SHAIKH KHALIFA BIN ZAYED
BANGLADESH ISLAMIA SCHOOL
ABU DHABI EDUCATION COUNCIL
(Licence No. 109/1 Dated 1/10/1980)
P. O. Box : 8174, ABU DHABI, UAE
Tel. : 02-4446904, Fax : 02-4446899
Email : bdschool80@yahoo.com

مدرسة الشيخ خليفة بن
زايد البنغلاديشية الإسلامية
مجلس ابوظبي للتعليم
(ترخيص رقم ١٠٩ / ١ بتاريخ ١٩٨٠/١٠/١م)
ص.ب : ٨١٧٤ - أبوظبي
الامارات العربية المتحدة
تلفون : ٠٢-٤٤٤٦٩٠٤ - فاكس : ٠٢-٤٤٤٦٨٩٩

Letter No. BISC/PL/147 رسالة الرقم

Date 09.12.2021 التاريخ

CYBERSECURITY POLICY

Shaikh Khalifa Bin Zayed Bangladesh Islamia School will:

- Educate students on the socially acceptable netiquette (Do's and Don'ts in the cyber world).
- Be giving cyber literacy to the extent where our students use cyber space for productive work which will help in the progress of the community.
- Educate students to recognize the pros and cons of cyberspace and to safeguard themselves and fellow beings.
- Ensure the safety of our students through regular monitoring by the IT Department, Teachers, Behaviour Management Committee during distance learning programs.
- Conduct awareness programs on cyber bullying and cyber security for our stakeholders.
- Provide school internet access that has been customised for student use, hence it includes appropriate filtering techniques.
- Educate students to evaluate internet content by ICT teachers.
- Educate students to the reporting line if they face any problem in cyberspace.
- Edify the stakeholders about the importance of password security and indispensability of logging out of accounts once they end their work.

Shaikh Khalifa Bin Zayed Bangladesh Islamia School Cyber Safety Policy for Students

1. Students have to respect the privacy of others.
2. Students have to report and flag content that is abusive or illegal.
3. Students have to adhere to copyright restrictions when downloading material from the Internet, including software, games, movies or music.
4. Students should not use an alias/alternate name as username when they interact/chat with others online.
5. Students have to report online bullying immediately to the teacher and parents or someone whom they trust.
6. Students have to use a strong and unique password with combinations of numbers, uppercase and lowercase letters and special characters for each account(s).
7. Students have to keep the browser, operating system and antivirus up-to-date.
8. Students have to obtain software from trusted sources. Always scan files before opening them.
9. Students should lock their screen when they are finished using their computer/ tablet/ phone. Further, they have to set it to lock automatically when it goes to sleep.
10. Students are expected to check to see if the web address begins with https:// whenever they sign in online.
11. Students should make privacy settings in social media accounts in such a way that profile and posts are visible only to close friends and acquaintances.
12. Students should connect only with known individuals.
13. Students have to be mindful of their digital reputation. Students shall not post something embarrassing, harmful or inappropriate.
14. Students have to report to the service provider immediately if the account is hacked. If possible, the student should deactivate the account.
15. Students shall not share their personal information: real name, date of birth, phone number etc. unnecessarily.
16. Students should never send their pictures to unknown persons or share them on social media.
17. Students should not open emails and attachments from strangers.

18. Students should not respond to any suspicious email, instant message or web page asking for personal information.
19. Students are expected not to enter their password when someone is sitting beside them as they may see it.
20. Students are expected not to share their password with anyone.
21. Students should not save their username and password on the browser.
22. Students should never steal other's information.
23. Students shall not access or use files without the permission of the owner.
24. Students should not copy software which has copyright without the author's permission.
25. Students should not bully others online by teasing, threatening, using rude or offensive language, making derogatory or hateful comments.
26. Students shall not use someone else's password even if it is shared with them.
27. Students shall not log in as someone else to read their emails or mess with their online profiles
28. Students shall not attempt to infect or in any way try to make someone else's computer unusable.
29. Students shall not meet unknown (even if they are known only through online interaction) people alone; always inform an adult or a friend.
30. Students should not open or download any attachments from an unknown source as they may contain viruses.

