Gulf Asian English School, Sharjah

Tel: +971 6 5340000, Fax: +971 6 53440000
P. O Box: 3406, Sharjah – UAE
Web: www.gulfasian.com

GULF ASIAN ENGLISH SCHOOL (GAES)
Anti-Cyber Bullying Policy 2026-2027

GAES Anti Cyber-Bullying Policy
Updated, 6th May, 2026

Introduction

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.

Aims and Objectives of the Anti-Cyberbullying Policy

The aims of this policy are to ensure that:

1. **Safeguarding and Protection:** All pupils are protected from cyberbullying and online harassment in both physical and virtual environments, promoting a safe, respectful, and inclusive school community.
2. **Awareness and Education:** Pupils, staff, and parents are provided with appropriate guidance and awareness to understand the nature, forms, and potential consequences of cyberbullying, including its impact on the emotional, psychological, and social well-being of pupils.
3. **Prevention and Awareness Measures:** Effective policies, procedures, educational programmes, and preventive strategies are established and implemented to minimise the risk of cyberbullying within the school and the wider school community.
4. **Reporting and Response Mechanisms:** Clear, accessible, and confidential reporting procedures are established to enable pupils, staff, and parents to report suspected or confirmed incidents of cyberbullying promptly and appropriately.
5. **Effective Intervention and Support:** Appropriate and timely measures are taken to address incidents of cyberbullying, protect affected pupils, provide necessary support, and ensure that appropriate consequences and follow-up actions are implemented in accordance with the school's Behaviour Management Policy and applicable regulations.

6. **Digital Citizenship and Responsible Online Behaviour:** Pupils are encouraged to demonstrate responsible, ethical, and respectful behaviour when using digital devices, online platforms, social media, and other forms of electronic communication.
7. **Monitoring and Continuous Improvement:** The effectiveness of prevention strategies, reporting mechanisms, and intervention procedures is regularly monitored and evaluated to identify areas for improvement and strengthen the school's approach to preventing and addressing cyberbullying.

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

Look out for the following sample scenarios where someone has been:

- Sending, sharing or posting nasty, hurtful or abusive messages.
- Humiliating someone by posting/sharing embarrassing videos or images.
- Tagging someone inappropriately in an image.
- Spreading rumors or lies about someone online.
- Trolling- saying mean things to stir people up against someone.
- Imitating someone online.
- Making threats towards someone online.
- Sending repeated harassment and threatening messages (Cyber Stalking)
- Deliberately excluding someone from a group/conversation.

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 all other stakeholders. 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 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.
- 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, Stakeholders meetings, and Yearly meetings.
- If you find yourself aware of any similar situations where someone is being subject to cyber bullying, you should report such incidents to the school immediately. Although you can

report to anyone in school, make sure you know how to contact the school Cyber Safety Committee who can provide specific help and support.

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.
- 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 Manager will:

- 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 to make reporting easier.
- Pupils may contact to the Class Teacher when they are concerned about a bullying issue.
- 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 he 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 incidents of bullying are investigated. However, some features of cyber-bullying 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

Parent Note:

Teach your children the safeguards for the scenarios and ensure they follow the below guidelines in cases where bullying might be happening:

- Notify a parent or guardian (someone whom you trust) about the incident immediately.
- Don't respond, forward or delete any of the offensive messages.
- Obtain screenshots and gather as many details as possible about the profile that has been sending offensive messages.
- Tell your teacher/ Wellbeing team members or other trusted adult as soon as possible.

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 immediate reporting person)
- 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.

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 Cyber Safety Committee for the purposes of investigation
- All cases (with the exception of Child Protection issues) will be referred to the concerned supervisor 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 school shall take appropriate steps to identify the pupil or individual responsible for the alleged cyberbullying through a fair, confidential, and impartial review of the reported incident and available evidence, such as messages, screenshots, emails, or

online posts. All concerns shall be handled sensitively, ensuring the privacy and dignity of those involved and avoiding premature conclusions before the facts are established.

- Any allegations of cyberbullying or inappropriate online conduct involving a member of staff shall be handled promptly, confidentially, and in accordance with the school's safeguarding and child protection procedures, applicable UAE laws and regulations, and relevant guidance issued by the competent educational authorities. The matter shall be referred to the appropriate authority for investigation and necessary action, ensuring the safety and best interests of the pupil are prioritized.

Sanctions and Disciplinary Measures

The Senior Leadership Team (SLT), in consultation with the ICT Manager, where appropriate, shall determine and implement proportionate sanctions for substantiated incidents of cyberbullying, in accordance with the school's Behaviour Management Policy, safeguarding procedures, and applicable UAE laws and regulations.

