THE WESTMINSTER SCHOOL, DUBAI

E-safety Policy

POLICY FOR	E-Safety
PERSON RESPONSIBLE	Head of Pastoral/ IT
REVIEW DATE	31st May 2021
REVIEWED BY	Assistant Principals and Head of School
APPROVED DATE	16th June 2021
APPROVED BY	Executive Principal
DATE OF NEXT REVIEW	May 2022
RELATED POLICIES	Behaviour Policy, Social Media Policy, Safeguarding Policy, Online Security Policy, Anti-bullying Policy, Acceptable use of digital resources Policy

Executive Principal / CEO .....

E-Safety Policy

Introduction:

The Westminster School, Dubai (TWS) is committed to providing an exceptional education for young people. The safety and welfare of our students is of the utmost importance. Ensuring that students can safely access new technology and learn how to participate in the digital world without compromising their safety and security is a key part of delivering a well-rounded programme of education.

E-Safety at a simple level means being safe on the internet. Some people also include the safe use of technology in this as well. The pace at which technology is evolving can make it difficult to know what to include when talking about the safe use of the internet.

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 pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

Information and Communications Technology (ICT) covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- Podcasting
- Video Broadcasting / Vlogs
- Downloading
- Gaming on multiple platforms
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

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.

Purpose :

This E-Safety policy enables our school to create a safe e-learning environment that:

- Protects children from harm
- Safeguards staff in their contact with pupils and their own use of the internet
- Ensures the school fulfils its duty of care to pupils
- Provides clear expectations for all on acceptable use of the internet.

Aims of the e-safety policy:

- Protecting and educating students and staff in their use of technology.
- Informing teachers and parents/guardians about their role in safeguarding and protecting RIS students at school and at home.
- Putting policies and procedures in place to help prevent incidents of cyber-bullying within the school community.
- Having effective and clear measures to deal with and monitor cases of cyber-bullying.

E-Safety education will be provided in the following ways:

- Key e-safety messages should be reinforced as part of a planned programme of assemblies/pastoral activities.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information
- Pupils should be helped to understand the need to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet
- Rules for use of ICT systems / Internet will be posted in the students' planner.

Threats of using digital technology

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to, loss of, and sharing of personal information
- Internet grooming
- Radicalisation

- The sharing and distribution of personal images without consent
- Inappropriate communication and contact with others
- Cyber-bullying
- Access to unsuitable video and internet games
- An inability to evaluate the quality, accuracy/reliability and relevance of information on the internet
- Plagiarism and copyright infringement
- Downloading illegal or offensive content or applications
- Excessive use which may impact on social and emotional development & Learning addiction

ROLES AND RESPONSIBILITIES

Roles & responsibility of E-safety Officer

- Leads the e-safety committee
- 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 the KHDA / relevant body
- Liaises with school technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering /change control logs
- Attends relevant meeting / committee of Governors
- Reports regularly to Senior Leadership Team

Protection / Safeguarding Designated Safeguarding Lead

Should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding 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 report any suspected misuse or problem to the Head of House for investigation / action / sanction
• All digital communications with students / parents / carers 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 activities
• Students understand and follow the e-safety and acceptable use policies
• Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
• They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
• In lessons where internet use is pre-planned pupils 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.

Rules for publishing material online (including images of pupils):

School websites are a valuable tool for sharing information and promoting pupils' and students' achievements. We recognise the potential for abuse. Therefore, the following principles will always be considered:

- If an image, video or audio recording of a pupil/student is used, their surname should not be used
- Staff must not take photographs of pupils or students using their personal devices –
- All pupil/student photographs must be taken using TWS equipment.
- Files should be appropriately named in accordance with these principles.
- Only images of pupils/students in suitable dress should be used and group photographs are preferred (though not exclusively) in preference to individual photographs.
- Parents are given the opportunity to withdraw permission for the school to publish images/audio/video of their child on the school website.
- Content should not infringe the intellectual property rights of others – copyright may apply to text, images, music or video that originate from other sources.
- All copied or embedded content should be properly referenced.
- Content should be polite and respect others.
- Material should be proofread by a member of the school's Senior Leadership Team before being published. Children and young people use a variety of online.

Pupil/student rules for acceptable internet use:

We will adopt the rules as laid out below in an age-appropriate way for the students at TWS.

- I will ask permission from an adult before using the Internet.
- I will use computers and tablets safely.
- I will not look for websites that I know I'm not allowed to see.
- If I see anything that I know is wrong I will tell an adult straight away.
- I will not download anything without permission from an adult.

- I will not use memory sticks on school computers without permission from an adult.
- I will ask an adult before sending emails to unknown people.
- I will be polite and respect others when using the Internet.
- I will not give out any personal information over the Internet.
- I will not share my login details with others.
- I understand that the school may check my computer files and check what I am doing.
- I may/may not be allowed to play games on the computer to enhance my educational knowledge

Visitor rules for acceptable internet use:

Visitors' Internet use will vary depending upon the purpose of their visit. Generally we expect all visitors to abide by the following rules:

- I will respect the facilities by using them safely and appropriately.
- I will not use the Internet for personal financial gain, political purposes, advertising, personal or private business.
- I will not deliberately seek out inappropriate websites.
- I will report any unpleasant or upsetting material to a member of staff immediately.
- I will not download or install program files.
- I will not use USB memory devices on school computers.
- I will be polite and respect others when communicating over the Internet.
- I will not share my login details.
- I will not carry out personal or unnecessary printing.
- I understand that the school may check my computer files and monitor my Internet use.

Students:

Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

- Students will be expected to know and understand policies on the use of mobile devices and digital cameras.
- Students should also know and understand policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realize that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parent:

Parents and caregivers will be encouraged to support the school in promoting good e safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the website / blog
- Their children's personal devices in the school (where this is allowed)
- The school will monitor the impact of the policy using: (delete / add as relevant)
- Logs of reported incidents
- Surveys of reported incidents: ➢ Students ➢ Parents / Caregivers ➢ Staff

Confidentiality:

All reported cases will be treated with utmost confidentiality at all times.

Referral:

The school may refer the student to government or non-government agency concerned if deemed necessary.

Monitoring and Evaluation:

Pastoral Team and the IT team will monitor and evaluate the effectiveness of E-safety Policy alongside with Behaviour Policy annually. In case new legislation from UAE government and United Nation pertaining to Bullying and or Cyber Bullying, the policy should be amended in accordance with the national and international law set forth.