

Anti-Cyber-Bullying Policy

The school recognizes that technology plays an important and positive role in everyone's lives, both educationally and socially. It is committed to helping all members of the school community to understand both the benefits and the risks, and to equip children with the knowledge and skills to be able to use technology safely and responsibly.

The aims of this policy are to ensure that:

- We safeguard the pupils in the real and virtual world
- Pupils, staff and parents are educated to understand what cyber-bullying is and what its consequences can be
- Knowledge, policies and procedures are in place to prevent incidents of cyber-bullying in school or within the school community
- We have effective measures to deal effectively with cases of cyber-bullying
- We monitor the effectiveness of prevention measures

Definition: What is Cyber-bullying?

Cyber bullying can be defined as exploiting the Internet to intentionally harm individuals or groups. It also involves continued harassment, abuse and ridicule by email or any other means of communication. Cybercrime also involves hacking and piracy, blackmailing and the traditional forms of online crimes.

Mr. Bill Belsey, defined this unpleasant and particularly intrusive phenomenon in the following terms:

"Cyber-bullying involves the use of information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group that is intended to harm others".

Cyber-bullying can involve Social Networking Sites, emails and mobile phones used for SMS messages and as cameras. In addition;

- It can be used to carry out all the different types of bullying; an extension of face-to-face bullying
- It can also go further in that it can invade home/personal space and can involve a greater number of people
- It can take place across age groups and school staff and other adults can be targeted
- It can draw bystanders into being accessories
- It includes: threats and intimidation; harassment or 'cyber-stalking';
- Vilification/defamation; exclusion or peer rejection;
- Impersonation; unauthorized publication of private information or images ('happy-slapping'); and manipulation
- It can be an illegal act

Preventing cyber-bullying Understanding and discussion:

- Staff will receive training in identifying cyber-bullying and understanding their responsibilities in developing e-safety. The Manager of ICT may

delegate this training to the Academic Coordinators, Head of the Departments, and Head of the Sections. In this training all staff will be helped to keep up to date with the technologies that children are using.

- The delivery of lessons is an important part of preventative strategy and will discuss keeping personal information safe and appropriate use of the Internet.
- It is desirable that the pupils will be involved in a response to cyber-bullying. They will have a voice through the School Student Council and the Parental Council.
- Pupils will be educated about cyber-bullying through a variety of means: assemblies, conferences, Anti-bullying Week and projects etc.
- Pupils will sign a Safe and Acceptable Use Policy before they are allowed to use school computer equipment and the Internet in school and parents will be encouraged to discuss its contents with their children.
- Parents will be provided with information and advice on e-safety and cyber-bullying via literature, talks, etc.
- Pupils and staff will be involved in evaluating and improving policies and procedures through Student Council, Houseparent meetings, and Yearly meetings.

Policies and procedures:

- Ensure regular review and update of existing policies to include cyber-bullying where appropriate
- School will keep good records of all cyber-bullying incidents. Heads of Year to log all incidents with the Coordinator and all staff to use the cyber-bullying recording cases
- Manager of ICT will do reviews as technologies develop
- Publicize rules and sanctions effectively
- The IT department will use filtering, firewall, anti-spyware software, anti-virus software and secure connections to safeguard the pupils. Though electronic controls alone can never be 100% effective, and pupils should adhere to the guidelines.

Promoting the positive use of technology:

ICT Admin:

- Make positive use of technology across the curriculum
- Use training opportunities to help staff develop their practice creatively and support pupils in safe and responsible use
- Ensure all staff and children understand the importance of password security and the need to log out of accounts Making reporting easier
- Ensure staff can recognize non-verbal signs and indications of cyber-bullying with regular safeguarding training.
- Publicize and promote the message that asking for help is the right thing to do and shows strength and good judgment
- Publicize to all members of the school community the ways in which cyber-bullying can be reported
- Provide information for all students including reassurances about 'whistleblowing' and the appropriate way of informing appropriate staff or

- parents about incidents they have witnessed
- Provide information on external reporting routes e.g. mobile phone Company, and Internet service provider.

