Stone Bay School.
Policy Document.

Non Statutory Group E Policy.

E4: Online safety. Acceptable Use Policy.

Online safety: Child Net.
Online Safety: KCC.
Policy Guidance.

Author:	Joe White
Approved by Board of Governors:	Tuesday, 24 January 2017
Date of Publication:	Tuesday, 24 January 2017

2 year review cycle. **Date for Review:** **Friday, 04 January 2019**

Signed. Richard Farr. Date: 24/01/2017
Chair of Governors.

Signed. Billy Mc Inally. Date: 24/01/2017
Headteacher.

Mission Statement.

We accept all students **as they are** and believe that every one of them is **entitled** to the very **best education**, delivered in an **environment** that is **supportive**, **caring** and **safe**.

Our goal is to develop our students to become:

· **Successful** Learners.

· As **independent** as possible.

· **Confident** individuals and self-advocates.

· **Effective** communicators and **contributors**.

· **Responsible** citizens.

We will do this by working to **ensure we get every aspect of their provision just right**, helping them to achieve academically, personally, socially and morally.

Stone Bay School: *"**getting it right for every student**"*.

Stone Bay School and online safety

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

Online safety covers issues relating to children and young people as well as adults, and their safe use of the Internet, social media, mobile phones, tablets and other electronic communications technologies, both in and out of school or settings. It includes education for all members of the community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children. It should be noted that the use of the term 'online safety' rather than "e-Safety" reflects a widening range of issues associated with technology and a user's access to content, contact with others and behavioural issues and a move away from a focus as online safety as an ICT issue. For this reason online safety is an essential part of our PHSE/Wellbeing curriculums.

As a school we endeavour to develop in our students' skills and attitudes that equip them for our increasingly technological society. To do this we all have to work within a framework, which allows for safety and security and raises awareness of issues affecting our school and the wider community. A breakdown of potential risks is available in appendix 1.

Internet use is a part of the statutory curriculum and a necessary tool for staff and students. Within a supported context, students will learn how to locate, retrieve and exchange information using ICT.

The school's Internet access has be designed expressly for pupil use and includes the filtering of inappropriate material using tools provided by the Local Authority. Students will be taught what Internet use is acceptable and given clear objectives for Internet use. They will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

The school will ensure that the use of Internet derived materials by staff and students complies with current copyright and intellectual property law. Students should be taught to be critically aware of the materials they read on the internet and shown how to validate information before accepting its accuracy.

The school has a number of students with an extensive internet presence through the use of online gaming, social networks and Youtube channels. The curriculum makes students aware of the dangers of interacting with strangers online and the channels to access if they are the victims of abuse or bullying online.

Online safety encompasses issues both within school and outside of school. Due to the rapid pace of change it is likely that the student's may use the internet differently to staff. For this reason we will work to gain an understanding of how our students use the internet and emerging technologies. It is essential that staff keep up to date with changing and emerging trends. Online safety training is provided yearly for all staff. The online safety coordinator is also a DSL and attends regular training and awareness training.

Writing and Re viewing the online safety acceptable use policy

The purpose of the Stone Bay School online safety policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that Stone Bay School is a safe and secure environment.
- Safeguard and protect all members of Stone Bay School community online.
- Raise awareness with all members of Stone Bay School community regarding the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to be followed

This policy relates to the following Stone Bay documents, policies and protocols;

- Child protection policy and procedures
- Social Networking
- Mobile 'Phone Protocol' covering taking photos and creating imagines including students at SBS.

Stone Bay School has an online Safety Coordinator who is the school ICT subject leader and a trained Designated Safeguarding Lea. The key responsibilities:

- Acting as a named point of contact on all online safety issues and liaising with other members of staff and agencies as appropriate.
- Keeping up-to-date with current research, legislation and trends. Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Monitor and record the school/settings online safety incidents to identify gaps/trends and update the education response to reflect need and to report to the school management team, Governing Body and other agencies as appropriate.
- Liaising with the local authority and other local and national bodies as appropriate.
- Reviewing and updating online safety policies, Acceptable Use Policies (AUPs) and other procedures on a regular basis with stakeholder input.
- Ensuring that online safety is integrated with other appropriate school policies and procedures.
- Leading an online safety team/group with input from all stakeholder groups.

