Pakistan Educational Academy, Dubai

Cyber Safety Policy

Rationale

Pakistan Educational Academy has a duty of care to ensure the safety of all students and staff. This involves the provision of a safe physical and emotional environment for students and staff.

The internet is a worldwide phenomenon that provides access to a continuously growing wealth of knowledge and information. This information comes from a vast range of sources including private and public institutions as well as individuals. The educational value of the information available on the Internet is significant; however, this also includes information of questionable educational value, not to mention information that is inaccurate, abusive, offensive or illegal.

It is the desire of PEA to support students in becoming responsible and discerning users of the Internet. It is the joint responsibility of the school and the parents of each student to educate the student about his or her responsibilities when using the various forms of Information Communication Technology now available at our fingertips. Use of ICT resources by students outside of school hours remains the responsibility of the parents.

The students of PEA are expected to use the school's ICT resources in a manner consistent with this policy and they will be held accountable and responsible for their use. PEA has an 'Acceptable Use Policy' and procedural guidelines for accessing and using the Internet at school for all staff and students.

Objectives

PEA will develop and maintain rigorous and effective cyber-safety practices which aim to maximize the benefits of the Internet and ICT devices/equipment to student learning and to the effective operation of the school, while minimizing and managing any risks.

These cyber safety practices will aim to not only maintain a cyber-safe school environment, but also aim to address the need of students' members of the school community to receive education about the safe and responsible use of present and developing information and communication technologies.

Implementation

- Use agreements apply to the use of school-owned ICT equipment as well as privately-owned ICT equipment on the school site, or at/for any school-related activity, regardless of its location. This includes offsite access to the school network from school or privately-owned equipment.
- PEA use agreements will cover all employees and all students, and any other individuals authorized to make use of the school Internet facilities and ICT devices/equipment.
- The use agreements are also an educative tool and should be used as a resource for the professional development of staff and the education of students in safe and responsible use of ICT equipment.
- Use of the Internet and the ICT equipment by staff, students and other approved users at PEA is to be limited to educational, professional development, and personal usage appropriate in the school environment, as defined in individual use agreements.
- Use agreements will be published on PEA website, and an appropriate system devised which facilitates confirmation that particular individuals are authorized to make use of the Internet and ICT equipment.
- The school has the right to monitor, access and review all use.
- The school has the right to audit at any-time any material on equipment that is owned by the school. The school may also request permission to audit privately owned ICT equipment used on the school site or at any school related activity.
- The safety of children is of paramount concern. Any apparent breach of cyber-safety will be taken seriously. The response to individual incidents will follow the procedures developed as part of the

school's cyber-safety practices. In serious incidents, advice will be sought from an appropriate source, such as someone with specialist knowledge in this area. There will be special attention paid to the need for specific procedures regarding the gathering of evidence in potentially serious cases. If illegal material or activities are suspected, the matter will need to be reported to relevant law enforcement.

Review

This policy will be reviewed at least every year.

Cyber-safety Use Agreement

Important terms used in this document

‘ICT’, the abbreviation ‘ICT’ in this document refers to the term “Information and Communication Technologies‟.

‘Cyber-safety’, refers to the safe use of the Internet and ICT equipment / devices, including mobile phones.

‘School ICT’, refers to the school’s computer network, Internet access facilities, computers, and other school ICT equipment/devices as outlined in below.

‘ICT equipment/devices’, used in this document, includes but is not limited to, computers (such as desktops, laptops, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, video tape, floppy disks,), cameras (such as video, digital, webcams), all types of mobile phones, gaming consoles, video and audio players/receivers (such as portable CD and DVD players), and any other, similar, technologies as they come into use.

‘Objectionable’ / ‘Inappropriate material’, in this agreement means material that deals with matters such as cruelty, discrimination or violence in such a manner that it is likely to be injurious to the good of students or incompatible with a school environment.

‘Cyber bullying’, is bullying which uses e-technology as a means of victimising others. It is the use of an Internet service or mobile technologies - such as email, chat room discussion groups, instant messaging, web pages or SMS (text messaging) - with the intention of harming another person.

