4.14 ICT Policy

4.14.1 INTERNET SAFETY AND ACCEPTABLE USAGE

At SIS, it will be deemed that use of the Internet will constitute an educational purpose, and that use therefore must be appropriate, relevant to duty, and mindful of security disciplines. Any information downloaded must be respectful of copyright, property rights and privacy. Information downloaded is stored in the cache of the system, therefore can potentially be observed by a third party. Information uploaded must be mindful of confidentiality and data security.

Downloading of offensive or explicit material, unlicensed software or software for personal use at all times is unacceptable. Offensive sites that escape a block by the filtering application or firewall must be reported to the Principal or ICT Co-ordinator.

Effort should be made to ensure sites visited are clean, thus avoiding the download into our system of any virus.

Children working on the internet should be clearly guided to the purpose of their activity. At times research may involve following blind links, so careful monitoring and quick intervention should be prepared for. When practical, likely links should be pre-investigated. Public domain pictures can be copied and pasted, and short texts for reference can be downloaded, but pasting large unedited text into own work should be discouraged.

Children should have the nature of the internet explained in age appropriate terms at the beginning of each year, with ongoing reminders. This will be done in ICT lessons for all children. Children’s work published to the web should have only first names as an identifier. Where identifiable faces appear in pictures, no names should be attached. Exceptions are only permitted with written parental consent.

Mobile Phones

Students are not allowed to have mobile phones with them during the day. However, we do recognise that many of our students travel to school by school bus or with a driver and that consequently some parents like their children to have a phone for the journey. If that is the case then the phone must be handed in to the Teachers on arrival and it may be collected again at the end of the day. Otherwise they must be switched off, placed in bags and not seen during the school day. Phones which are found in students' possession during the day are liable to confiscation. They are also brought into school at the risk of the owner, and the school cannot be held liable in case of loss, damage or theft.

4.14.2 E-SAFETY

The school will deliver lessons and information to the children, staff, parents and wider community regarding e-safety guidelines and practices.

Safe use of ICT

Internet and search engines

- When using the internet, students should receive the appropriate level of supervision for their age and understanding. Teachers should be aware that often, the most computer-literate children are the ones who are most at risk.
- Students should be supervised at all times when using the internet. Teachers should remain vigilant at all times during lessons.
- Students should not be allowed to aimlessly "surf" the internet and all use should have a clearly defined educational purpose.
- Despite filtering systems, it is still possible for pupils to inadvertently access unsuitable websites; to reduce risk, teachers should plan use of internet resources ahead of lessons by checking sites and storing information off-line where possible.
- Social networking, chat rooms and instant messaging should not be accessed in school.

Evaluating and using internet content

As the information generated by internet searches could be vast, and much of it irrelevant to the subject being taught, teachers should teach pupils good research skills that help them to maximise the resource. They should also be taught how to critically evaluate the information retrieved by:

- questioning the validity of the source of the information; whether the author's view is objective and what authority they carry

- carrying out comparisons with alternative sources of information

- considering whether the information is current and whether the facts stated are correct. In addition, pupils should be taught the importance of respecting copyright and correctly quoting sources and told that plagiarism (copying others work without giving due acknowledgement) is against the rules of the school and may lead to disciplinary action.

Emails

- Pupils should be taught not to disclose personal contact details for themselves or others such as addresses or telephone numbers via email correspondence.

- All email communications should be polite; if a pupil receives an offensive or distressing email, they should be instructed not to reply and to notify the responsible teacher immediately.

- Pupils should be warned that any bullying or harassment via email will not be tolerated and will be dealt with in accordance with the school's anti-bullying policy.

- Users should be aware that as use of e-mail via Fronter is for the purposes of education or school business only, and all emails may be monitored.

- Access to email systems by SIS pupils should be via school email address only. All email messages sent by pupils in connection with school business must be checked and cleared by the responsible teacher.

- Apart from the Principal, individual email addresses for staff or pupils should not be published on the school website.

- Pupils should be taught to be wary of opening attachments to emails where they are unsure of the content or have no knowledge of the sender.

Computers and Laptops at home or school

- Do not install, attempt to install, or store programs of any type on the computers without permission from the network administrator.
- Do not damage, disable, or otherwise harm the operation of computers, or intentionally waste resources.
- Do not use the computers for commercial purposes, e.g. buying or selling goods.
- Do not open files brought in on removable media(such as CDs, flashdrives etc.) until they have been checked with antivirus software, and been found to be clean of viruses.
- Do not connect any mobile equipment to the network until they have been checked with antivirus software, and been found to be clean of viruses.
- Do not eat or drink near computer equipment.
- Check all websites, information, etc being used for classroom activities before it is used by children in order to ensure that there is nothing of an inappropriate nature.