This policy has been written by the school, building on the Kent online safety Policy and government guidance.

Student views

Student views were sort to inform this policy in. This is essential to ensure our provision and safeguarding is focussed on the correct areas. It also ensures our curriculum is relevant to the evolving needs of our learners.

Internet Access and Learning

Within the school a number of internet enabled devices are provided for use by classes and individual students to support the curriculum. The majority of these access the internet through our monitored and filtered wi-fi. Students are not to access these devices without supervision. They may be used in a range of teaching environments. When monitoring use staff should be aware of the proximity of other students and their specific needs and sensitivities. Students have stated they benefit from using iPads and android devices in lessons.

School ICT systems capacity and security will be constantly reviewed. Virus protection will be updated regularly by the network manager.

Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use (see Appendix 1).

E-mail

Email is an essential means of communication for staff and is encouraged in our students. It is an effective way of ensuring our students maintain regular contact with family members and friends and can bring significant educational benefits.

Students may only use approved e-mail accounts on the school system. Students email use will be appropriately monitored by staff. They must not be allowed to reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.
E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

The forwarding of chain letters is not permitted.

Published Content and Stone Bay School Website

Stone Bay School has a website available at www.stone-bay.kent.sch.uk. Administrative Access to the website is limited to HR manager, Clerk to the governors, network manager, Assistant Headteacher, Headteacher

The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education and based on the following document https://www.gov.uk/what-maintained-schools-must-publish-online

- The contact details on the website will be the school address, email and telephone number. Staff or students' personal information will not be published.
- The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- Students work will only be published with their permission or that of their parents/carers.
- The administrator account for the school website will be safeguarded with an appropriately strong password.
- The school will post information about safeguarding, including online safety on the school website.
- The Headteacher has overall responsibility for ensuring that content on the school website is accurate and appropriate.

Publishing Students' Images and Work

Photographs that include students will be selected carefully and will not enable individual students to be identified by name. Students full names will not be used anywhere on the website or external electronic communications, particularly in association with photographs. Parents have to agree in writing to images of their child being used on the school website or other published materials.

Developing effective practice in using the Internet for teaching and learning is essential. Students need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet. Any material published publically must be able to be reviewed by a member of the leadership team

Social Networking and Personal Publishing

The school will block/filter access to social networking sites. Students are advised never to give out personal details of any kind which may identify them or their location.

Due to their vulnerability it is essential that students are aware of the risk of using social networks. The rising popularity of social media and networking means it is no longer appropriate to purely block or encourage parents to block access. Throughout the curriculum reference is made to online safety. We will conduct individual or group sessions to meet an identified need or address issues arising throughout the school year.

Expectations regarding safe and responsible use of social media will apply to all members of the Stone Bay School community and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger, Apps.

Staff will support parents with information about online safety including a bi-annual digital parenting magazine. Parents are encouraged to raise concerns about student's internet use outside of school. We are aware a number of students maintain Facebook, Twitter, Snapchat and Instagram accounts. This group of students undertake additional online safety learning sessions. They have been made aware that staff or not able to become friends with them on any social network.

Students bringing mobile internet enabled devices into school from home will be managed on an individual basis. the use of personal networks and hotspots on site is forbidden. Due to the vulnerability of other student's camera enabled devices will not be permitted to be used in class or residential settings. Students will be asked to leave devices in their bag or will be stored for them.

In response to student wishes and due to the extensive learning potential of Youtube.com this domain has been unblocked and is fully accessible on the school system. At present students are restricted from logging onto their own accounts and uploading videos on the school system. This was felt to be an appropriate compromise to ensure safe access for all our students.

Any breaches of school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with the relevant school policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

Managing Filtering

The school will work with the LA, DfE and the Internet Service Provider to ensure systems to protect students are reviewed and improved.

