Providence English Private School

E-Learning & E-Safety Policy

Reviewed :August:2024

This policy has been developed to ensure that all stakeholders at Providence English Private School (PEPS) are working together to safeguard and promote the welfare of children and young people.

Overview

The policy covers educational provision leading to an award or part of an award which is delivered and/or supported and/or assessed through means which generally do not require the student to attend particular classes or events at particular times and particular locations. This includes practice such as e-learning, distance learning, blended learning, flexible learning, instructor led training and the use of web-based materials to supplement classroom-based learning. E-Safety is a safeguarding issue not an ICT issue and all members of the school community have a duty to be aware of e-safety at all times, to know the required procedures and to act on them.

Introduction

The purpose of internet use in school is to help raise educational standards, promote pupil achievement, and support the professional work of staff as well as enhance the school's management information and business administration systems. The internet is an essential element in 21st century life for education, business and social interaction and the school has a duty to provide children and young people with quality access as part of their learning experience. A risk assessment will be carried out before children and young people are allowed to use new technology in schools and settings.

This document aims to put into place effective management systems and arrangements which will maximize the educational and social benefit that can be obtained by exploiting the benefits and opportunities by using ICT, whilst minimizing any associated risks. It describes actions that should be put in place to redress any concerns about child welfare and safety as well as how to protect children, young people and staff from risks and infringements.

ROLES AND RESPONSIBILITIES

The Governing Body of the Providence English School (PEPS) will ensure that:

- A designated Senior Member of Staff for E-Learning /Safety is identified and receives appropriate on-going training, support and supervision and works closely with the designated person for safeguarding.
- All staff of PEPS are made aware of the school's E-Learning/Safety Policy and arrangements.
- All teachers have access to appropriate E-Learning training.
- A commitment to E-Safety is an integral part of the safer recruitment and selection process of staff.
- Are students able to report easily to a nominated person at the school.
- HOD or designated staff able to enter virtual classrooms to monitor lessons on ad hoc basis.

The E-Learning/ E-Safety officer will:

- Act as the first point of contact with regards to breaches in E-safety and security.
- Liaise with the designated person for Safeguarding as appropriate.
- Ensure that ICT security is maintained, and attend appropriate training.
- Ensure that all teaching and non teaching staff understand and aware of the school's E-Learning/Safety Policy.
- Ensure that the School's ICT system's are regularly reviewed (usually weekly) with regard to security.
- Ensure that the virus protection is regularly reviewed and updated.
- Ensure that the staff and teachers are able to block a user if that user starts sharing in appropriate material in a virtual break-out session.
- Ensure that the staff and teachers know how to report any illegal content that might be shared online, both internally within your organization and externally to law enforcement.

Delivery

Schools should ensure students have access to:

- information that sets out the respective responsibilities of the school for the delivery of the program module, or element of study;
- module descriptors, to show the intended learning outcomes and teaching, learning and assessment methods of the module(s);
- a clear schedule for the delivery of their study materials and for assessment of their work.

Schools should ensure that students can be confident that:

- study materials, whether delivered through staff of a program presenter or through web-based or other distribution channels, meet the expectations of the school in respect of the quality of teaching and learning-support material for a program or element of study leading to one of its awards;
- The provision is subject to Annual Monitoring and the School Periodic Review process.

Teaching and Learning

Benefits of internet use for education

- The internet is a part of the statutory curriculum and a necessary tool for staff and children and young people and benefits education by allowing access to world – wide educational resources to specialists in many fields for pupils and staff.
- The internet offers opportunities for mentoring pupils and providing peer support for them and their teachers.
- Children and young people shall be encouraged to question what they read and to seek confirmation of matters of fact from more than one source. They will be taught research techniques including the use of subject catalogues and search engines and encouraged to question the validity, currency and origins of information.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.
- Students will be taught what internet use is acceptable and what is not and be given clear objectives for internet use. Staff will guide pupils in on-line activities that will support the learning outcomes planned for the student's age and maturity.
- Students will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.
- Students will be taught to be critically aware of the materials they read as well as how to validate information before accepting its validity.

MANAGING E-MAIL AND WEBSITE CONTENT

- Access in school to external personal e-mail accounts may be blocked
- Student must not reveal details of themselves or others in any e-mail communication or by any personal web space such as an address, telephone number and must not arrange meetings with anyone.
- Staff should use the school portal if they need to communicate with pupils about their school work e.g.: study leave, course work etc.
- Incoming e-mail should be monitored and attachments should not be opened unless the author is known.
- Editorial guidance will ensure that the school's ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material.
- The website will comply with the school's guidelines for publications and parents/care takers will be informed of the school policy on image taking and publishing.
- Pupils will be taught to consider the thoughts and feelings of others when publishing material to websites and elsewhere. Material which victimizes or bullies someone, or is otherwise offensive, is unacceptable and appropriate sanctions will be implemented.

- Students will not access social networking sites, and they will be taught the importance of personal safety when using social networking sites and chat rooms out of school. (Refer social media policy)
- Regular checks by E-safety office will ensure that the filtering methods selected are appropriate, effective and reasonable.