Evaluating the effectiveness of prevention measures:

- Identify areas for improvement and incorporate pupils, teachers, IT professionals and counselors ideas for anti-cyber bullying in school
- It is desirable to conduct an annual evaluation including a review of recorded cyber- bullying incidents.

Responding to Cyber Bullying:

Most cases of cyber-bullying will be dealt with through the school's existing Anti-bullying Policy and this must remain the framework within which incidents of bullying are investigated. However, some features of cyberbullying differ from other forms of bullying and may prompt a particular response. The key differences are:

- Impact: the scale and scope of cyber-bullying can be greater than other forms of bullying
- Targets and perpetrators: the people involved may have a different profile to traditional bullies and their targets
- Location: the 24/7 and anywhere nature of cyber-bullying
- Anonymity: the person being bullied will not always know who is bullying them
- Intent: some pupils may not be aware that what they are doing is bullying
- Evidence: unlike other forms of bullying, the target of the bullying will have evidence of its occurrence
- It is possible that a member of staff may be a victim and these responses apply to them too.

Support for the person being bullied:

- Offer emotional support; reassure them that they have done the right thing in telling someone
- Advise the person not to retaliate or reply. Instead, keep the evidence and take it to their parent or a member of staff (in the case of staff they should take it to their line manager)
- Advise the person to consider what information they have in the public domain
- Unless the victim sees it as a punishment, they may be advised to change e.g. mobile phone number
- If hurtful or embarrassing content is being distributed, try to get it removed from the web. If the person who posted it is known, ensure they understand why it is wrong and ask them to remove it. Alternatively, contact the host provider and make a report to get the content taken down.
- In some cases, the person being bullied may be able to block the person bullying from their sites and services. Appendix 1 contains information on what service providers can do and how to contact them

Investigation:

- The safeguarding of the child is paramount and staff should investigate in accordance with the Safeguarding and Child Protection Policy.
- Members of staff should contact the HoS for the purposes of investigation
- All cases (with the exception of Child Protection issues) will be referred to the concerned HoS first.
- Interviews will be held in accordance with the Anti-Bullying Policy Guidelines.
- Staff and pupils should be advised to preserve evidence and a record of abuse; save phone messages, record or save-and-print instant messenger conversations, print or produce a screenshot of social network pages, print, save and forward to staff whole email messages.
- If images are involved, determine whether they might be illegal or raise child protection concerns. If so, contact the Child Protection Manager, who may involve the LADO (Local Authority Designated Officer), the local police in cases of actual/suspected illegal content.
- Identify the bully.

The UAE Cyber Crime Law:

The UAE Cybercrime Law Number five of UAE 2012 stipulates penalties like

- Jail terms that could go up to a life sentence.
- Fine ranging between Dh50, 000 and Dh3 million depending on the severity and seriousness of the cybercrime
- Can even be ordered to leave the country if they insulted people or even their spouse on messaging platforms such as WhatsApp.

Social Media Dos and Don'ts under UAE Law:

- Do not post other people's pictures or videos without consent: Don't post without asking, whether it's a friend or a photographer. It could be breach of

privacy or copyright.

- Do not make threats: Posts or comments that are abusive or threatening to other people can land you in court.
- Do not post vulgar pictures or of alcohol: Non-Muslims can drink, but keep it under control if pictures are inappropriate. Drunken photos that offend Islamic values or morals of the UAE can lead to legal trouble.
- Do not post pornographic or material that contains nudity without permission can be a breach of defamation and privacy laws, both of which can carry hefty fines and even jail time.
- Do not insult Islam: warns against offending Islamic morals and values.
- Do not gossip: People could face fines of up to Dh1 million if they spread false information.
- Do not bully or harass: Users must not post content which includes hate speech, incites violence or which is threatening or contains graphic or gratuitous violence.

Six Steps to Deal with Cyber-Bullying:

- Block a suspected bully immediately
- Leave the subject matter in dispute when chatting
- Resisting the desire for revenge or retaliation
- Submit the bullying report to the communications service provider
- Using the Internet securely
- Informing the competent authorities about a suspected bully.