E-Safety Policy

The E-Safety Policy of the school seeks to ensure that students in the DIA Community are allowed the privilege of use of technology for educational, interactive and communicative purposes without causing offense or negative impact on fellow students, staff or other members of the community. As the E-Safety Policy also encompasses the Information Technology, Bring Your Own Device and Cyber-Bullying Policies existing in the school, it also covers any issues relating to willful damage or unauthorized use of hardware, software or network folders in the school at any time.

The E-Safety Policy of the school can be elaborated as follows:

Being a Responsible Student User of Devices and the School Network:

- Following the Information Technology Policy @ DIA (Policy H, Student Parent Handbook) which emphasizes the proper and appropriate use of technology and school network folders in accordance with the Acceptable Usage Guidelines of the same policy;
- Recognizing that the use of school devices and the network is privilege, not a right.

Being a Responsible and Caring Social Communicator:

- Following the Information Technology Policy @ DIA (Policy H, Student Parent Handbook) and the Bullying and Harassment Policy (Policy C, Student Parent Handbook) which emphasize proper and appropriate conduct online at all times in accordance with school expectations;
- Recognizing that any online conduct which can be regarded as cyber-bullying, even if it occurs off-campus during the academic year, and negatively impacts the academic environment of the school will be registered and dealt with by possible removal of technology privileges by the school.

Technology Mission Statement

The technology mission at DIA is to enable, energise and enhance education. DIA provides access to various hardware and software resources, as well as to the internet. The Information Technology policy at DIA is intended to allow the appropriate use of the technology resources of the school, and students will be encouraged to make use of the internet to support curriculum and research activities, either individually or as part of a group. Students will also be able to access a variety of information sources to which the school has acquired access; including news, selected information databases and holdings from other libraries.

DIA believes that the benefits of having access to the internet are huge for both students and educators, but among the vast resources of content on the internet are materials that are not suitable for school-age children. **It is not appropriate for students or teachers to purposefully locate material that is illegal, defamatory or offensive.** As responsible members of the school community, it is expected that all students and other members of the community will follow and adhere to the guidelines contained within this section.

Accessing Information Technology Equipment

It is expected that all students will respect the Information Technology equipment with which they have been provided, and realise that **using this equipment is a privilege, not a right.** Students are encouraged to use the school's computer network and internet connections for educational purposes. Students must conduct themselves in a responsible, efficient, ethical and legal manner at all times. Unauthorised or inappropriate use of the resources, including violations of any of the guidelines below, may result in cancellation of the privilege and further disciplinary action being taken.

Acceptable Usage Guidelines

- Students may not enter a computer room unless a teacher is present or unless they have permission to do so;
- The computers may not be used for any other purpose other than as directed by the teacher in charge, and students are responsible for their behaviour and communication whilst using the internet;
- Students should not play games or use any other software unless the teacher has given specific permission for this;
- The network and computers may not be used for commercial or profit-making purposes, advertising or political lobbying;
- Students should not tamper with the setup of the computer system or network, and should not seek to cause damage or engage in any unlawful activities, or develop or use any programmes that harass other users, infiltrate other computer systems, or cause disruption to the school's network and computing resources;
- Students should avoid intentionally wasting storage, printing, connectivity or processing resources ;
- Students should not seek access to restricted areas of the computer network from within or outside of the school;
- The equipment provided should not be swapped around, e.g., changing of keyboards, mice or other equipment from one computer to another is not allowed;
- Transmission or storage of any material in violation of any law or regulation or school policy is prohibited, including but not restricted to pornography or other material that is obscene, objectionable, inappropriate and/or harmful to children of any age;
- Privacy of communications over the internet and the school network cannot be guaranteed, and may be monitored, reviewed and inspected. Files stored on the school's network may also be subject to review and inspection;
- All communications and information accessible via the internet should be assumed to be privately owned property and subject to copyright. Correct attribution of authorship and reference must be observed at all times, without violation of copyright or other contracts;
- Students must not make use of another person's account/id/username/password, and should not allow other users to utilise theirs, or share this information with other people;
- Students are expected to abide by the generally-accepted rules of network etiquette:
    - Be polite, courteous and respectful in all communications, and use language appropriate to a school situations at all times while using the school's resources, or when interacting with members of the school community,
    - Do not reveal names, addresses, phone numbers, other identifying content or passwords, of yourself or other people, when communicating on the internet, unless approved by the teacher,
    - Do not agree to get together with someone you "meet" online without prior parental approval.

Network Folders

The school will issue each student a network folder (sometimes referred to as a home folder) that resides on the school's network. These are administered by the DIA technology team. The purpose of this folder is for students to have a convenient storage location for work and assignments throughout the year, and to develop an electronic portfolio.

The network folder is the personal property of the student to whom access has been granted to it. No student should attempt to gain access to any other individual's personal network folder. When necessary, access can be gained by school administrators.

Individuals are responsible for backing up their stored data, and it is strongly recommended that all network users purchase and use a USB memory stick of appropriate storage capacity for this purpose. At the end of the academic year, the student should remove all data from their network folder and store it on a CD/DVD/USB or other portable device. A copy of each student's completed electronic portfolio will be retained by the school.

Usage of network folders should be in accordance with the 'Acceptable Usage Guidelines' detailed earlier in this section.

Violation of the e-Safety Policy by a Student:

Any violation of the above policy may result in the following sanctions:

- *Loss of school-provided technology and network privileges;*
- *Sanctions as prescribed by the Student-Parent Handbook and possible referral to other appropriate authorities in more extreme cases;*
- *Monetary reimbursement to the school for any material damages or loss.*

Disciplinary sanctions may include student contract, suspension, or expulsion depending on the nature and severity of the bullying/harassment. ***Cyber-bullying*** *– even where the incident has been recorded out of school times and off the school premises - may result in technology privileges being removed and the administration of aforementioned disciplinary procedures.*

Date of Policy Formulation: March, 2014

Date of Policy Update: August, 2023