- The school uses Light Speed filtering system which analyses and blocks (in real time), sites that fall into specific categories see appendix 3.
- However if staff or students discover an unsuitable site, it must be reported to the online safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Requests to allow access to specific websites will be requested via email to the network manager who will liaise with the online safety coordinator and the ISP to ensure the suitability of using the site in school.

Managing Videoconferencing

IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet. Students should ask permission from the supervising teacher before making or answering a videoconference call. Videoconferencing will be appropriately supervised for the students' age. Staff using video conferencing need to be ensure no personal student information is visible.

Currently Skype is permitted for use on the system but will need to be installed on request by the network manager. In addition the following guidance should be followed.

- Students will ask permission from a teacher before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately for the students' age and ability. (schools should list how this will be enforced and achieved)
- Parents and carers consent will be obtained prior to children taking part in videoconferences.
- When recording a videoconference session written permission will be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material will be stored securely.

- If third party materials are to be included, the school will check that recording is acceptable to avoid infringing the third party intellectual property rights.
- The school will establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site the school will check that they are delivering material that is appropriate for the class.

Sexting and online abuse.

Self-Generated Indecent Images of Children (SGIIOC or "Sexting") can be defined as images or videos generated by children under the age of 18 that are of a sexual nature or are considered to be indecent. These images may be shared between children and young people and/or adults via a mobile phone, webcam, handheld device or website.

It is important to be aware that young people involved in sharing sexual videos and pictures may be committing a criminal offence. Specifically, crimes involving indecent photographs (including pseudo images) of a person under 18 years of age fall under Section 1 of the Protection of Children Act 1978 and Section 160 Criminal Justice Act 1988. Under this legislation it is a crime to take an indecent photograph or allow an indecent photograph to be taken, make an indecent photograph (this includes downloading or opening an image that has been sent via email); distribute or show an indecent image, advertise indecent images and possess an indecent image or possess an indecent image with the intention of distribution. This applies even if the images are sent or shared by someone under the age of 18 with "consent". "Sexts" may be viewed as police evidence and it is essential than schools secure such devices and seek advice immediately when dealing with concerns.

The current Association of Chief Police Officers (ACPO) position is that:
'*ACPO does not support the prosecution or criminalisation of children for taking indecent images of themselves and sharing them. Being prosecuted through the criminal justice system is likely to be upsetting and distressing for children especially if they are convicted and punished. The label of sex offender that would be applied to a child or young person convicted of such offences is regrettable, unjust and clearly detrimental to their future health and wellbeing.*'

Formal advice on images on electronic devices.

Stone Bay School views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Leads

If the school are made aware of incident involving indecent images of a child the school will:

- Act in accordance with the schools child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.
- Immediately notify the Designated Safeguarding Lead.
- Store the device securely.
- Consider the vulnerabilities of children(s) involved (including carrying out relevant checks with other agencies)

- Make a referral to children's social care and/or the police (as needed/appropriate).
- Put the necessary safeguards in place for children e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- Inform parents/carers about the incident and how it is being managed.
- Review the handling of any incidents to ensure that the school is implementing best practice and the leadership team will review and update any management procedures where necessary.

Stone Bay School will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.

Stone Bay School views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Leads. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.

If the school are made aware of incident involving online child sexual abuse of a child then the school will:

- Act in accordance with the schools child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.
- Immediately notify the designated safeguarding lead.
- Store any devices involved securely.
- Immediately inform Kent police via 101 (using 999 if a child is at immediate risk) or alternatively to CEOP by using the Click CEOP report form: http://www.ceop.police.uk/safety-centre/
- Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse
- Make a referral to children's social care (if needed/appropriate).
- Put the necessary safeguards in place for pupil(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- Inform parents/carers about the incident and how it is being managed.

The school will take action regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.

Radicalistion and Online Extremism – PREVENT

From 1st July 2015 specified authorities, including all schools are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015(“the CTSA 2015”), in the exercise of their functions, to have “due regard to the need to prevent people from being drawn into terrorism” This duty is known as the Prevent duty. The statutory Prevent guidance summarises the requirements on schools as undertaking risk assessment, working in partnership, staff training and IT policies.