Internet

- Do not access the Internet unless for school related activities.
- Do not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials, which are unlawful, obscene or abusive.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
- Do not engage in ‘chat’ activities of a personal nature over the Internet including social networking sites,blogs and forums during school time.
- You should not post any e-comments that purport to represent the school unless specifically authorized by the Principal. Any public posting on the school website or other similar means of communicating information must be first proof-read by the Principal.

4.14.3 INTERNET USE AGREEMENTS AND RESPONSIBILITIES

All staff and students should sign the school's ICT user agreements in order to ensure safe use. Parents will also sign the agreements in the student planners.

Primary Student Responsibilities

Students will:

· Sign the Acceptable Use Policy with their parents.

· Always follow the Safety and Acceptable Usage Policy.

· Only use the internet or computers for learning purposes during school times.

· Only use chromebooks in classrooms or designated learning environments (such as the library) whilst supervised by an adult.

· Only access online material that has been approved by a teacher.

· Only access their own personal accounts, under no circumstances should students be accessing the accounts of others.

Failure to adhere to this will result in students facing sanctions as outlined below.

Secondary Student Responsibilities

Students will:

· Take personal responsibility for their own e-safety e.g. when online, will not give out any personal details or arrange to meet someone without the written permission of a parent, carer or teacher.

· Only use their chromebooks for educational purposes and when under supervision by a teacher whilst on school premises.

· During break or lunch time only use chromebooks on level 5 under supervision

· Use email responsibly and always be polite and respectful. Only use email systems, chat rooms and other messaging methods that are approved by the school and for educational purposes. Never use ICT for bullying or harassing others or in a way that will bring the school into disrepute.

· Not download or install any software or files on school's ICT equipment (unless it is a requirement of an agreed course of study) or open emails or attachments from people that they do not know.

· Run a virus check before using a flash drive (USB memory stick) in school.

· Not intentionally gain access to unsuitable or illegal sites eg pornography, child abuse, racism, incitement to violence. Will report as soon as possible accidental access to such sites. Understand that the report will be confidential and would protect other students and themselves.

· Only access computer systems using their own login and password, which they will keep secret. Realise that if they access files that are not their own (hacking) they will be breaking the law.

· Ensure that work does not infringe copyright laws. Will always acknowledge the source of information (words, images etc) used. Not copy other people's work and pass it off as their own (plagiarism).

· Use school ICT equipment and chromebooks with care and tell a teacher of any damage which occurs as soon as possible.

Failure to adhere to this will result in students facing sanctions as outlined below.

RESPONDING TO INCIDENTS

Unintentional access of inappropriate websites

· If a pupil or teacher accidently opens a website that has content which is distressing or upsetting or inappropriate to the pupils' age, teachers should immediately (and calmly) close or minimise the screen.

· Teachers should reassure pupils that they have done nothing wrong and discuss the incident with the class to reinforce the online safety message and to demonstrate the school's "no blame" approach.

· The incident should be reported to the online safety contact officer and details of the website address and URL provided.

- The online safety contact officer should liaise with the IT Technician or Schools IT team to ensure that access to the site is blocked and the school's filtering system reviewed to ensure it remains appropriate.

Intentional access of inappropriate websites by a pupil

- If a pupil deliberately accesses inappropriate or banned websites, they will be in breach of the acceptable use policy and subject to appropriate sanctions. (See Sanctions For Pupils)

- The incident should be reported to the Pastoral lead and details of the website address and URL recorded.

- The Pastoral lead should liaise with the IT Technician and Schools IT team to ensure that access to the site is blocked.

- The pupil's parents should be notified of the incident and what action will be taken.

Inappropriate use of ICT by staff

- If a member of staff witnesses misuse of ICT by a colleague, they should report this to the Principal immediately.

- The IT Technician will ensure laptop/computer is taken out of use and securely stored in order to preserve any evidence. A note of any action taken should be recorded.

- The IT Technician and the Schools IT team will carry out an audit of use to establish which user is responsible and the details of materials accessed.

- Once the facts are established, the Principal should take any necessary disciplinary action against the staff member and the police where appropriate.

- If the materials viewed are illegal in nature the Principal should report the incident to the police and follow their advice, which should also be recorded.

