مدرسة الدوحة البريطانية
DOHA BRITISH SCHOOL

E-Safety Policy

Last Review: September 2023

Next Review: June 2024

Reviewer: Policy Committee

HORSES ORYXES CAMELS FALCONS SCORPIONS

1. Purpose

The purpose of this E-Safety policy is to establish a comprehensive framework for safeguarding our students while using digital technologies within our school community. This policy outlines our commitment to creating a safe and secure online environment, setting high standards for online behavior, and ensuring the responsible use of the internet and digital devices in support of teaching and learning.

2. Scope

This policy applies to all students, staff, and members of our school community who use digital technologies and have access to the internet within the school premises or during school-related activities.

3. Policy Statement

Our school is committed to ensuring the safety and well-being of our students in the digital age. We recognise the importance of harnessing technology for educational purposes while also protecting students from potential online risks.

4. Teaching and learning

4.1 Internet use by pupils at DBS is intended to enhance pupil learning. Towards this end, pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

4.2 Pupils will be taught to be critically aware of the internet based materials that they read and shown how to validate information before accepting its accuracy. The school will ensure that the use of internet derived materials by staff and pupils complies with academic honesty.

4.3 Pupils will be taught what internet use is acceptable and what is not and given clear objectives for Internet use. Pupils are informed that network and Internet use is monitored and inappropriate usage is appropriately followed up.

4.4 Through assemblies, Computer Science, IT and PSHE, pupils are taught how to behave and how to protect themselves in a digital environment. However, the school does not accept liability for events that occur outside the school.

4.5 Emerging technologies will be examined for educational benefit before use in school is allowed.

5. Cyberbullying

5.1 DBS takes the issue and occurrence of cyberbullying seriously. PSHE content about cyberbullying is delivered to pupils.

Downloaded and/or hard copies are uncontrolled. Verify that this is the correct version before use.

5.2 The school is committed to educating students about the consequences of cyberbullying and the importance of respectful online interactions.

5.3 If the school is aware of any cyberbullying incident within the school, the processes and consequences are the same as those of non-cyberbullying as defined in DBS' Anti-Bullying Policy and related procedures.

6. Internet access

6.1 DBS' internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. The school ensures that the filtering is regularly reviewed and improved. Virus protection is updated regularly and this aspect of internet security is also systematically updated.

6.2 If, even within the filtered digital environment, staff or pupils discover an unsuitable site, it must be reported to the IT Network Administrator who will take action.

6.3 The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.

6.4 Social networking and personal publishing: the school will deny access to social networking sites and pupils will be advised not to use these at home until they reach the age stipulated by the site administrators.

6.5 Personal Devices: the usage of personal devices by pupils is outlined in DBS' BYOD policy. Mobile phones will only be permitted to be used on teacher instruction. Wearable technology, such as smart watches should be treated in the same way as other devices that allow internet communication.

6.6 While connected to the school network, pupils are restricted by school filtering and security. If using a mobile network, the school is not accountable for what is accessed by pupils.

6.7 If a student brings a mobile phone into school and there is evidence that it has been used for taking photographs or filming in school, or there is evidence of inappropriate or indecent images stored on it or there is evidence of cyberbullying, then this will be treated as a serious disciplinary matter and further action will be taken. This will involve confiscation of the phone, contact with the parent/carer, appropriate sanctions applied and the Governing board may be informed.

7. E-safety concerns and complaints

7.1 Members of the school's Senior Leadership Team will deal with parental or pupil concerns about e-safety in line with the school's complaint procedure, with matters escalated to the level of the Principal as appropriate.

7.2 Any complaint about staff misuse of the internet must be referred to the Principal.

7.3 Complaints of a child protection nature must be dealt with in accordance with DBS' Child Protection Policy and the related procedures.

Downloaded and/or hard copies are uncontrolled. Verify that this is the correct version before use.

8. Roles and responsibilities

The Principal is to:	• accept overarching responsibility for e-safety in the school; • be the point of contact for staff misconduct related to internet usage.
Heads of School are to:	• follow through incidences of pupil misconduct related to internet usage.
Teachers are to:	• deliver content about e-safety and provide reminders when using portable devices in other curriculum areas; • enforce this policy; • deal with matters of cyber bullying, logging such occurrences on the school management information system (ISAMS); • preview any internet content that they intend to share with pupils.
DSLs	• follow related Child protection and Safeguarding Procedures in the case of internet related child abuse.
Pupils are to:	• follow school guidance and regulations for the use of personal devices and the internet.
Parents are to:	• support the school's e-safety policy and guidelines.
The IT Network Administrator is to:	• remove access to inappropriate sites as requested by teaching staff; • assume responsibility for the security of the school's system (inclusive of filtering and virus protection) under the direction of the IT Manager (Artan Holding) .

9. Related documents

Staff Acceptable Usage Policy

Student Acceptable Usage Policy

BYOD Policy

Anti- Bullying Policy

A.I Policy

Child Protection Policy

Child Protection Procedure

Safeguarding Policy

Downloaded and/or hard copies are uncontrolled. Verify that this is the correct version before use.


Thank you