

On-line Safety with Student User Agreement Forms

1. What is an On-line Safety Policy?

This On-line Safety Policy sets out the roles, responsibilities and procedures for the acceptable, safe, and responsible use of all digital and communication technologies, including the use of school based devices, the internet, email, instant messaging, and other social networking technologies, mobile phones, and games, to safeguard adults and students at Southbank. It details how the school will provide support and guidance to parents and the wider community (where appropriate) for the safe and responsible use of these technologies. It also explains procedures for any unacceptable or misuse of these technologies by adults or students.

2. Why have an On-line Safety Policy?

The use of the internet as a tool to develop teaching, learning and administration has become an integral part of school and home life. There are always going to be risks using any form of communication, which lies within the public domain. Therefore, it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst students use these technologies. These risks include:

- Being vulnerable to inappropriate contact from strangers
- Cyber-bullying
- Illegal activities of downloading or copying any copyright materials and file-sharing via the internet or mobile devices
- Issues with spam and other inappropriate email
- Online content which is abusive, offensive, or pornographic
- The use of social media to encourage extremism
- Viruses

It is also important that staff are clear about the procedures; for example only contacting students about homework via a school email address or the school's Virtual Learning Environment (VLE), Firefly, not via personal emails.

Whilst Southbank will endeavour to safeguard and mitigate against all risks, it will never be able to completely eliminate them all. Any incidents that may come to its notice will be dealt with quickly and according to the school's policies to ensure the school continues to protect students.

It is the duty of the school to ensure that students, teachers, administrative staff, and visitors are protected from potential harm whilst they are on school premises.

The involvement of students and parents is also vital to the successful use of online technologies. This policy thus also aims to inform how parents and students are part of the procedures, and how students are educated to be safe and responsible users so that they can make good judgments about information they see, find and use.

3. Aims of this policy

- To ensure the safeguarding of all students within the school by detailing appropriate and acceptable use of all online and digital technologies
- To outline the roles and responsibilities of all students, staff and parents

- To ensure all students, staff and parents are clear about procedures for misuse of any online technologies
- To develop links with parents and the wider community to ensure continued awareness of online technologies

4. Students

Our students are:

- Involved in the review of our On-line Safety Agreement through discussion in lessons and other forums
- Responsible for following the On-line Safety Agreement whilst within school as agreed each academic year or whenever a new student starts at the school for the first time, and required to sign that they have read and understood the rules
- Taught to use the internet in a safe and responsible manner through, for example, ICT and PSPEE lessons
- Taught to immediately tell an adult about any inappropriate materials or contact from someone they do not know
- Made aware of the potential use of on-line digital technologies to expose young people to inappropriate contact from strangers and to extremist ideas and know what to do if they encounter such issues
- Taught and encouraged to consider the implications for misusing the internet and, for example, posting inappropriate materials to websites
- Taught that the downloading of materials, for example music files and photographs, needs to be appropriate and 'fit for purpose', based on research for school work, and be copyright free
- Taught to understand what is meant by e-safety through age appropriate delivery
- Taught that sending malicious or hurtful messages outside of the school can become a matter whereby the school may set sanctions or involve outside agencies such as the police
- Taught not to put themselves at risk online or through mobile phone use and taught what to do if they are concerned they have put themselves at risk
- Given explicit guidelines and procedures for using mobile phones and other personal devices in school and are expected to abide by our On-line Safety Policy
- Must connect to the internet whilst on premises owned or rented by Southbank using the Southbank Student wireless network, and must not circumvent internet access by using a personal device's cellular data services (3G, 4G, or other)

4.1 In the event of inappropriate use by students

Should a student be found to deliberately misuse digital or on-line facilities whilst at school, then appropriate sanctions will be applied. If a student accidentally accesses inappropriate materials the student is expected to report this to an appropriate member of staff immediately and take action to minimize the screen or close the window. Deliberate abuse or damage of school equipment will result in parents being billed for the replacement costs of the equipment. Should a student use the internet whilst not on the school premises in such a way as to cause hurt or harm to a member of the school community, the school will act quickly and in accordance with our *Behaviour Policies*.