Password policy:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.)
- Remember passwords instead of writing them down. If students need to write their passwords, they are obliged to keep the paper or digital document confidential.
- Exchange credentials only when absolutely necessary.
- Changing passwords every two months.

Disciplinary Action:

We expect all our students to always follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: Verbal warning & Written warning will be given and the student will be trained on cyber security policy (Behavior Policy will be followed).
- Intentional, repeated or large scale breaches (which cause severe financial or other damage): School will invoke more severe disciplinary action (Behavior Policy will be followed).

***The school will examine each incident on a case-by-case basis.**

Anti-Cyber Bullying Policy

Shaikh Khalifa Bin Zayed Bangladesh Islamia School, in partnership with parents and community, strives to prepare every student to be digitally literate, a lifelong learner and a productive citizen.

Shaikh Khalifa Bin Zayed Bangladesh Islamia School gives technological advancement, in its careful attention for the benefit it has on students' lives, achievement, and career development. However, the school is mindful of the potential for bullying to occur. Central to the School's anti-bullying policy is the belief that 'all pupils have a right not to be bullied' and that 'bullying is always unacceptable'.

By cyber-bullying, we mean bullying by electronic media:

- Bullying by texts or messages or calls on mobile phones
- The use of mobile phone cameras to cause distress, fear or humiliation

- Posting threatening, abusive, or humiliating material on websites, blogs, personal websites, social networking sites
- Using e-mail to send threatening messages to others
- Hijacking/cloning email accounts
- Making threatening, abusive, and defamatory or humiliating remarks in chat rooms, Facebook, YouTube etc.

Whilst education and guidance remain at the heart of what we do, the school reserves the right to take action against those who take part in cyber-bullying

- All bullying is damaging but cyber-bullying and harassment can be invasive of privacy at all times.
- The school will use, as appropriate, the full range of sanctions to correct, punish or remove pupils who bully fellow pupils or harass staff in this way, both in or out of school.
- The school will use its power of confiscation where necessary to prevent pupils from committing crimes or misusing equipment.
- All members of the School community are aware of the fact that they have a duty to bring to the attention of the Principal any example of cyber-bullying or harassment that they know about or suspect.

GUIDANCE FOR STUDENTS

If you believe you or someone else is the victim of cyber-bullying, you must speak to an adult as soon as possible. This person could be a parent/guardian, your tutor, or the Supervisor.

- Do not answer abusive messages but log and report them.
- Do not delete anything until it has been shown to your Class Teacher, parents/guardian or the Supervisor (even if it is upsetting, the material is important evidence which may need to be used later as proof of cyber-bullying).
- Do not give out personal ID details.
- Never reply to abusive emails.
- Never reply to someone you do not know.
- Stay in public areas while you are using chat rooms.

GUIDANCE FOR PARENTS

It is vital that parents and the school work together to ensure that all pupils are aware of the serious consequences of getting involved in anything that might seem to be cyber-bullying.

- Parents can help by making sure that their child understands the school's policy and, above all, how seriously the school takes into account incidents of cyber-bullying.
- Parents should also explain to their children legal issues relating to cyber bullying .
- If parents believe their child is the victim of cyber-bullying, they should save the offending material (if need be by saving an offensive text on their or their child's gadget) and make sure they have all relevant information before deleting anything.
- Parents should contact the respective Supervisor of the class as soon as possible. A meeting can then be arranged with the Principal, which may involve other relevant members of staff.

Signed:

Mir Anisul Hasan
Principal

Shaikh Khalifa Bin Zayed Bangladesh Islamia Private School L.L.C.
ابوظبي
Abu Dhabi - U.A.E
Estb 1980