Handling E-Safety concerns and incidents

It is very important that all staff should understand that E-safety is a part of safeguarding; all stake holders of PEPS community should err on the side of talking to the e-safety coordinator to the effective way of handling all incidents. The school ensures that all our users access only relevant material.

E-safety concerns and incidents are linked with other policies such as **Child Protection & Safeguarding Policy, Behavior Policy, Anti-Bullying Policy, BYOD Policy, and Wellbeing Policy.**

Learner support

Prospective students should receive a clear and realistic explanation of the expectations placed upon them for study of the programme or elements of study, and for the nature and extent of autonomous, collaborative and supported aspects of learning.

- Students should have access to schedule for any learner support available to them through timetabled activities, for example tutorial sessions or web-based conferences.
- Appropriate opportunities to give formal feedback on their experience of the programme.
- Schools shall ensure that students are confident that staff provides support to learners on these programmes have appropriate skills, and receive appropriate training and development.

Assessment of students

Students should have access to:

- Information on the ways in which their achievements will be judged, and the relative weighting of units, modules or elements of the program in respect of assessment overall.

Schools should ensure that students can be confident that:

- Those with responsibility for assessment are capable of confirming that a student's assessed work is the original work of that student only, particularly in cases where the assessment is conducted through remote methods.

Maintaining ICT Security

- Personal data sent over the network will be encrypted or otherwise secured.
- Unapproved system utilities and executable files will not be allowed in pupils work areas or attached to e-mails.
- The E-safety officer will ensure that the system has the capacity to deal with increased traffic caused by internet use.

Photographs and Videos

- Publishing photos and videos of students on the website should be with written permission from parents. This consent form will be considered for the entire period of student attends this school.
- Parents can withdraw this consent anytime in writing.
- School will send consent forms to parents for photographs/videos being taken in the school. The exception to this may be photographs taken at events such as seminars, competitions, picnics, graduation ceremony etc.
- Photos taken on events or educational activities may display around the school and then archived or shredded.
- E-Safety officer shall ensure that all printing of all photographs is carried out on the school premises and all photos held on cameras will be deleted at the end of each week.
- If the photographs taken by anyone other than school, E-Safety officer shall ensure we obtained consent and not allow unsupervised access to pupils.

Mobile Phones and Electronic devices

Students

- Students are not allowed to use any of the electronic devices such as tablets, smart phones, smart watches, or other devices during school timing. (Unless they have been requested). **Refer to User Agreement Policy & BYOD Policy**
- Students must sign in their mobile phones to their section supervisor in the morning for safe keeping in the locker and must sign out their mobile phones just before they leave the school premises.
- If any of the student breaches the school policy the school will release the mobile phones/devices to parents in accordance with school policy. (Read Handbook)

Staff

- Staffs are allowed to bring their mobile phones to work.
- School will not take any responsibility for the lost, theft, damage of any of their mobile phones or devices.
- Staffs are not allowed to use their mobile phones during lessons or formal school time, and uses of mobile phones are limited to break time/after school.
- During lesson times mobile phones should be either switched off or silent.
- In case of emergency for using mobile phones during lesson time they should request permission to the Supervisor/Head of department.
- Strict disciplinary action will take if any of the staff member breaches the school policy.
- Staff Tablets/Laptops must be registered at the IT office for compatibility and login permissions.

Dealing with Complaints on E-safety

- Staff, students, parents must know how and where to report incidents. Concerns related to Safeguarding issues must be dealt with through the School's Policy and Procedures.
- The School's designated person for e-safety will be responsible for dealing with complaints and any complaint concerning staff or student misuse of the internet must be reported to the concerned person immediately.
- Sanctions for misuse through Interview/counseling by an appropriate member of staff, informing parents, removal of internet access for a specifies period of time, which may ultimately prevent access to files held on the system, including examination coursework.
- Refer to Complaint Policy for General complaint procedure.

PARENTS SUPPORT

- Parents will be informed of the School's E-Learning & E-Safety Policy which cabe accessed on the school website.
- Any issues concerning the internet will be handled sensitively to inform parents without undue alarm.
- Advice on filtering systems and appropriate educational and leisure activities including responsible use of the internet will be made available to parents.
- Through parents committee it will be encouraged with parents to attend practical sessions as well as suggestions for safe internet use at home.

POLICY DECISIONS

- School ICT resources may be increasingly used as part of the extended school agenda.
- Adult users will sign the school's acceptable use policy, **Refer to Acceptable use policy**.
- Parents of children and young people under 16 years of age will be required to signthe acceptable use policy on behalf of their child.
- **Password Security – Refer to Password Policy.**

Monitoring and review

This policy is the senior leadership's responsibility and they shall review its effectiveness annually, conducted between the e-learning/e-Safety and well being team. Ongoing incidents will be reported to the top management.

References to Read:

- **BYOD Policy**
- **Cyber Bullying Policy**
- **Complaint Policy**
- **Wellbeing Policy**
- **Password Policy**