5.0 Staff

It is the responsibility of all adults within the school to:

- Be up to date with e-safety knowledge appropriate for different age groups
- To ensure they are familiar with and fully support the student On-line Safety Agreement
- To be vigilant when using technology as part of lessons
- To model safe and responsible use of technology
- To provide reminders and guidance to students on On-line Safety
- Ensure that students are protected and supported in their use of online technologies, and that they know how to use them in a safe and responsible manner
- Not leave a computer or other device unattended whilst they are logged on
- Lock away or safely secure all portable ICT equipment when not in use
- Not connect with any current Southbank student under the age of nineteen on any social networking site, or via personal mobile phones and follow the school's Social Media Policy
- Protect confidentiality and not disclose information from the network, or pass on security passwords
- Make sure that any information subject to Data Protection is not stored on unencrypted portable media or transported in an insecure form
- Protect confidentiality and not disclose information from the network, or pass on security passwords
- Use their discretion when communicating electronically about work-related issues and not bring the school's reputation into disrepute
- Follow the school's 'dos' and 'don'ts' in our *Email Best Practice Policy*
- Not make or take personal calls or engage in personal texting when they are on duty
- Report any concerns about a student related to safeguarding and e-safety to the Designated Safeguarding Lead
- Report accidental access to inappropriate materials to the Director of Information Systems or a Network Manager so that inappropriate sites are added to the restricted list
- Only use school owned devices and memory cards to take photographs or videos.

5.1 In the event of inappropriate use by staff

If a member of staff is believed to have misused the internet or network in an abusive or illegal manner from school, a report must be made to the Principal and Executive Principal, along with the Director of Information Systems immediately. Safeguarding procedures must be followed to deal with any serious misuse, a report filed, and all appropriate authorities contacted as necessary.

6. Parents and visitors

All parents have access to a copy of this On-line Safety Policy on our website. Parents are asked to explain and discuss the rules with their child, where appropriate, so that they are clearly understood and accepted.

As part of the approach to developing e-safety awareness with students, the school may offer parents the opportunity to find out more about how they can support the school to keep their child safe whilst using online technologies beyond school; this may be by offering parent education sessions or by providing advice and links to useful websites. The school wishes to promote a positive attitude to using the internet and therefore asks parents to support their child's learning and understanding of how to use online technologies safely and responsibly.

Parents should be aware that the school cannot take responsibility for a student's misuse or abuse of IT equipment when they are not on the school premises. This includes social networking with other students, and the possibility of students accessing inappropriate content. However should parents or guardians become aware of an issue we strongly encourage prompt communication with the school so we can offer advice and support. The school has a duty to report serious concerns to local authority safeguarding teams or to the police, in line with statutory requirements.

6.1 Wifi access

Parents and visitors to the school are expected to abide by this policy. Should visitors wish to access the internet via the school's wifi, they will be issued with a time sensitive password. Access is only permitted once they have agreed to the school's terms and conditions.

6.2 Video and photography at school events

Parents are asked to be considerate when taking videos or photographs at school events and are requested not to publish material of other children in any public forum without the permission of the relevant family. It is illegal to sell or distribute recordings from events without permission. Any parent who does not wish for their child to be videoed or photographed at school events by other attendees must notify the school in advance and in writing.

7.0 The School's responsibilities

The school takes its responsibilities in relation to the acceptable use of technology by students and adults seriously and understands the importance of monitoring, evaluating and reviewing its procedures regularly.

7.1 Filtering and safeguarding measures

The school's internet has a robust filtering system which is set at an appropriate level such that inappropriate content is filtered. The system logs all attempts to access the internet, including all attempts to access inappropriate content. All such attempts are reported to the Director of Information Systems.

Anti-virus, anti-spyware, junk mail and SPAM filtering is used on the school's network, stand-alone PCs, laptops and tablets, and is updated on a regular basis. Security measures are in place to ensure information about our students cannot be accessed by unauthorised users.

Strong encryption is used on the wireless network to provide good security.

7.2 Email use

The school provides school email addresses for students (Grade 3 to 12) to promote safe and efficient communication in the school. Student email accounts are provided by Google. Google is registered with the US-EU Safe Harbour agreement, which helps ensure that their data protection compliance meets EU standards for educational institutions.

7.3 The school's use of images and videos

The school abides by the Data Protection Act 1998 and understands that an image or video is considered personal data. It seeks written consent from parents to publish images or videos for external publicity purposes, such as the website, and for internal purposes, such as the Yearbook or on the Parent Portal. Parents and Guardians may withdraw their permission at any time by informing the administration team in writing at a specific campus.

Staff are not permitted to use their own devices or memory cards to record videos or photographs of students and when storing images within the school's network are requested to only use the student's first name.

