HHIS E-safety policy

Reviewd May 2021

Background / Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the headteacher and directors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- Sexting
- Personal online behaviour that increases the likelihood of, or causes, harm, for example pro-anorexia, self-harm, substance abuse, hate or suicide sites.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

While children and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them. E-Safety issues can also affect adults who work or are associated with the school. For example school and

personal data being entered on web/social networking sites, fraudulent email traps and cyberbullying. It is impossible to eliminate risk completely. It is therefore essential, through good educational provision to manage the risk and deal with any threat to safety.

Teaching and Learning Using Online Technologies

The internet is a part of everyday life for education, business and social interaction. Benefits of using online technologies in education include:

- Access to world-wide educational resources
- Access to experts who would otherwise be unavailable
- Access to anytime, anywhere learning
- Collaboration between students and across classes, schools, networks of schools and services

When using online technologies, it is essential that children understand how to behave in a safe and responsible manner and also how to react when faced with inappropriate content or situations which make them feel uncomfortable.

At Hua Hin International School we believe that a comprehensive programme of e-safety education is vital for developing our students' ability to use technologies safely. This is achieved using a combination of discrete and embedded activities drawn from a selection of appropriate materials. We believe that just as children learn how to swim by going to a swimming pool so they will learn safe life-long online behaviours by accessing and using the internet. Members of staff constantly monitor students' use of the internet and other technologies. Our programme for e-safety education is evidenced in teachers' planning either as discrete or embedded activities.

Technology in Hua Hin International School

The school's ICT infrastructure is designed to minimise the risks associated with adult and pupil use of technology. This is provided by (CS Loxinfo) through Google Workspace for Education (GWE) which includes free, web-based programs like email, document creation tools, shared calendars, and collaboration tools. This service is available through an agreement between Google and Hua Hin International School. By default, Google advertising is turned off for Apps for Education users. No personal student information is collected for commercial purposes.

The school must also get parental consent before allowing any students under the age of 18 to use Additional Services (Youtube, Maps, Blogger, etc.).

Google Apps for Education runs on an Internet domain purchased and owned by Hua Hin International School and is intended for educational use. Teachers use GWE for lessons, assignments, and communication. GWE is also available at home, the library, or anywhere with Internet access. School staff will monitor students' use of GWE when students are at school. Parents are responsible for monitoring their child's use of GWE when accessing programs from home. Students are responsible for their own behaviour at all times.

Student safety is our highest priority.

Acceptable Use Policy (Privacy and Safety)

Google Workspace for Education (GWE) is primarily for educational use. Students may use GWE for personal use subject to the restrictions below and additional school rules and policies that may apply.

- Privacy - School staff, administrators, and parents all have access to student email for monitoring purposes. Students have no expectation of privacy on the GWE system.
- Limited personal use - Students may use GWE tools for personal projects but may not use them for:
    - Unlawful activities
    - Commercial purposes (running a business or trying to make money)
    - Personal financial gain (running a web site to sell things)
    - Inappropriate sexual or other offensive content
    - Threatening another person
    - Misrepresentation of Hua Hin International School, its staff or students. Apps, sites, email, and groups are not public forums. They are extensions of classroom spaces where student free speech rights may be limited.
- Safety
    - Students may not post personal contact information about themselves or other people. That includes last names, addresses and phone numbers.
    - Students agree not to meet with someone they have met online without their parent's approval and participation.
    - Students will tell their teacher or other school employee about any message they receive that is inappropriate or makes them feel uncomfortable.
    - Students are responsible for the use of their individual accounts and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should a user provide his or her password to another person.

This helps to ensure that staff and students rarely encounter material which is inappropriate or offensive. If / when they do, the school's AUAs and E-safety education programme ensure that they are equipped to deal with any issues in the most appropriate way.

Technologies regularly used by students and adult stakeholders include:

Staff:

- Laptops and desktops
- Mobile phones, cameras, iPads and Android tablets
- Interactive whiteboards
- Web-based programs like email, document creation tools, shared calendars, and collaboration tools
- Cloud-hosted services providing access to Schoolbase and Pupil Asset, including confidential pupil information

Students:

- Chromebooks and desktops
- Mobile phones, cameras, iPads and Android tablets
- Interactive whiteboards
- Web-based programs like email, document creation tools, shared calendars, and collaboration tools
- Other peripherals such as programmable toys, dataloggers, control technology equipment

We use year group logins for ease of access for students in Key Stage 1; all students from Year 3 upwards as well as all members of staff have their own individual, password protected logins to GWE.
As default, Safesearch is enabled which blocks inappropriate or explicit images from Google search results and Youtube is restricted so that signed-in users can only watch restricted and approved videos.
The school has separate networks - Admin, Teachers and Students - which can be accessed using a wired or wireless connection. Both wireless networks are encrypted and the wireless keys are kept securely by the school office. School staff and students are permitted to connect personal devices to the school's wireless network but the wireless key is not given to visitors to the school.

