Online/Cyber safety Policy

Cyber-bullying is defined as the use of electronic and information devices, such as email, instant messages, text messages, mobile phones and websites to send or post messages or images that may harm an individual or a group.

Scope of the policy: Students, teaching and non-teaching staff and other stake-holders.

Aim of the policy:

- To protect students from morally offensive, inappropriate or other undesirable content on the Internet and preventing to access websites that contain such materials.
- To educate students on the proper use of the Internet and sharing of personal information.
- To promote good practices in using secure Internet systems.
- Informing teachers and parents/guardians about their role in safeguarding and protecting Bright Riders' students at school and at home.
- Putting policies and procedures in place to prevent incidents of cyber-bullying within the school community.

At Bright Riders School, internet access is designed expressly for students use and includes filtering appropriate to the needs of our students. It prohibits the children of viewing or downloading of any inappropriate material which may not be useful for their mental development.
In addition to this,

- Instructions are given to the teachers and librarians to play an active role in protecting the students from the dangers of Internet and monitoring websites accessed by students as well as monitoring students during a School trip in case they have access to electronic devices that are connected to the Internet.
- Social Media sites have been blocked for student/staff access within the school boundaries.
- Teachers guide the students in on-line activities that will support the learning outcomes, depending on the students' age and maturity.
- Prohibiting the use of the Internet to attempt unauthorized access to other computers, information or prohibited services.

- All students and staff are educated on the importance of password security and the need to log out of accounts and not toopen e-mails or attachments from unknown sources.
- Prohibiting the downloading or copying of copy righted material,including software, books, articles, and photographs etc., which are not licensed for use by the School.
- Prohibiting the undertaking of any activity that may introduce viruses or other malicious software to the School's network.

The school ensures that the personal information placed on the School's Internet and intranet is secure, even for a password-protected website.

Roles and Responsibilities

School:

- To ensure that an effective and reliable Internet filtering system is in place.
- To develop and implement an online/cyber Security Policy that includes, by way of example, the requirements prescribed in this policy.

School Principal:

- Schedules continuing professional development to keep teachers aware of the most recent Internet safety developments.
- Periodically reviews the School's technology infrastructure with appropriate technology staff and makes improvements as needed.

Teachers, librarians and other staff members:

- To educate the students not to open e-mail or attachments from unknown sources.
- To educate students on the types of information that are safe to share with others online, and information that should never be shared as it could put them at risk.
- To teach students to recognize the various forms of cyber-bullying and know what steps to take if confronted with that-behaviour.
- To educate students on how to report unpleasant Internet-content to their class teacher, Counsellor or parents.

Parents' Role

- Keep the computer in a central place, where everyone can see what's on the screen.
- Stay involved on what they are doing online, especially if it'sgot to do with searching and looking for new information etc.
- Check out which sites they want to access, or which games theywant to play and tell them if they are acceptable or no-go zones,until they reach a certain specified age.
- Set time limits. Giving kids unlimited access to online causes unlimited problems for parents. Tell them how many hours they have in a week.
- Explain online habits. Explain strangers often play pretend games and they are not really who they claim to be. They need to be clearly told that no matter how interesting or "just like me"the stranger sounds like, they are not to respond.
- Remind them that they should not engage in any form of cyber bullying – even in jest.
- Beyond online, watch what content you have on your computer.Often we receive email that is not age appropriate for our children, but we leave that in our mail boxes or desktops.

If your children have started to do their homework online, or are gathering information, researching facts etc., explain to them clearly how they should not "copy and paste" (plagiarize) content for their homework, unless they mention sources etc. Their teachers should help them to understand this, but parents should ensure that their ward follows the instructions given by the teacher.

Note: Any such case is brought to the notice of the school Principal and IT department for the corrective measures and further action.

Dr. Rishikesh Padegaonkar
School Principal

Prepared on: 25/03/2021
Review Date: 25/03/2023
Review Date: 26/01/2024
Next review date: 26/01/2025