7.4 The curriculum and tools for learning

The school teaches our students how to use the internet safely and responsibly, for researching information, exploring concepts, deepening knowledge and understanding, and communicating effectively in order to further learning, through ICT and/or PSPEE lessons. The following concepts, skills and competencies are taught by the end of Grade 10:

- Digital citizenship
- Future work skills
- Internet literacy
- Making good judgments about websites and emails received
- Knowledge of risks such as viruses, and opening mail from a stranger
- Access to resources that outline how to be safe and responsible when using any on-line technologies
- Knowledge of copyright and plagiarism issues
- file-sharing and downloading illegal content
- Uploading information – knowing what is safe to upload, and not to upload personal information
- Where to go for advice and how to report abuse

These skills are taught explicitly within the ICT curriculum but are likely to be covered in other subjects; students are taught skills to explore how online technologies can be used effectively, in a safe and responsible manner. Further details about the content of the curriculum related to ICT can be found in the *ICT and PSPEE Scope and Sequence* documentation.

7.5 Monitoring

It is the responsibility of the Director of Information Systems to ensure appropriate systems and technologies are in place to monitor and maintain the safeguarding and security of everyone using the school network. They monitor the use of online technologies and the use of the internet by students and staff, and provide at least a monthly report regularly to the Senior Leadership Team. Designated Safeguarding Leads, ICT teachers and lead pastoral staff will conduct regular audits with students on each campus to assess their knowledge and understanding of issues related to e-safety and act on any areas of vulnerability.

To audit e-safety and the effectiveness of this policy, the following questions should be considered:

- Has recording of e-safety incidents been effective – are records kept?
- Did the school feel able to respond effectively to any incidents?
- Were incidents resolved to the best of the school's ability?
- Do all students demonstrate an awareness of e-safety appropriate to their age?
- Have complaints or concerns with the policy been recorded and addressed?
- Have there been significant developments in technology that should be addressed either within the curriculum or as part of staff awareness training?
- Is the policy clear to all staff and seen as appropriate and working?
- Is the current wording fit for purpose and reflective of technology use in the school?
- Do all members of the school community know how to report a problem?
- Is e-safety observed in teaching and present in curriculum planning documents?

[On-line Safety with Student User Agreement Form](#)

Forms Date reviewed: September 2016

Date for next review: September 2018

Further detail of explicit responsibilities related to ICT can be found in the job descriptions of all staff employed in the ICT Department and in other job descriptions as relevant.

Appendix 1

Procedures for staff in the event of a breach of this policy by a student or adult

- A. **An inappropriate website is accessed inadvertently**
- Report website to the Director of Information systems or the Network Manager.
 - Contact ICT Support via email (itsupport@southbank.org) so that it can be added to the banned or restricted list.
- B. **An inappropriate website is accessed deliberately**
- Ensure that no one else can access the material, by shutting down the computer.
 - Record the incident in writing
 - Report to the Principal and Director of Information Systems immediately
 - Principal to refer to the On-line Safety Agreement and follow agreed actions for discipline.
- C. **An adult receives inappropriate material**
- Do not forward this material to anyone else – doing so could be an illegal activity
 - Alert the Director of Information Systems immediately
 - Ensure the device is shut down, and record the nature of the material.
- D. **An adult has used ICT equipment inappropriately**
- Follow the procedures for B.
- E. **An adult has communicated with a student, or used ICT equipment, inappropriately**
- Ensure the student is reassured
 - Report to the Principal who should then follow the Safeguarding Policy including recording the details of the incident
 - Preserve the information received by the student if possible, and determine whether the information received is abusive, threatening or innocent
 - If illegal or inappropriate use is established, contact the Principal or the Executive Principal (if allegation is made against the Principal) and the Designated Safeguarding Lead immediately, and follow the Safeguarding Policy.
- F. **Threatening or malicious comments are posted to the school website or distributed via the school email system (or printed out) about an adult in school**
- Preserve any evidence.
 - Inform the Principal and Executive Principal immediately and follow Safeguarding Policy as necessary.
- G. **Where images of staff or adults are posted on inappropriate websites, or have inappropriate information about them posted anywhere**
- The Principal and Executive Principal should be informed.

Appendix 2 - On-line Safety Agreement

Kindergarten and Grade 1 On-line Safety Agreement

These are our rules for using the internet safely at school.

- We use the internet safely to help us learn
- We learn how to use the internet
- If we see anything on the internet, or receive a message, that is unpleasant, we must inform an adult
- We learn to keep our password a secret
- We know who and when to ask for help
- If we see something on a computer that we do not like or makes us feel uncomfortable we know what to do
- We know that it is important to follow the rules
- We aim to look after each other by using the internet safely.

Grades 2, 3, 4, and 5 On-line Safety Agreement

These are our rules for using the internet safely and responsibly at school.

