

The American School of Egypt



Cyber Bullying Policy & Student Acceptable Use Policy Guidance

Adoption August 2023

Academic Year 2023/2024

Policy & Guidance Contents

Policy & Guidance Contents	2
Student Acceptable Use Policy and Internet Use	3
Terms of AUP Agreement:.....	3
Student Safety/Education:	3
Cyber Bullying Policy & Guidance	3
Introduction.....	3
Aims.....	3
What is Cyberbullying?.....	3
Definitions:.....	4
Understanding and discussion:.....	4
Ensure regular review and update of existing policies to include cyberbullying where appropriate.....	4
Promoting the positive use of technology at ASE will:.....	5
Making reporting easier.....	5
Evaluating the effectiveness of prevention measures.....	5
Responding to cyberbullying:.....	5
Support for the person being bullied:.....	5
The aim of the sanctions will be:.....	6
Guidance for Pupils specific to Cyberbullying:.....	6
Notes specific to Cyber Bullying:.....	6
Student Acceptable Use Policy and Internet Guidelines:	7
Basic Internet/Network Etiquette & Safety Rules:.....	7
ASE Responsibilities:.....	8

Student Acceptable Use Policy and Internet Use

Students will digitally sign an age appropriate version of this Acceptable Use Policy and the Internet/Network Safety Agreement at school through a link provided in Google Classroom.

- The purpose of providing technology devices and Internet and network access in schools and homes is to support the ASE's educational objectives.

Terms of AUP Agreement:

- To be allowed access to school computer systems, computer networks, software applications, including Google Applications for Education, and the Internet, students must read the appropriate version of this agreement and sign the consent form.
- Students will digitally sign the consent form on Google Classroom.
- Parents, please read this document so that you are familiar with policy and the rules for Internet/Network Usage:

The ASE is providing access to its school computer systems, computer networks, ASE-adopted tools and devices, software applications, including Google Applications for Education, and the Internet for educational purposes only, including accessing and sharing information with teachers and other students, storing files, conducting research, and collaborating on projects with others.

- If you have any doubt about whether a contemplated activity is educational, consult with the Principal or teacher assigned to assist you.
- Use of the ASE's network and Internet is a privilege.
- A user who violates this agreement shall, at a minimum, have access to the network and Internet terminated and is subject to additional disciplinary action based on the severity of the violation.

All users are bound by the ASE Code of Conduct and the following terms and conditions - The same policies and behaviour expectations extend to students throughout the school and the use of all internet based activities - this includes social media use and to behaviour outside of school that affects students from The ASE.

Student Safety/Education:

Cyber Bullying Policy & Guidance

Introduction

The ASE recognises that technology plays an important and positive role in everyone's lives, both educationally and socially. The ASE 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

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 cyberbullying.
- We monitor the effectiveness of prevention measures.

What is Cyberbullying?

- Cyber-bullying means any intentional, electronically transmitted (including the use of text messaging, instant messaging, or the posting of text or images) verbal or graphic act that a student or group of students repeatedly exhibit toward another student(s) and the behaviour causes mental harm (including humiliation and embarrassment) and is sufficiently severe, persistent or pervasive.
- Any cyber-bullying, harassment or intimidation is strictly prohibited.
- If a student is found to have engaged in cyber-bullying, disciplinary action will be recommended.
- If a student thinks that he or she is the victim of cyber-bullying, the situation should be immediately reported to an adult staff member.
- Students are encouraged to notify school staff if they suspect another student is being cyber-bullied.
- Any form of Sexting: Sexting is the sending of sexually explicit images through any electronic media, including but not limited to text messaging, instant messaging, or email. Sexting is strictly prohibited and is considered a serious offence. Sexting should be immediately reported to an adult staff member.

Definitions:

- Willful: The behaviour has to be deliberate, not accidental.
- Repeated: Bullying reflects a pattern of behaviour, not just one isolated incident.
- Harm: The target must perceive that harm was inflicted.
- Computers, phones, and other electronic devices: Cyberbullying can involve Social Networking Sites, emails and mobile phones used for SMS messages and as cameras.
- 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 'cyberstalking'; vilification/defamation; exclusion or peer rejection; Impersonation; unauthorised publication of private information or images ('happy slapping / AFWA'), and manipulation
- It can be an illegal act Preventing cyberbullying

Understanding and discussion:

- Staff should complete training in identifying cyberbullying and understanding their responsibilities in developing e-safety.
- The delivery of PSHE and Computing lessons are 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 cyberbullying.
- They will have a voice through the Student Council.
- Pupils will be educated about cyberbullying through a variety of means: assemblies,

conferences, Anti-bullying Week, projects (Computing, PSHE, Drama, English),

- 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 cyberbullying via literature and workshops.
- Pupils and staff will be involved in evaluating and improving policies and procedures through School Council, Staff Meetings.