‘E-crime’, occurs when computers or other electronic communication equipment/devices (eg Internet, mobile phones) are used to commit an offence, are targeted in an offence, or act as storage devices in an offence.

The Technologies included in Cyber-Safety

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. The Current and emerging technologies used by children include:

- The Internet
- email
- Instant messaging (msn, aol, yahoo, skype, whatsapp) which often using simple web cams
- Blogs (an on-line interactive diary)
- Social networking sites (myspace, hi5, facebook, twitter)
- Video broadcasting sites (youtube, tune.pk)
- Chat Rooms (teenchat)
- Gaming Sites (neopets, miniclip, runescape, clubpenguin)
- Music download sites (apple, napster, kazzaa, livewire, soundcloud)
- Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles) that are „internet ready‟.
- Smart phones now come with e-mail, web functionality and cut down “Office‟ applications.
- X-Box and Play Station (these also have the capacity of internet connection)
- Other applications or technologies still to be released.

Cyber-Safety Rules

1. **School ICT for uses the school deems appropriate**
   This helps to ensure the equipment is available when students need to use it for their learning. It will also help to reduce the likelihood of any inappropriate activities taking place which put at risk the safety of the learning environment.
2. **If student is unsure whether he/she is allowed to do something involving ICT, he/she will ask the teacher first.**

This helps the students of PEA to take responsibility for their own actions, and seek advice when they are unsure of what to do. It provides an opportunity for the teacher and student to work through an issue and so avoid the student making an unwise decision which could possibly lead to serious consequences. Young children need ongoing advice and guidance to help them become safe and responsible users of ICT.

3. **Student will follow the cyber-safety rules, and will not join in if others are being irresponsible. Student will tell the teacher of such behaviours straight away.**
   Unfortunately, along with many benefits, technology has also provided new ways to carry out anti-social activities. Bullying and harassment by text message, for example, is becoming a major problem in Australia and in many other countries. Often children become involved in these acts through peer pressure, without thinking of the consequences.
4. **If student accidentally come across mean, rude, or dangerous material, student will tell the teacher straight away, without showing any other students. The teacher will then notify the network administrator to block this material.**
   Because anyone at all can publish material on the Internet, it does contain material which is inappropriate, and in some cases illegal. The school takes a number of steps to prevent this material from being accessed. However, there always remains the possibility that a student may inadvertently stumble across something inappropriate. Encouraging students to tell a teacher immediately if they find something which they suspect may be inappropriate, encourages critical thinking and helps students to take responsibility for their actions and keep themselves, and others, safe. This way, they contribute to the cyber-safety of the school community.
5. **If student is not feeling safe at any time while using the ICT equipment, student will tell the teacher straight away.**
   PEA strives to create a safe and secure learning environment for all members of the school community. Examples of situations involving the use of ICT which might cause a student to feel unsafe could include: contact being made by a stranger through email or text message, the presence of ‘scary’ images on a computer screen, and/or misconduct by other students. Staff needs to be made aware of such situations as soon as they occur to ensure the school can respond immediately.
6. **Student will not share password with any other person.**
   Passwords help to ensure only approved persons can access the school ICT facilities.
7. **Student will log off or shut down the computer when student have finished using it.**
8. **Students often work together at a single computer. It is important that your child takes responsibility for sensible use of the computer at all times, and tells the teacher if there is any concern.**
9. **Student will check with the teacher before giving anyone information about student or others when using the Internet – this includes name, home and email addresses, and phone numbers.**
   This reduces the risk of students being contacted by someone who wishes to upset or harm them, or use their identity for purposes which might compromise the student’s privacy or security online.
10. **Student will not be careless, try to damage, or steal any school ICT equipment. (If this happens, the school will need to inform parents about what has happened. Parents may have responsibility for the cost of repairs or replacement.)**
11. **Student will not try to stop the network or any other equipment from working properly.**
    If student accidentally break school ICT equipment, damage it through mishandling, or student find it broken when student start to use it, student will tell a teacher straight away.
12. **Student will not change any screensavers, desktop backgrounds, themes or hardware settings.**
13. **Student will have no involvement with making or sending malware (such as viruses, worms & trojans) on purpose.**
14. **Student will use good judgment to decide whether printing is necessary. If student is unsure, student will seek advice from a teacher.**
    Rules 10-14 are designed to help protect the investment the school has made in expensive ICT technologies. Also, certain settings may have been applied to maximize the safety of the students and the equipment (such as antivirus settings or restrictions on Internet access).
15. **Student will not download any files such as music, videos, or programs.**
    Many files available on the Internet are covered by copyright, and although they can be easily downloaded, it may be illegal to do so. Sometimes even innocent-looking files may contain