- We use the internet to help us learn, and we will learn how to use the internet safely and responsibly
- We send emails and messages that are polite
- Approval from an adult may be needed before we email, chat to, or video-conference anyone at school
- We never give out passwords or personal information (like our last name, address or phone number)
- We never post photographs or video clips without a teacher's permission and never include names with photographs
- If we need help we know who and when to ask
- If we see anything on the internet or in an email or other electronic message that makes us uncomfortable or appears unpleasant, we inform an adult
- I accept that the school monitors my use of the internet at school and my school email account
- If we receive a message sent by someone we do not know, we inform an adult
- We aim to look after each other by using our safe internet in a responsible way
- We agree not to send hurtful words, images or messages outside of school on the internet or mobile phones about anyone in our school community.

Student On-line Safety Agreement (Grade 2-5)

Name: _____ Grade: _____

I understand the On-line Safety Agreement for using the internet, email and online tools safely and responsibly. I am aware that the adults working with me at school will help me to check that I am using the computers appropriately.

Student signature: _____ Date: _____

Appendix 2 - On-line Safety Agreement

Grades 6, 7, 8, 9, 10, 11 and 12 On-line Safety Agreement

At Southbank, I am encouraged to use and be aware of the safety rules and procedures which regulate my use of the ICT resources, including the internet. Access to the school's network and the internet enables me to find resources, to communicate, and to help my research for the completion of school work.

I accept that these facilities are to be used for educational purposes only and in an appropriate manner. I take responsibility for my actions and know that any breach of the rules will be considered a serious disciplinary matter.

- I will make targeted use of the internet to support my studies
- I accept that the school monitors my use of the internet at school and my school email account
- If I bring a personal device to school, including a mobile phone, I agree to log on to the internet via the school's wifi
- I will not access, create or display any material (images, sounds, text, and video) which is likely to cause offence, inconvenience or anxiety to anyone
- I will follow fully our teachers' instructions over the use of ICT and the internet
- I do not assume that information published on the Web or written in an email is accurate
- I keep my username and password confidential
- I am careful about what I write on a computer. I check my work before I print or send it. I do not use bad language. I do not write racist, sexist, abusive, homophobic or aggressive words. I do not write things that could upset or offend others
- I understand that sending malicious messages outside of school can become a matter whereby the school will set sanctions or involve outside agencies such as the Police
- I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk
- I do not make available online personal information about myself or anyone else, such as an address, telephone number and private details, in an email or on a website
- I do not respond to offensive, abusive or rude messages. I let a teacher know immediately if I am sent anything I do not feel comfortable with.
- At school I do not go to sites or download any materials which are in bad taste, offensive, violent or pornographic
- If I quote from a text I will always attribute my sources and acknowledge use of anyone else's ideas, images or data by citing the author, using quotation marks, and compiling a bibliography as required (please refer to the school's *Academic Honesty Policy*)
- I always respect the privacy of other users' data
- I will report to a teacher any incident that breaches the On-line Safety Policy rules, even if that incident does not affect me
- I treat school ICT equipment with respect and will report any damages to a teacher
- If I deliberately damage a piece of school equipment I will be charged for its replacement
- I will not bring the school's name into disrepute when using the school's IT equipment or school email
- I will check my school emails regularly to enable me to work and learn effectively
- I will follow the school and IB rules on academic honesty and not practice plagiarism
- I know that if I am worried about something related to technology outside of school I can ask for advice or help from my teachers.

Student On-line Safety Agreement (Grade 6-12)

Name: _____ Grade: _____

I understand the contents of the school's On-line Safety Policy and the rules for using the internet, email and online tools safely and responsibly. I am aware that the adults working with me at school will help me to check that I am using the computers appropriately.

Student signature: _____ Date: _____

Appendix 3

Useful Links for Advice and Support

For students

www.thinkuknow.co.uk

www.kidsmart.org.uk

www.childnet.com

<http://www.childline.org.uk/Explore/OnlineSafety/Pages/OnlineSafety.aspx>

For teachers

<http://ceop.police.uk/>

<https://www.thinkuknow.co.uk/Teachers/Resources/>

www.nspcc.org.uk/onlinesafety

<http://www.thegrid.org.uk/eservices/safety/index.shtml>

<http://www.getsafeonline.org>

For parents

www.thinkuknow.co.uk/parents

<http://ceop.police.uk/>

www.internetmatters.org

www.saferinternet.org.uk

www.chatdanger.com

www.internetmatters.org

www.digizen.org

www.bullying.co.uk