# Gulf Asian English School, Sharjah

# Cyber Safety Policy

# 2026-2027

## Introduction

The internet provides valuable opportunities for teaching, learning, communication and collaboration. However, its use also exposes students and staff to potential risks, including cyberbullying, online fraud, data breaches, inappropriate content and other cybersecurity threats. Ensuring a safe and responsible digital environment is therefore essential to protecting the privacy, security and wellbeing of all members of the school community.

This Cyber Safety Policy establishes guidelines and preventive measures to safeguard students and staff against common cyber threats, promote responsible online behaviour, protect digital information and ensure the safe and ethical use of digital technologies within the school community.

## Aims of the Cyber Safety Policy

- Protecting and educating students and staff in their use of technology.
- Informing teachers and parents/guardians about their role in safeguarding and protecting students at school and at home.
- Putting policies and procedures in place to help prevent incidents of cyber-bullying within the school community.
- Having effective and clear measures to deal with and monitor cases of cyber-bullying.

**Gulf Asian English School ensures that:**

- Students will be made aware of acceptable and unacceptable Internet use.
- Students will be taught, where appropriate, to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Students will be educated about the effective use of the Internet.
- Students will be taught how to evaluate online content by ICT teachers.
- Students will be taught how to report unpleasant online content to their class teacher or supervisor.
- The school Internet access is designed expressly for student use and includes filtering appropriate to the needs of our students.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites they visit.
- The use of Internet-derived materials by students and staff complies with copyright law.
- All students and staff understand the importance of password security and the need to log out of accounts.

## Social networking and personal publishing:

The school has a duty of care to provide a safe learning environment for all its students and staff and will ensure the following:

- Blocking student access to social media sites within school boundaries.
- Educating students about why they must not reveal their personal details or those of others, or arrange to meet anyone from an online site.
- Educating both students and staff as to why they should not engage in online discussion revealing personal matters relating to any members of the school community.
- Educating both students and staff about ensuring all technological equipment is always password/PIN protected.
- Informing staff not to accept invitations from students or parents/guardians on social media.
- Informing staff about regularly checking their security settings on personal social media profiles to minimize risk of access of personal information.

### Maximum Limits on Digital Use

The school shall adopt a balanced and age-appropriate approach to digital learning, taking into consideration students' developmental needs, learning objectives, health, well-being and the nature of the educational activity.

| Educational Stage | Indicative Maximum of Daily Instructional Time Allocated to Digital Learning |
|---|---|
| KG1 & KG2 | 10% |
| Class 1–4 | 25% |
| Class 5–8 | 50% |
| Class 9–12 | 75% |

*The above percentages shall serve as indicative maximum limits, subject to applicable SPEA directives and the school's review of their suitability and impact.*

### Prohibited Uses of Digital Technology

Students and staff shall not use school devices, networks or digital platforms for:

- Accessing unauthorized websites, social media platforms or applications during school hours.
- Playing non-educational electronic games without specific teacher authorization.

- Viewing, sharing or distributing entertainment content unrelated to approved educational activities.
- Cyberbullying, harassment, threats, discriminatory conduct or any form of digital abuse.
- Photographing, recording or sharing images, videos or audio recordings of individuals without appropriate authorization.
- Bypassing school security systems, content filters or network restrictions, including the unauthorized use of VPNs or similar circumvention tools.
- Cheating, plagiarism, impersonation or other forms of academic dishonesty.
- Accessing, downloading, creating or distributing unlawful, harmful or inappropriate digital content.
- Sharing passwords, accessing another person's account or attempting to gain unauthorized access to school systems.

**Digital Content Standards**

Gulf Asian English School shall ensure that digital learning materials and online resources used for educational purposes are:

a. Appropriate to the age, maturity and educational needs of students.

b. Relevant to the curriculum and intended learning outcomes.

c. Consistent with UAE laws, national identity, cultural values and ethical standards.

d. Free from harmful or inappropriate content, including pornography, violence, extremism, hatred, gambling, illegal drugs and deliberately misleading information.

e. Free from unnecessary advertisements, inappropriate commercial promotions and unauthorized third-party content.

f. Obtained from reliable, legitimate and approved sources.

Teachers shall review digital resources before classroom use and report unsuitable content to the relevant school authority.

**Reporting, Documentation and Incident Management**

- The school shall maintain a secure record of significant digital incidents, including the nature of the incident, date of reporting, actions taken, persons responsible for follow-up and the outcome, as appropriate.
- All digital incidents shall be managed through the school's established reporting, safeguarding, behaviour management and information security procedures.

- Records shall be maintained confidentially, with access restricted to authorized personnel and information handled in accordance with applicable data protection requirements.
- Serious incidents involving child safety, cyberbullying, unauthorized disclosure of personal information or cybersecurity breaches shall be escalated promptly to the appropriate school leadership and external authorities where required.
- Corrective and preventive measures shall be implemented to reduce the likelihood of similar incidents recurring.

## Parents' Role at Home

- It is important that you are aware of your child's internet activities including the social media channels they utilise, games or other online activities they are involved in. Being aware of your child's online activities will help you identify possible threats to educate and advise your child accordingly.
- Keep the computer in a central place, where everyone can see what's on the screen.
- Stay involved (without stepping on their toes constantly) on what they are doing online – especially if it's got to do with searching and looking for new information etc.
- Tell them the "No-Can-Go" sites and "No-Can-Play" games rules ahead of time. Check out which sites they want to access, or which games they want 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 a week.
- Explain online behaviour: Explain strangers often play pretend games and they are not really who they claim to be. Explain how sometimes a nine year girl from the US is really a 50 year old man from Bangkok. They need to be clearly told that no matter how interesting or "just like me" the stranger sounds like, they are not to respond.
- Switch Safe Search on as a setting: It's great that most inappropriate content does get filtered by Etisalat or du here in UAE, but there are many slip ups and search results may often have content that's not age appropriate.
- Remind them that they should not engage in any form of cyber bullying – even in jest. They should not do anything online that they would be ashamed of doing in real life.
- 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 mailboxes or desktops. Set the example, clean up.

- 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 understand this, but you should make it clear that this is not on.
- There are parental control tools available to help and protect your children from harmful and inappropriate online content. Phones, Tablets, Game Consoles and other devices that connect to the internet have parental control settings.
- Be involved. Be courteous. Be alert. Show on-going interest in what they are playing, reading, and doing online. And always remind them that there is life (and a wonderful one) outside that screen.

***Parents are expected to ensure that their ward(s) do not carry devices or electronic goods of any form without the approval of the Supervisor concerned. They must at all times demonstrate restraint and respect for the members of the school community, including all students and personnel while using social media. Parents must not breach confidentiality, defame or make threats to any person in the school community.***

## Monitoring, Compliance and Continuous Improvement

Gulf Asian English School annually review the implementation and effectiveness of this Policy to ensure that digital technologies continue to support educational achievement, student safety and well-being.

- ***This policy is aligned with and supports the Sharjah Private Education Authority (SPEA) Policy on the Safe and Balanced Use of Digital Learning, 2026.***
- ***All sanctions relating to cyber safety incidents will be applied fairly and consistently, in line with the school's Behaviour Management Policy.***

| | |
|---|---|
| **Approved By** | **Principal** |
| **Last Review Date** | **21st April 2026** |