Tokyo West International School

e-Safety Policy

Introduction

The ability to use technology and access information has transformed learning in schools. Young people need to develop the skills, knowledge, and understanding of using technology to develop as lifelong learners and for future employment. Teachers using information technology can increase student involvement and interest in a variety of topics. The benefits of using technology in school are certainly perceived to outweigh the risks. It is therefore essential, through good educational provision, to build students' awareness of the risks to which they may be exposed, so that they have the confidence and skills to face and deal with those risks.

Tokyo West International School (TWIS) will work with all concerned stakeholders (administration, staff, students, parents, community) to take necessary precautions to reasonably manage and reduce risks. The following e-safety policy explains how TWIS aims to achieve this, while also addressing wider educational issues in order to help young people and their parents/caregivers to be responsible users and stay safe while using the internet and other communications technologies for educational, personal, and recreational purposes. Some of the dangers they may face include:

1. The overuse of technology that may affect the social-emotional development and learning of the students.
2. Downloading harmful and/or illegal music, photo, or video files.
3. Issues related to plagiarism and copyright.
4. A failure to assess the quality and accuracy of information that they access on the internet.
5. Cyber-bullying
6. Inappropriate communication with strangers that may affect their daily life after school
7. Access to illicit, destructive or inappropriate websites on the internet.
8. Unauthorized access to/loss of/sharing of personal information.

Scope of the Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents/caregivers, visitors, community users) who have access to and are users of school information technology systems, both in and out of school. TWIS in collaboration with homeroom and specialist teachers as well as academic leaders, has the responsibility to control student behavior by upholding appropriate rules and disciplinary actions. If any inappropriate incident happens to the students regarding the use of technology, TWIS will, where known, inform parents/guardians of the incident that perhaps also may take place

outside of school.

Roles and Responsibilities

a. **The Head of School (headmistress/academic lead/administration lead, etc)**

The Head of School will be responsible for ensuring that:

- all staff members are trained and informed of the e-Safety policy
- a balanced information technology curriculum is in place and taught
- there is a system in place to allow for monitoring electronic correspondence and that internet activity incidents of abuse are reported
- a log of incidents are recorded which will inform future policy improvements

b. School Staff (teacher/admin staff/ nurse)

The school staff will be responsible for ensuring that:

- They have the awareness and knowledge about technology usage rules as well as appropriate disciplinary action.
- If they are aware that the suspected misuse happens, they are responsible for reporting to the head of school for further investigation.
- Their respective students understand basic copyright knowledge and avoid any plagiarism for their research.
- Their respective students follow the current e-safety and BYOD (Bring-Your-Own-Devices) policy.
- They monitor technology use in lesson, extracurricular, and expanded school activities.
- They are mindful of e-safety issues related to the use of portable phones, cameras, and handheld gadgets and they monitor their use and implement current school policies with regard to these devices

c. Students are responsible for:

Refer to BYOD policy and guidelines.

d. **Parents /Guardians**

Parents/Guardians play a crucial role in ensuring that their children understand the need to use the internet, social media and mobile devices in an appropriate way. Research shows that many parents and caregivers do not fully understand the issues and are less experienced in the use of information technology than their children. TWIS will therefore take every opportunity to help parents understand these issues through meetings and correspondences.

e. Parents and caregivers will be responsible for:

- endorsing (by signature) the student BYOD policy – staff and students whilst regulation and technical solutions are very important, must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognize and avoid e-safety risks and build their resilience. e-Safety education will be provided in the following ways:
- An age-appropriate digital citizenship curriculum should be provided as part of ICT/Well-being/PHSE/other lessons and should be regularly revisited –this will cover both the use of ICT and new technologies in school and outside school
- Key digital citizenship ideas should be reinforced as part of a planned program of assemblies and meetings
- Students should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- Students should be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of information communication technology, the internet and mobile devices both within and outside school
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff should always act as good role models in their use of ICT, the internet and mobile devices

Education – parents / caregivers

Some parents and caregivers may have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online experiences. Parents sometimes either underestimate or do not realize how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they should do about it.

f. Data Protection

Staff must ensure that they:

- Take care at all times to ensure the safekeeping of personal data, minimizing the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly logged-off at the end of any session in which they are using personal data.
- Transfer sensitive personal data using encryption and secure password protected devices. When personal data is stored on any portable computer system, USB stick or

any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (note that many memory sticks/cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device once it has been transferred or its use is complete