Any personal data used by staff 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.

8. All participants will be made aware if a system records activity.

9. Staff will not record lessons or meetings using personal equipment.

Session management

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

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

12. When live streaming with students:
    ● contact will be made via a parents/carers account.
    ● at least 2 members of staff will be present.
        o If this is not possible, SLT approval will be sought.

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

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

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

Behaviour expectations

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

17. All participants are expected to behave in line with existing school policies and expectations.

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

19. 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.

20. 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

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

22. 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 SLT.

23. 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.

24. Any safeguarding concerns will be reported to the Designated Safeguarding Lead, in line with our child protection policy.

I have read and understood the Stone Bay School Acceptable Use Policy (AUP) for remote/online learning.

Staff Member Name:
....

Date...
....

Remote/Online Learning AUP Template – Pupil/Student Statements

Stone Bay School Student 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 Microsoft Teams, Google Meet.
   - I should read and talk about these rules with my parents/carers.
   - remote/online learning will only take place using Google and Microsoft and during usual school times.

2. Only members of the Stone Bay School community can access Stone Bay's systems.
   - I will only use my school provided email accounts and login to access remote learning.
   - I will use privacy settings as set up by 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
   - Not taking or recording images/content without agreement from the teacher and/or those featured.

4. When taking part in live sessions I will
   - 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 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. I understand that inappropriate online behaviour or concerns about my or others safety during remote/online learning will be taken seriously.