The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of students. Schools will need to highlight specifically how internet use will be monitored either here or within subsequent sections. When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the school safeguarding policy.

The Prevent team can be contacted for advice and support in respect of Prevent via channel@kent.pnn.police.uk and prevent@kent.pnn.police.uk

Cyberbullying

Online or cyberbullying can be defined as the use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone.

Mobile, internet and wireless technologies have increased the pace of communication and brought significant benefits to users worldwide but their popularity provides increasing opportunity for misuse through 'cyberbullying', with worrying consequences. It's crucial that students and staff use their devices and the internet safely and positively and they are aware of the consequences of misuse. As technology develops, bullying techniques can evolve to exploit it.

Cyberbullying, along with all other forms of bullying, of any member of the Stone Bay School community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.

- All incidents of online bullying reported will be recorded.
- There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
- Students, staff and parents/carers will to keep a record of the bullying on the school’s recording system.

- The school will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

Managing Emerging Technologies

Emerging technologies will be examined for educational benefit. Appropriate risk assessments may need to be formulated.

Mobile phones will not be used by staff or students during lessons or formal school time unless authorised by the teacher leading the class. The sending of abusive or inappropriate text messages is forbidden. Staff will not contact students by telephone outside of communication lessons and only in school time. Mobile phones provided to senior staff for on call duties may be used within school for school related purposes only.

Apps including PUPIL ASSET.

The Headteacher is ultimately responsible for the security of any data or images held of children. Personal staff mobile phones or devices will not be used for any apps which record and store children's personal details, attainment or photographs. Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs.

Protecting Personal Data

Devices including USB drives must be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Authorising Internet Access

All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource. The school will keep a record of all staff and students who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a student's access be withdrawn.

Assessing Risk

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor KCC can accept liability for the material accessed, or any consequences of Internet access.

A risk assessment need to be completed for any device that poses an enhanced risk.

Password policy

All users are requireded not to share passwords or information with others and not to login as another user at any time. Staff and students must always keep their password private and must not share it with others or leave it where others can find it. All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private and use different passwords for each account. We require staff and students to use STRONG passwords for access into our system.

Handling online safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff though should be reported to the online safety coordinator. Any complaint about staff misuse must be referred to the Headteacher.

A minor transgression of the school rules may be dealt with by a member of staff. Other situations could potentially be serious and a range of sanctions may then be required, which should be linked to the school's disciplinary policy.

Potential child protection or illegal issues must be referred to the school Designated Safeguarding Lead (DSL) or online safety lead (Joe White). Advice on dealing with illegal use of internet or technology should be discussed with the Kent Police or the Education Safeguards Team.

Incidents and concerns should also be dealt with in line with Kent Police's Schools Policy.

http://www.kent.police.uk/about_us/policies/crime-intelligence/n17.html

Communication

Online safety rules is posted in all networked rooms and discussed with the students throughout the year in class in in whole school assemblies. Students will be informed that network and Internet use will be monitored.

Staff and the online safety Guidance

All staff have full access to this School online safety Guidance and its importance will be explained and highlighted in the staff handbook. Staff will be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. Breaches of such professional conduct may be dealt through our formal disciplinary procedures.

Enlisting Parents' Support

Parents' attention will be drawn to the School online safety guidance in newsletters. The guidance will be available to parents on the school website.

