مدرسة الدوحة البريطانية

DOHA BRITISH SCHOOL

E-Safety Policy

Last Review: September 2021

Next Review: June 2022

Reviewer: Policy Committee

HORSES ORYXES CAMELS FALCONS SCORPIONS

1. Purpose

The purpose of this policy is to ensure that all staff, parents, governors and pupils understand the school's approach and commitment to e-safety.

2. Scope

The policy applies to all schools.

3. Definitions

Bring Your Own Device (BYOD) refers to the practice of pupils bringing their own technology including smartphones, tablets and laptops for educational use and improvements in their learning processes.

4. Policy Statement

Doha British School (DBS) recognises that the internet is an essential element in 21st Century life for education, business and social interaction. Internet use is also a part of the curriculum and a necessary tool for staff and pupils.

The school is committed to providing pupils with quality internet access as part of their learning experience and assumes a responsibility for informing pupils about how to safely make use of the internet and about potential risks.

DBS adopts the use of internet filters in the interest of e-safety.

1. Teaching and learning

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.

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.

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.

Through assemblies, Computer Science 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.

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

4.2 Cyberbullying

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

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.

4.2 Internet access

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.

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

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.

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.

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.

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.

Parental advice to their child for home Internet usage

Parents are advised to provide guidance to their child for using the internet at home including to:

- never to give out personal details of any kind which may identify them, their friends or their location;
- not to post personal photographs on social networking spaces;
- set passwords, to deny access to unknown individuals and to block unwanted communications;
- report abuse or cyberbullying to their parents or to a member of school staff.

The school's published contact details

The contact details on the school's website and in print literature should be the school's address, email address and telephone number. Staff or pupils' personal information will not be published.

E-safety concerns and complaints

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.

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

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

5. 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:	• enforce this policy; • follow through incidences of pupil misconduct related to internet usage.
Teachers are to:	• deliver content about e-safety via Computer Science and PSHE 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.
Designated Child Protection Officers are to:	- follow related Child protection 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) .

6. Related documents

Staff Acceptable Usage Policy

Student Acceptable Usage Policy

BYOD Policy

Anti- Bullying Policy

Child Protection Policy

Child Protection Procedure

Health and Safety Policy

Thank you