The E-Safety Curriculum

In line with the E-safety strand of the Computing Curriculum we have planned a range of age-related teaching and learning opportunities to help our students to become safe and responsible users of new technologies. These opportunities include:

- Specific activities, for example during Internet safety day (traditionally held in February) and Anti-bullying week (held traditionally in November)
- Parent workshops
- Age-related classroom activities using the ThinkUKnow materials
- Related work in PSHE lessons
- Posters and reminders in and around the school

Digital literacy

Students should be taught in all lessons to be critically aware of the content they access online and be guided to validate the accuracy of information by employing techniques such as:

- Checking the likely validity of the URL (web address)
- Cross checking references (can they find the same information on other sites)
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students are taught how to make best use of internet search engines to arrive at the information they require

Responsibilities

E-Safety Coordinator :

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with school ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- meets regularly with the Headteacher to discuss current issues, review incident logs and filtering / change control logs

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Agreement (AUA)
- they report any suspected misuse or problem to the E-Safety Co-ordinator or Headteacher for investigation / action / sanction
- digital communications with students (email / Hangouts / voice) should be on a professional level and only carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other school activities
- students understand and follow the school e-safety and acceptable use policy
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor internet activity in lessons, extra curricular and extended school activities

- they are aware of e-safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- when using school devices, such as class computers and IPads, teachers should log-out so students do not have access to staff user accounts

Designated person for child protection / Child Protection Officer
should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Students / pupils:

- are responsible for using the school ICT systems in accordance with the Student Acceptable Use Agreements, which they will be expected to sign before being given access to school systems.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Safeguarding Children Online

Our school recognises that different users will be expected to use the school's technology systems in different ways – appropriate to their age or role in school. We acknowledge the need to:

- Equip children to deal with exposure to harmful and inappropriate content and contact, and equip parents to help their children deal with these things and parent effectively around incidences of harmful and inappropriate conduct by their children.
- The school has published Acceptable Use Agreements for students and staff who sign to indicate their acceptance of our AUAs and relevant sanctions which will be applied should rules be broken. Any known or suspicious online misuse or problem will be reported to the designated E-Safety Coordinator for investigation/ action/ sanctions.

Responding to Incidents
It is important that all members of staff – teaching and non-teaching – are aware of how to respond if an e-safety incident occurs or they suspect a child is at risk through their use of technology. It is important that responses to e-safety incidents are consistent with responses

to other incidents in school. This may mean that serious actions have to be taken in some circumstances.
If an e-safety incident occurs Hua Hin International School will follow its agreed procedures for dealing with incidents including internal sanctions and involvement of parents (for ICT, this may include the deactivation of accounts or restricted access to systems as per the school's AUPs.

Where the school suspects that an incident may constitute a Child Protection issue, the usual Child Protection procedures will be followed.

Dealing with Incidents and Seeking Help
If a concern is raised, refer immediately to the designated person for child protection. If that is not possible refer to the headteacher. It is their responsibility to:

Step 1: Identify who is involved – any combination of child victim, child instigator, staff victim, or staff instigator

Step 2: Establish the kind of activity involved and whether it is illegal or inappropriate. If in doubt they should consult the E-safety coordinator or Headteacher.

Step 3: Ensure that the incident is documented using the standard child protection incident logging form.

Depending on the judgements made at steps 1 and 2 the following actions should be taken:

Staff instigator – if the incident involves or leads to an allegation against a member of staff, the school will follow the agreed procedures for dealing with any allegation against a member of staff .

Staff victim – Seek advice from your Human Resources (HR) officer.

Illegal activity involving a child – refer directly to the police – make clear that it is a child protection issue.

Inappropriate activity involving a child – follow standard child protection procedures.

Use of digital and video images

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In

particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. If personal equipment is used to take photos, the photos should be uploaded onto Google Drive and then deleted from the teacher's device.
- Members of staff must be aware of permissions granted by parents for the appropriate taking and sharing of images and video for students in their class.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.