The objectives of sanctions shall be to:

1. **Ensure the Safety and Well-being of the Affected Pupil:** Take appropriate measures to protect the pupil affected by cyberbullying, restore their sense of safety, and prevent further incidents.
2. **Promote Accountability:** Ensure that the pupil responsible for cyberbullying understands the nature and impact of their actions, accepts responsibility, and recognises the importance of respectful online behaviour.
3. **Deter Further Incidents:** Reinforce the school's zero-tolerance approach to cyberbullying and promote a school culture in which online harassment, intimidation, and misuse of digital platforms are not accepted.
4. **Apply Appropriate Sanctions:** Implement proportionate disciplinary measures in accordance with the school's Behaviour Management Policy, Acceptable Use Policy, and relevant agreements governing the use of technology and online platforms.
5. **Consider the Circumstances of the Incident:** Determine appropriate sanctions after considering the nature, severity, frequency, and impact of the incident, the age and developmental needs of the pupils involved, the available evidence, and any relevant

mitigating circumstances, including whether the behaviour was intentional or occurred in retaliation. Such circumstances shall not automatically excuse harmful behaviour.

6. **Promote Behavioural Modification:** Provide appropriate educational interventions, counselling, guidance, and follow-up support to help the pupil responsible understand the consequences of their actions, develop empathy, and demonstrate positive and responsible online behaviour.
7. **Address Harmful Digital Content:** Where appropriate and lawful, require the removal or deletion of harmful content, images, messages, or files associated with the incident, while ensuring that relevant evidence is preserved for safeguarding purposes and that no unauthorised access to personal accounts or devices takes place.

The school shall document the actions taken, monitor the well-being of the affected pupil, and conduct appropriate follow-up to ensure that the cyberbullying has ceased and that further incidents are prevented.

Legal duties and powers:

- The school has a duty to safeguard all members of the school community and provide a safe, healthy, and respectful learning environment.
- Authorised school staff may ask a pupil to show relevant messages or other mobile phone content when necessary to address a suspected cyberbullying incident.
- Where a mobile phone may contain evidence of cyberbullying or a suspected criminal offence, authorised staff may review only the relevant content, in accordance with school procedures and applicable laws.
- Cyberbullying may constitute a legal offence under applicable UAE laws and regulations. Serious cases shall be referred to the appropriate authorities when necessary.

Social Media Dos and Don’ts under UAE Law:

All pupils are expected to use social media responsibly, respectfully, and safely, in accordance with applicable UAE laws and the school’s Digital Safety and Anti-Cyberbullying Policies.

- **Respect Privacy and Consent:** Do not take, share, or publish another person's photographs, videos, private messages, or personal information without appropriate consent and lawful authorisation.
- **Avoid Threats and Abusive Language:** Do not post or send threatening, insulting, humiliating, or defamatory messages about others.
- **Maintain Appropriate Online Conduct:** Do not share obscene, sexually explicit, or otherwise prohibited content, or content that violates UAE laws and public morals.
- **Respect Religious and Cultural Values:** Do not publish or share content that insults religions, promotes hatred, or disrespects the religious and cultural values protected under UAE law.
- **Do Not Spread False Information:** Verify information before sharing it. Do not circulate rumours, fabricated content, or misleading information that could harm individuals or the wider community.
- **Never Cyberbully or Harass Others:** Do not engage in online bullying, stalking, intimidation, hate speech, discrimination, blackmail, or the sharing of harmful content targeting another person.
- **Respect Copyright and Ownership:** Do not copy, distribute, or publish another person's photographs, videos, or creative work without the necessary permission or legal authorisation.
- **Report Inappropriate Content:** Report cyberbullying, online threats, suspicious activity, or harmful content to the school's designated safeguarding personnel and, where necessary, the appropriate authorities.

Six Steps to Deal with Cyber-Bullying:

- Block the Perpetrator: Block the person responsible for cyberbullying on the relevant platform.
- Disengage Safely: Avoid responding to provocative or abusive messages.
- Do Not Retaliate: Refrain from threats, arguments, or revenge.
- Preserve Evidence and Report: Save screenshots and relevant messages, and report the incident to the platform or service provider.
- Practise Online Safety: Strengthen privacy settings and protect personal information.

- Seek Help and Report: Inform the school's designated safeguarding personnel and, where necessary, the competent UAE authorities.

Review & Monitoring

The school shall regularly review and monitor the implementation and effectiveness of this Anti-Cyberbullying Policy, including prevention strategies, reporting procedures, and intervention measures. The policy shall be reviewed annually to ensure alignment with applicable UAE laws, educational regulations, and emerging online safety concerns.