Useful Contacts

- Kent e–Safety Officer, Children's Safeguards Team, Families and Social Care, Kent County Council. The online safety Officer is Rebecca Avery email: esafetyofficer@kent.gov.uk Tel: 01622 221469
- Children's Officer for Training & Development, Children's Safeguards Team, Families and Social Care, Kent County Council. The Children's Officer for Training & Development is Mike O'Connell email: mike.oconnell@kent.gov.uk Tel: 01622 696677
- Cyberbullying - http://www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/e-safety/cyberbullying
- Think U Know: www.thinkuknow.co.uk
- Childnet: www.childnet.com
- Kidsmart: www.kidsmart.org.uk
- Digital Literacy Scheme of Work: www.digital-literacy.org.uk

Appendix 1: KCC Categories of risk:

	Commercial	**Aggressive**	**Sexual**	**Values**
Content Child as recipient	Advertising Spam Copyright Sponsorship	Violent content Hateful Content	Pornographic content Unwelcome sexual comments	Bias Racist and extremist content Misleading info/advice Body Image and self esteem Distressing or offensive content

Contact Child as participant	Tracking Harvesting Sharing personal information	Being bullied, harassed or stalked	Meeting strangers Grooming Online Child Sexual Exploitation	Self-harm and suicide Unwelcome persuasions Grooming for extremism
Conduct Child as actor	Illegal downloading Hacking Gambling Privacy Copyright	Bullying, harassing or stalking others	Creating and uploading inappropriate or illegal content (including "sexting") Unhealthy/inappropriate sexual relationships Child on child sexualised or harmful behaviour	Providing misleading information and advice Encouraging others to take risks online Sharing extremist views Problematic Internet Use or "Addiction" Plagiarism

Appendix 2

These are the website categories that are currently blocked against student use:

* Adult	Sites which display full or partial nudity in a sexual context
* Advertising	Unwanted advertisements on websites
* Allowed Staff	Adverts which are required for websites to function correctly ie 4 on Demand
* Blogs	Web blogs
* Dropbox	Dropbox.com
* Facebook	Facebook.com
* File Hosting	Filehosting websites: dropbox, rapid share, mega upload...
* Forums	Message boards, bulletin boards, and other discussion web forums
* Forums (Instant Messaging)	Sites that enable instant messaging
* Forums (Moderated)	Moderated Web Forums
* Games (Educational)	Educational games for students
* Games (General)	Web based and Online games
* Games (Inappropriate)	Violent or lewd online games
* Logmein	Logmein.com
* MP3	Sites providing MP3s and other audio formats downloads
* Nudity	Depictions of nude or seminude human forms, singly or in groups, not overtly sexual in intent or effect

* Search Engines (Blocked)	Search Engines which do not have safe search functions
* Security (Remote Access)	Websites which enable remote access to PCs
* Security (Risk)	Sites found to be hosting known and potential exploit code
* Software Downloads	Application downloads: Download.com, sourceforge.net, brothersoft.com...
* Sports (Violent)	Sites focused on Violent Sports
* Streaming Video	Video Streaming Sites (Non YouTube or Google Video)
* Spotify	Spotify.com
* Tasteless	Sites with content that is gratuitously offensive or shocking
* Tumblr	Tumblr.com
* Twitter	Twitter.com
* Video Sites	Youtube and Google Video
* Skydrive	Skydrive.live.com
* Local-Security.virus	Conflicker Ips
Local-Block	Local Override of Allowed Domains
access-denied	Sites of Pages that Deny Access, or are unauthorized to access
access-denied	Sites of Pages that Deny Access, or are unauthorized to access
adult	Adult Products, Services, Situations of humor
adult.art	Adult art
adult.bodyart	Body art, tattoos, body piercings
adult.games	Adult games
adult.language	Strong language
adult.lifestyles	Adult lifestyles
alcohol	Production, promotion and sale of alcoholic beverages
drugs	Sites promoting illicit and illegal drug use
gambling	Gambling, casinos, betting, lottery and play-for-cash/sweepstakes
offensive	Websites considered to be offensive to both adults and children
porn	Pornography related sites
porn.child	Porn sites involving children
suspicious	Recently discovered sites with suspicious words or phrases
violence	Sites promoting violence and anarchy
forums	Unmoderated Personal Expression
forums.blogs	Webblogs
forums.dating	Dating websites such as friendfinder.com, eharmony.com, match.com, etc.
forums.im	Instant messaging
forums.newsgroups	Newsgroups, usenet and subscription newsletters
forums.p2p	Peer to peer sites