malicious content such as viruses, or spyware (software that searches for personal information from your computer and transmits it to others over the Internet). As well, some files may contain inappropriate or illegal material.

16. **Student must have permission from school, before bringing any disk or other ICT equipment / device from home. If student is given permission, then student must use that ICT sensibly.**
    This rule is designed to protect the school's online security and equipment from viruses which can easily be transferred using disks or other storage devices such as memory cards.
    Parents should be mindful of the school's specific policy regarding students and mobile phones.
17. **Student will not bring software or games from outside school to use on school equipment.**
    Installing software from home may cause conflicts with the software installed by the school. PEA must also abide by any licensing requirements included within the software. This means that unless the school has purchased a copy, it will not usually be legally entitled to install the software.
18. **Student will acknowledge where work has come from if student have copied it from somewhere. This includes graphics and sounds files student might have used in schoolwork.**
    The Internet has allowed easy access to a huge range of information which can be incorporated into students' work by simply cutting and pasting. Most of this material is copyrighted, and thus involves intellectual property issues. Also, the value to students' learning is questionable if they have not thought through this information themselves.
19. **Student will check with the teacher before using school equipment to copy software, music, videos or other files, in case they are copyrighted.**
    Any such copying is likely to be restricted by copyright laws. PEA cannot condone the use of its equipment for these activities.
20. **Student will not use the internet, mobile phones or any other ICT equipment to be mean, rude, offensive, or to harass any members of the school community like students and staff, while at school or when involved in any school-related activity. The same rule applies when using school ICT at any time, whether at school or not.**
    The basic principles of respect extend to the use of information and communication technologies.
21. **Cyberbullying can involve a range of misconduct including the creation of abusive websites.**
22. **If student break these rules, the school may need to talk to parents about what has happened. Disciplinary action should be expected.**
    Depending on the seriousness of a particular breach, possible school responses could include one or more of the following: a discussion with the student, informing parents, loss of ICT privileges, parents possibly having responsibility for the cost of ICT repairs or replacement, the school taking disciplinary action.

BREACHES OF THIS AGREEMENT

1. Breaches of the use agreement can undermine the values of the school and the safety of the learning environment, especially when ICT is used to facilitate misconduct.
   Such a breach which is deemed harmful to the safety of the school (for example, involvement with inappropriate material, or anti-social activities like harassment), may constitute a significant breach of discipline and possibly result in serious consequences. The school will respond to any breach of the use agreement in an appropriate manner, taking into account all relevant factors on a case by case situation.
2. Depending on the seriousness of a particular breach, possible school responses could include one or more of the following: a discussion with the student, informing parents, loss of ICT privileges, the family possibly having responsibility for the cost of ICT repairs or replacement, the school taking disciplinary action which is outlined within the school's behavior management policy.
3. If there is a suspected breach of use agreement involving privately-owned ICT e.g. (USB flash drive) on the school site or at a school related activity, the matter may be investigated by the school. The school may request permission to audit that equipment/device(s) as part of its investigation into the alleged incident.
4. Involvement with material which is deemed inappropriate in a school setting is a very serious matter, as is involvement in an activity which might constitute criminal misconduct, such as cyber bullying.
   In such situations parents will be contacted and it may be necessary to involve law enforcement in addition to any disciplinary response made by the school.