E-Safety Policy

Reviewed on September 2016

PRINCIPAL

E-Safety Policy

Policy: The Acceptable Use of the Internet and related Technologies

Context: E-Safety

ICT in the JSSPS (JSS Private School)

- The extent to which information and communication technology (ICT) capability and other key skills enable learners to improve the quality of their work and make progress
- The extent to which learners adopt safe and responsible practices in using new technologies, including the Internet.
- Through the development of literacy, numeracy, information and communication technology, enterprise capability, economic and business understanding and financial capability.
- We have a duty to ensure that all students are able to make a valuable contribution to society & this is impossible to achieve if we do not ensure that students develop and apply their ICT capability effectively in their everyday lives.

Working towards ICT Mark

- Safeguarding

  The school is aware of its responsibilities in ensuring that ICT usage by all network users is responsible, safe and secure. There are relevant and comprehensive policies in place which are understood and adhered to by many network users.

- Effective and safe use of digital resources

  Most pupils have a good range of skills that enable them to access and make effective use of digital resources to support their learning. They understand the issues relating to safe and responsible use of ICT and adopt appropriate practices

"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.

To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom."

The 'staying safe' outcome includes aims that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death

- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- Secure, stable and cared for.

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

1. The technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging (http://www.msn.com, hhtp://www.gmail.com) often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (Popular www.twitter.com http://www.hi5.com / http:www.facebook.com)
- Video broadcasting sites (Popular: http://www.youtube.com/)
- Chat Rooms (Popular www.teenchat.com, www.habbohotel.co.uk)
- Gaming Sites (Popular www.neopets.com, http://www.miniclip.com/games/en/, http://www.runescape.com/ / http://www.clubpenguin.com)
- Music download sites (Popular http://www.apple.com/itunes/ http://www.napster.co.uk/ http://www-kazzaa.com/, http://www-livewire.com/)
- Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles) that are 'internet ready'.
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

2. Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive e-Safety education programme for pupils, staff and parents.
- School's AUP has been drawn recently (Attached Annexure1)

3. Roles and Responsibilities

e-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The head teacher ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for e-Safety has been designated to a member of the senior management team.

Our school **e-Safety Co-ordinator** is IT Coordinator.

The school's e-Safety coordinator ensures the Head, senior management and Governors are updated as necessary.

Governors need to have an overview understanding of e-Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance [1] on e-Safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the schools' Policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- publication of pupil information/photographs and use of website;
- e-Bullying / Cyber bullying procedures;
- their role in providing e-Safety education for pupils;

Staff are reminded / updated about e-Safety matters at least once a year.School ensure that every pupil has been educated about safe and responsible use. Pupils need to know how to contrail and minimise online risks and how to report a problem.

Schools should ensure that they make efforts to engage with parents over e-safety matters.

4. Communications

How will the policy be introduced to pupils?

Discussion: Many pupils are very familiar with the culture of new technologies, they can be involved them in designing the School e-Safety Policy, possibly through a student council. Pupils' perceptions of the risks may not be mature; the e-safety rules may need to be explained or discussed.

Consideration must be given as to the curriculum place for teaching e-safety. Is it an ICT lesson activity, part of the pastoral programme or part of every subject? Or all of these?

Useful e-safety programmes include:

- Think U Know; currently available for secondary pupils. (www.thinkuknow.co.uk/)
- Grid Club www.gridclub.com
- The BBC's Chat Guide: www.bbc.co.uk/chatguide/

Possible statements:

- An e-safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.
- Instruction in responsible and safe use should precede Internet access.
- An e-safety module will be included in the covering both school and home use.

How will the policy be discussed with staff?

Discussion: It is important that all staff feel confident to use new technologies in teaching. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies

Staff must understand that the rules for information systems misuse. If a member of staff is concerned about any aspect of their ICT use in school, they should discuss this with their line manager to avoid any possible misunderstanding.

ICT use is widespread and all staff including administration, caretaker, governors and helpers should be included in appropriate awareness raising and training. Induction of new staff should include a discussion of the school's e-Safety Policy.

Possible statements:

- Staff should be aware that Internet traffic is monitored and can be traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.

How will parents' support be enlisted?

Discussion: Internet use in pupils' homes is increasing rapidly. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. The school may be able to help parents plan appropriate supervised use of the Internet at home.

