Cyberbullying Policy

This is a whole school policy and applies to the School as a Whole

This policy should be read in conjunction with the ***Behavior Policy****,* ***Safeguarding and Child Protection Policy*** *and* ***Code of Conduct.***

Knowledge International School (KIS) believes that everyone in the school community has the right to learn and to teach in a supportive and caring environment without fear of being bullied. We are committed to helping all members of the school community to benefit from information and communication technology, whilst understanding its risks, and to equip children with the knowledge and skills to be able to use it safely and responsibly.

Aims:

This policy aims to ensure that:

- Staff, Students, and parents know about cyberbullying and its consequences.
- We have the knowledge, policies, and procedures to prevent and, if necessary, to deal with cyberbullying in school or within the school community.
- We monitor the effectiveness of our procedures.

What is Cyberbullying and Categories:

Cyberbullying may be defined as the use of electronic communication particularly by using the Internet and mobile phones, to bully a person, typically by sending messages of an intimidation, harassment or cyber-stalking (e.g. sending unwanted texts messages), sexting (e.g., sending and receiving sexually explicit messages), vilification/defamation, unauthorized publication of private information/images and ‘trolling’ (e.g. abusing the internet to provoke or offend others online). It can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target.

Cyberbullying is significantly different from other types of bullying and can take place at any time and it typically can hit the large audience due to the global and worldwide domains infrastructure. In some cases, **bullying can lead to be a criminal offence and would be addressed according to the Federal state law.**

Preventing Cyberbullying: The best way to deal with cyberbullying is to prevent it from happening in the first place. There is no single solution to the problem of cyberbullying, but the school will do the following as a minimum to impose a comprehensive and effective prevention strategy:

Roles and Responsibilities: **Designated Safeguarding Lead (Safety officer/ Social Worker)** will take overall responsibility for the co-ordination and implementation of cyberbullying prevention and response strategies, and will:

- Ensure that all incidents of cyberbullying both inside and outside the school are dealt with immediately and managed and/or escalated in line with the procedures set out in the school's Anti-bullying Policy, Behavior Policy, and Child Protection Policy.
- Ensure that all staff know that they need to report any issues concerning cyberbullying to the Designated Safeguarding Lead.
- Ensure that all staff are aware of Cyberbullying Prevention Duties and that all staff are aware of their responsibilities by providing clear guidance for staff on the use of technology within school and beyond. All staff should sign s declaration stating that they have read and understood the Staff Code of Conduct.

Guidance for Staff to Report

Guidance on safe practice regarding the use of electronic communications and storage of images is contained in the Code of Conduct. The school will deal with inappropriate use of technology in line with the Code of Conduct which could result in disciplinary procedures.

If you suspect or are told about a cyber-bullying incident, follow the protocol outlined below:

- Ask the student to show you the device, take a clear note and save the message/image and everything on the screen relating to an inappropriate text message or image, make a transcript with the date and times.
- Print out the offending material; if necessary, make sure you have got all pages in the right order and that there are no omissions.
- Inform the Designated Safeguarding Lead immediately and pass them the information you have including normal procedures of interviewing the child in presence of the Safeguarding Lead and taking statements, which will then be followed, particularly if a child protection issue is presented.

The IT Department will

- Ensure adequate safeguards are in place to filter and monitor inappropriate content and alert the Designated Safeguarding Lead to safeguarding issues. The internet filter records access to prohibited sites which enables the IT department to report issues immediately to the Designated Safeguarding Lead.
- Ensure that school visitors are given clear guidance on the use of technology at school. Visitors will be given highly restricted guest accounts which will not allow any access to personal data.
- Ensure that any misuse of the system will result in access to the system being withdrawn.

Use of Technology at School: **All members of the school community are expected to take responsibility for using technology positively, as well as training.** The following is in place:

- All staff are expected to sign to confirm that they have read and understood the Acceptable Use Policy. All staff are expected to sign to confirm they have read and understood the Staff Code of Conduct.
- All staff are expected to have read and understood Guidelines for Staff when Children are using Digital Devices. All children are expected to have been taken through and understood IT Safety Agreement.

Guidance for Parents at Home:

- Do not wait for something to happen before you act. Make sure your child understands how to use these technologies safely and knows about the risks and consequences of misusing them.
- Encourage and give the confidence to your child to talk to you in case of any problems regarding cyberbullying. If they do have a problem, contact the school or Internet provider to do something about it.
- Keep the electronic devices in public places area in the house; if you have the standalone PC then keep the screen to the visible side, so you can watch the activities.
- Be up front with your child that you will periodically investigate the files on the computer, the browser history files, and your child's public online activities. Watch out for secretive behavior as you approach your child when they are online, such as rapidly switching screens, changing passwords and for attempts to hide online behavior, such as an empty history file.

Guidance for Students:

- If you believe that you or someone else is the victim of cyberbullying, you must speak to an adult as soon as possible. This person could be a parent/guardian, or a staff member on your safety network.
- Be careful of whom you allow to become a friend online and think about what information you want them to see.
- Protect your password. Do not share it with anyone else and change it regularly
- Always log off from the computer when you have finished or if you leave the computer for any reason.
- Never reply to abusive e-mails, nor reply to someone you do not know
- Always stay in public areas in chat rooms
- Do not answer abusive messages but save them and report them

Think carefully about what you write – do not leave yourself open to bullying

REMEMBER: Always tell your Parents or Teachers

The school will ensure parents are informed of the cyberbullying policy and cyberbullying leaflet for children and the procedures in place in the Anti-Bullying Policy to deal with all forms of bullying including cyberbullying.

Disciplinary Action & Sanction:

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 ethical, financial or other damages: School will invoke a more severe disciplinary action which leads to complete ban and/or confiscation of use of technology and suspension from school. All the actions will take place for a set period of time agreed by the principal. (Behavior Policy will be followed).
- If the conduct causes or threatens to cause a substantial disruption at school or interferes with the rights of students to be secure, the school administration may impose consequences in conjunction with the **Behavior Policy**, **Safeguarding and Child Protection Policy** and **Code of Conduct.**
- All copies of correspondence are placed in the files of both the victim and the bully.
- If the incident is repeated, the matter would be referred to the Higher Management/Ministry/ADEK with a recommendation about the future of that student at KIS.
- The Administration may also report the Cyberbullying or Harassment to the police.

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