forums.personals	Personal web pages and personal ads
forums.social_networking	Social networking and related websites such as myspace.com, facebook.com, orkut.com
parked	Web sites using internet scams in an attempt to get personal information
security	Security risks
security.nettools	Net tools, remote admin tools, internet server and client applications
ads	Ad servers and advertising companies
shopping.spam	Shopping websites that use spam email for marketing
spam	Sources of spam mail that does not involve porn, gambling, or drugs
computers.filehosting	Image, filehosting, shareware, freeware websites
weapons	Web sites about guns, swords, knives, and other weapons
education.games	Educational games for kids
kids_and_teens.chat	Monitored chat websites suitable for kids
expired	Domains whose registration has expired
plagiarism	Websites that sell term papers, research papers and other ways to help students cheat
audio-video	Sources of MP3s, mpegs, and streaming
games	Games, anime, cartoons, wallpapers and screen savers
shopping.auctions	Auctions

And the following are blocked against Staff access:

Adult	Sites which display full or partial nudity in a sexual context
Advertising	Unwanted advertisements on websites
Facebook	Facebook.com
Nudity	Depictions of nude or semi-nude human forms, singly or in groups, not overtly sexual in intent or effect
Proxy Avoidance	Proxy Avoidance Websites
Security (Risk)	Sites found to be hosting known and potential exploit code
Tasteless	Sites with content that is gratuitously offensive or shocking
Twitter	Twitter.com
adult.art	Adult art
adult.bodyart	Body art, tattoos, body piercings
adult.games	Adult games
adult.language	Strong language
adult.lifestyles	Adult lifestyles

drugs	Sites promoting illicit and illegal drug use
offensive	Websites considered to be offensive to both adults and children
suspicious	Recently discovered sites with suspicious words or phrases
suspicious.script	Websites whose only content is javascript - frequently used to hide porn sites
violence	Sites promoting violence and anarchy
violence.hate	Sites that promote hate against different groups
violence.weapons	Web sites about guns, swords, knives, and other weapons
adult	Adult products, services, situations and humor
pornography	All types
security.spyware	Gambling, casinos, betting, lottery and play-for-cash/sweepstakes
forums.dating	Dating websites like friendfinder, eharmony, and match.com
forums.newsgroups	Newsgroups, usenet and subscription newsletters
forums.personals	Personal web pages and personal ads
forums.social_networking	Social networking and related websites such as myspace, facebook, and orkut.
forums.p2p	Peer to peer sites
parked	Pay per click hosting web sites that park expired domains
security.proxy	Web proxy servers and open SMTP relays
security.ware	Sites promoting illegal access and sharing of software and other copyrighted material
security	Security risks
security.hacking	Computer hacking
security.phishing	Web sites of internet scams that try to get personal information
security.spyware	Spyware - advertising supported software
security.virus	Viruses, malware, trojans, backdoors, hacker tools
security.virus_ignore	Virus signatures that should be ignored
ads	Ad servers and advertising companies
ads.banner-ads	Banners ads
ads.html-ads	HTML ads
ads.popup-ads	Popup ads
shopping.spam	Shopping websites that use spam email for marketing
spam	Sources of spam mail that does not involve porn, gambling, or drugs

Safeguarding, Equality and Equal Opportunities Statement

Stone Bay School, and all policies and procedures, will promote equality of opportunity for all students and staff from all social, cultural and economic backgrounds. The school will ensure that no student or staff member is disadvantaged, discriminated against or treated less favourably because of their gender (including gender reassignment), race, disability, religion or belief, sexual orientation or due to pregnancy or maternity.

Stone Bay School aims to;

- Foster good relationships and create effective partnerships with all sections of the community
- Ensure that the school's service delivery, commissioning and employment practices will not discriminate unlawfully, either directly or indirectly
- Provide an environment free from fear and discrimination, where diversity, respect and dignity are valued and celebrated

All aspects of Safeguarding will be embedded into school life and will remain the responsibility of all members of our school community.