Possible statements:

- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

5. How will complaints regarding e-Safety be handled?

The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- interview/counselling by tutor / Head of Year / e-Safety Coordinator / Headteacher;
- informing parents or carers;
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];

Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Head teacher.

Complaints of cyber bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

ANNEXURE 1 – AUP

JSS PS ACCEPTABLE USE OF TECHNOLOGY (AUP)

JSS PS students are expected to use technology in a respectful, responsible and safe manner following the guidelines below:

RESPECTFUL

Be courteous and ethical in all communications (email, social networking, etc...)
For example:

- When creating, publishing, posting or sending information in a private or public matter avoid profane language or bullying.
- Respect others' privacy, For example:
  - Only access personal files, folders or accounts of others with their permission.
- Respect others' ownership of property For example:
  - Ask permission before using the personal property of others (laptops, tablets etc.…).
  - Avoid eating or drinking near your devices or those of your friends and the school.
- Know where your devices are at all times.
- Respect others' ownership of information (Copyright), For example:
  - Taking someone else's work without giving them credit is plagiarism; you must properly cite all sources in your work.
- Respect your teachers and the learning environment of others, For example:
  - Students must comply with any teacher's request to shut down the device or close the screen.
  - Devices should be kept on silent or with the volume muted unless otherwise instructed by the teacher.

SAFE

Never share your passwords or personal information with anyone For example:

- Ask for teacher or parent permission before posting personal information online (personal information includes your full name, address, phone number, etc.).
- Ask permission of a teacher before downloading or installing any applications over the school network
- Notify a teacher if there are actions that do not follow the rules or seem unsafe

RESPONSIBLE

Ensure your usage of any technology devices is in line with school curriculum and approved sources
For example:

- During classroom instruction time, technology devices should only be used for class related projects and activities approved by the teacher.
- Only use websites that are allowed at that time by teachers.

Ensure that all personal and school property is used in the way that it was intended
For example:

- Only use the school network for school related activities.Use of 3G & 4G wireless connections is not allowed.

- Act responsibly when using personal or school hardware, software and the school network.

The use of personal devices to support educational goals is a privilege. Teachers and administrators have the right to see what the students are doing on the devices at all times.
The school has the right to collect and examine a device if at any time it is used inappropriately or if the IT team suspects a virus that may be affecting the school network.
Any use of technology that does not fit within these guidelines, as determined by a teacher or administrator, will result in disciplinary action.

BREACH OF POLICY

- If a student uses a phone during class in a manner that does not follow these guidelines, the phone will be confiscated and returned to the student at the end of class.
- If a student repeatedly uses a phone in a manner that does not follow these guidelines (determined by the teacher or administrator), the phone will be confiscated and the student or parent will be able to pick it up at the end of the school day from the assistant principal's office.

At the beginning of each new school year, students need to read, agree, and electronically sign the school AUP (Form 1)

(Form 1) PERMISSION FORM

Any parent must read and sign this agreement and submit to the administration upon registering their children at JSS PS.
1. The student takes full responsibility for his or her device and keeps it with himself or herself at all times. The school is not responsible for the security of the device.
2. The student is responsible for the proper care of their personal device, including any costs of repair, replacement or any modifications needed to use the device at school.
3. The school reserves the right to inspect a student's personal device if there is reason to believe that the student has violated school policies, administrative procedures, school rules or has engaged in other misconduct while using their personal device.
4. Violations of any school policies, administrative procedures or school rules involving a student's personally owned device may result in the loss of use of the device in school and/or disciplinary action.
5. The student must comply with teachers' request to shut down the computer or close the screen.
6. The student may not use the devices to record, transmit or post photos or video of a person or persons on campus. Nor can any images or video recorded at school be transmitted or posted at any time without the express permission of a teacher.
7. The student should only use their device to access relevant files.
8. The student will use the school's secured wireless network. Use of 3G & 4G wireless connections is not allowed.

SIGN AND RETURN TO SCHOOL ADMINISTRATION.
Student's name _____

Parent's name _____

I understand and will abide by the above policy and guidelines. I further understand that any violation of the above may result in the loss of network and/or device privileges as well as other disciplinary action.

As a parent I understand that my child will be responsible for abiding by the above policy and guidelines. I have read and discussed them with her/him and they understand the responsibility they have in the use of their personal device.

Parent's Signature _____

Date _____