Russian International School
Academic Year 2023 - 2024

E-CYBER SAFETY POLICY

1. WHAT IS E-CYBER SAFETY POLICY?

E-Cyber Safety is a prevention of the following misuses of technology: harassing, teasing, intimidating, bullying, threatening or terrorizing another student by way of any technological tool.

School E-Cyber Safety is a guide for prevention of sending or posting inappropriate email messages, instant messages, text messages, digital pictures or images or website postings, including Facebook, Instagram and blogs, which have the effect of:

- Physically, emotionally or mentally harming or disturbing a student;
- Disturbing or causing a student to fear physical, emotional or mental harm;
- Disturbing or causing a student to fear damage to or loss of personal property;
- Creating an intimidating or hostile environment that significantly interferes with a student's educational opportunities.

2. WHAT DOES THE SCHOOL DO TO PREVENT CYBER BULLYING?

- Students are made aware of the dangers of the Internet and issues like Cyber Bullying through their Information Technology classes across phases.
- Parents-School Contract has clauses for the use of Technology Devices at school premises.
- There is strict enforcement of the school's policy regarding student use of mobile phones included in the Parent-School Contract.
- Regular monitoring by the school of the students' use of technology at school premises.
- Encouraging students to use technology as innovative techniques of learning in a Safe and Right way by using educational websites/learning apps provided by the teachers.
- Incidents of Cyber Bullying can be reported through a direct way of communication via an Electronic E-School Management System or designated channels of communication.

3. HOW DOES THE SCHOOL RESPOND TO INSTANCES OF CYBER BULLYING?

Bullying in any form needs to be dealt with according to the individual issues that arise. Incidents of bullying might be brought to School attention by:
- Students, Parents to Class Teachers, Head Teachers, SEND Coordinators, Administration.
The consultation process is usually handled by the counseling staff and can include:

Responses to the "victim(s)"
- talking with the student(s) experiencing the bullying
- talking with parents, staff or friends of the student(s)
- counseling and giving the student(s) strategies to effectively manage the bullying

Responses to the perpetrator(s)

- talking with the individual or group doing the bullying and directing them into a more positive and caring way of behaving
- talking to parents regarding their child bullying behavior
- implementing appropriate consequences from a range of sanctions
- alerting staff to the negative patterns of behavior for purposes of monitoring, preventing further occurrences and promoting positive patterns amongst the students concerned
- supporting the student over a period of time to ensure that the bullying has stopped

4. WHAT CAN PARENTS DO?

- Learn about and understand how the new technologies work.
- Talk to children and find out what technologies they use.
- Develop a relationship with children so that they will be comfortable and confident to come to you if they are being bullied, or someone they know is being bullied.
- Watch out for signs such as suddenly not going online as much as before, or conversely, going online more frequently, or unwillingness to go to school.
- Contact the school to talk about the issue, even if the bullies are from a different school.
- If the bullying is occurring through mobile phone, contact police or the phone service provider. You may also want to change your child's telephone number and try to have the child understand that he/she shouldn't widely give out the phone number.
- Teach your child to behave in a moral and ethical way when using the technologies. They shouldn't post or message anything that they wouldn't want you, their friends, community members or their teachers could see.

5. WHAT CAN STUDENTS DO?

Watch their own online behavior.

- Never post or message anything that they would feel ashamed of or embarrassed by if parents, grandparents or one of teachers should see it.
- Remember that once sent, students have lost control of that material.

What should you do if you are being bullied in cyber space?

- Respond and tell the bully to stop. State clearly that the behavior is not right, and that you find it offensive.
- Make no further responses from this point.
- Keep copies of any offensive messages or images.
- Tell your parents.
- Report it to the Class Teacher or Coordinator.
- Do not be afraid that reporting will only make the bullying worse. It won't get better if you don't do something about it.
- Report it via an E-School Management System.

What should you do if you know someone else is being bullied?

- Care enough to do something about it, even if it does not affect you personally.
- Tell someone – your Class Teacher or a Coordinator
- Report it via an E-School Management System.

Channels of communication:

Hotline School Whats App:	+971-50-613-60-91
Tel. Administration:	+971-4-264-15-15
Tel./Whats App IT Support:	+971-584-65-29
Tel./Whats App Health and Safety:	+971-50-358-02-99
Parents communication:	parents.ris@dubairuschool.com
Teachers communication:	student.ris@dubairuschool.com

E-Safe School - Online Safety is aimed at:

- dealing with online challenges
- guidance on the online use of technology
- empowering Students with Online Safety, skills, knowledge and IT tools
- supporting Parents Engagement in Online Safety
- developing innovative, creative and socializing skills through consolidation of Teachers – Students – Parents efforts
- enriching Teachers Training for Online Safety
- providing IT support/expert consultancy for E-Safety
- managing Password Security, Technical Security and Digital Content
- protecting Data Management
- monitoring Online Safety Incidents
- promoting Anti-Bullying/E-Cyber Safety across all phases.

RIS provides technology for teaching and learning; creates safe and secure online environment for children to learn. Both protecting children online and providing them with the skills and understanding to protect themselves online is of RIS prioritized objectives.

E-Safety Online Risk Assessment:

- ➢ Content - what Students see online
- ➢ Contact - who they communicate with online
- ➢ Code of Conduct - how they act online

E-Challenges Offline Risk Assessment:

- Online bullying
- Access to inappropriate content
- Over-engagement with technology (gaming, social media, screen time)

Online Safety is in relation to:

- Online Safety
  a) *the curriculum reflects the personal, social and technical aspects; differentiation for SoD*
  b) *students are aware of the content they access online; research skills are based on social media resources and copyright regulations.*
- School Policies (E-Cyber Safety; Code of Conduct; Anti-Bullying; Child Protection; Safeguarding; Wellbeing)
- consistent online safety messages to all members of the School Community
- communication with the Dubai Police Headquarters
- supervision by Safety Coordinator - *responsible for monitoring incidents and handling sensitive issues*
- the use of mobile technology - users understand the risks associated with the use of mobile technology and are encouraged to be responsible users, both in school *(safe use within School to support teaching and learning)* and outside
- the use of social media – *the content/images/video/links sharing is monitored*
- Staff Training (*all Staff takes active responsibility for Online Safety*).

The use of computer systems, system users and personal data is subject to regular review and updating:

- password security (appropriate password requirements for user access);
- Internet access online at School is filtered for all users/password protected and regularly updated;
- differentiated Internet access is available for Staff and customized filtering changes are managed by School;
- anti-virus and malware prevention is applied and regularly updated across school systems;
- system backups are regularly made and are an integral component of system recovery routines.