Cyber bullying

Definition and description Traditionally, bullying took place face to face in the physical world; online, bullying can take on a new dimension with technologies such as email, mobile phones and social networking sites used as a platform to hurt, humiliate, harass or threaten victims.

Cyber bullying is defined as the use of ICT to deliberately hurt or upset someone. Unlike physical forms of bullying, the internet allows bullying to continue past school hours and invades the victim’s home life and personal space. It also allows distribution of hurtful comments and material to a wide audience.

Cyber bullying is extremely prevalent as pupils who would not consider bullying in the physical sense may find it easier to bully through the internet, especially if it is thought the bullying may remain anonymous.

Cyber bullying can affect pupils and staff members. Often, the internet medium used to perpetrate the bullying allows the bully to remain anonymous. In extreme cases, cyber bullying could be a criminal offence.

Dealing with incidents

The following covers all incidents of bullying that involve pupils at the school, whether or not they take place on school premises or outside school.

- School anti-bullying and behaviour policies and acceptable use policies should cover the issue of cyber-bullying and set out clear expectations of behaviour and sanctions for any breach.

- Any incidents of cyber bullying should be reported to the Pastoral lead who will record the incident and ensure that the incident is dealt with in line with the school’s anti-bullying policy. Incidents should be monitored and the information used to inform the development of anti- bullying policies.

- Where incidents are extreme, for example threats against someone's life, or continue over a period of time, consideration should be given to reporting the matter to the police as in these cases, the bullying may be a criminal offence.

- As part of online safety awareness and education, pupils should be told of the "no tolerance" policy for cyber bullying and encouraged to report any incidents to their teacher.

Risk from inappropriate contacts

Teachers may be concerned about a pupil being at risk as a consequence of their contact with an adult they have met over the internet. The pupil may report inappropriate contacts or teachers may suspect that the pupil is being groomed or has arranged to meet with someone they have met online.

- All concerns around inappropriate contacts should be reported to the online safety contact officer and the Principal.

- The Principal should discuss the matter with the referring teacher and where appropriate, speak to the pupil involved, before deciding whether or not to make a referral to the police.

- The police should always be contacted if there is a concern that the child is at immediate risk, for example if they are arranging to meet the adult after school.

- Teachers should advise the pupil how to terminate the contact and change contact details where necessary to ensure no further contact.

- Where inappropriate contacts have taken place using school ICT equipment or networks, contact the Schools IT team to ensure that all evidence is preserved and that an audit of systems is carried out to ensure that the risk to other pupils is minimised.

4.14.4 SANCTIONS

<u>Sanctions for pupils</u>

Sanctions will fall under three levels as per the Sentral Behaviour system:-

a) **Level 1 negative behaviours**

These are basically low-level breaches of acceptable use agreements such as:

- use of non-educational sites during lessons when not permitted by a teacher (games/youtube/messageboards).
- unauthorised use of prohibited sites for instant messaging or social networking.

These behaviours equate to a level 1 negative behaviour mark on Sentral.

These incidents will also result in chromebook access being stopped for the day the event happens. Chromebook to be passed to the Heads of Primary/Secondary of Heads of Pastoral care.

b) Level 2 negative behaviours

These are persistent breaches of acceptable use agreements following warnings and use of banned sites or serious breaches of online safety policy that are non-deliberate, such as:

- continued use of non-educational sites during lessons
- continued use of prohibited sites for instant messaging or social networking
- use of file sharing software
- accidentally corrupting or destroying other people's data/work without notifying staff
- accidentally accessing offensive material without notifying staff.

These behaviours equate to a level 2 negative behaviour mark on Sentral. The behaviour will also lead to a loss of chromebook access for one week after discussion with the parents/guardians of the student in question. Chromebooks to be held by Heads of Pastoral/ Head of Primary/Secondary

c) Level 3 negative behaviours

These are deliberate actions that are serious breaches of acceptable use agreements or anti-bullying policies, such as:

- deliberately bypassing security blocked sites
- deliberately corrupting or destroying other people’s data/work or violating other’s privacy
- cyber bullying
- deliberately accessing, sending or distributing offensive or pornographic material
- purchasing or ordering items over the internet
- transmission of commercial or advertising material
- deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent

School policy - Immediate stage 3 behaviour sanction (Thursday or Saturday detention - depending on incident) and parent is informed - referral to Head of Pastoral/Head of Primary/Secondary - loss of chromebook access for an agreed period after discussions with the parent/guardian