Ensure regular review and update of existing policies to include cyberbullying where appropriate

- The American School of Egypt will keep good records of all cyberbullying incidents.
- Heads to log all incidents using Bullying Report Form.
- Publicise rules and sanctions effectively
- The IT department will use filtering, firewall, anti-spyware software, anti-virus software and secure connections to safeguard the pupils.

Promoting the positive use of technology ASE International School 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.

Making reporting easier

- Pupils may contact teachers through Google Classroom or by email when they are concerned about a bullying issue
- Ensure staff can recognise non-verbal signs and indications of cyberbullying with regular safeguarding training.
- Publicise and promote the message that asking for help is the right thing to do and shows strength and good judgement.
- Publicise to all members of the school community the ways in which cyberbullying 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

Evaluating the effectiveness of prevention measures.

- Identify areas for improvement and incorporate pupil ideas derived from Student Council
- It is desirable to conduct an annual evaluation including a review of recorded cyberbullying incidents.

Responding to cyberbullying:

- Most cases of cyberbullying 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.

- 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 cyberbullying 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 cyberbullying
 - 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
- The safeguarding of the child is paramount and staff should investigate in accordance with the ASE International School Safeguarding and Child Protection Policy
- Members of staff should contact the appropriate Head for the purposes of investigation
- All cases (with the exception of Child Protection issues) will be referred to and logged by the Safeguarding Lead.
- Interviews will be held in accordance with the ASE International School Anti Bullying Policy
- 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 email
- If images are involved, determine whether they might be illegal or raise child protection concerns. If so, contact the SLT.
- Identify the bully. See Notes for guidance ·

The aim of the sanctions will be:

- to help the person harmed to feel safe again and be assured that the bullying will stop
- to hold the perpetrator to account, getting them to recognise the harm caused and deter them from repeating the behaviour
- to demonstrate to the school community that cyberbullying is unacceptable and that the school has effective ways of dealing with it, so deterring others from behaving similarly
- Sanctions for any breaches of AUP or internet/mobile phone agreements will be applied
 - In applying sanctions, consideration must be given to type and impact of bullying and the possibility that it was unintentional or was in retaliation
 - The outcome must include helping the bully to recognise the consequence of their actions and providing support to enable the attitude and behaviour of the bully to change
 - A key part of the sanction may well involve ensuring that the pupil deletes files

Guidance for Pupils specific to Cyberbullying:

- Due to the anonymous nature of digital communication, anyone with a mobile phone or internet connection can be the target of cyberbullying.
- If you feel you are being bullied by email, text or online, do talk to someone you trust.
- Never send any bullying or threatening messages.
- Keep and save any bullying email, text or images.
- If you can make a note of the time and date bullying messages or images were sent and note any details about the sender.
- Use blocking software; you can block instant messages from certain people, “unfriend” people on social networking sites or use mail filters to block email.
- Do not reply to bullying or threatening messages or emails; this could make matters worse. It also lets the bullying people know that they have found a “live” number, email address or “active” social networking contact.
- Do not give out your personal details online; if you are in a chatroom, online game or IM session
- Watch what you say about where you live, the school you go to, your email address, your friends and family. All these things can help someone build up a picture about you.
- Do not forward abusive texts, email or images to anyone. If they are about you, keep them as evidence.
- Do not ever give out passwords!
- Do report instances of cyberbullying you have seen or heard about, even if not directed at you. There is no such thing as an innocent bystander, if you have seen the posts, messages or images then you could be considered as part of it if you do not report it!

Notes specific to Cyber Bullying:

Identifying the Bully - Although the technology seemingly allows anonymity, there are ways to find out information about where bullying originated.

It is important to be aware that this may not necessarily lead to an identifiable individual and often is beyond the capabilities of what The ASE can do. It is common for teachers at The ASE to be presented with screenshots of examples of cyberbullying - however information from these cannot be extracted (non-original source material).

It has been found that if another person’s phone or school network account has been used, locating where the information was originally sent from will not, by itself, determine who the bully is. There have been cases of people using another individuals’ phone or hacking into their IM or school email account to send nasty messages.

In cases where you do not know the identity of the bully, some key questions to look at:

- Was the bullying carried out in the school system?
- If yes, are there logs in school to see who it was?
- Contact the school IT helpdesk to see if this is possible.
- Are there identifiable witnesses that can be interviewed?
- There may be children who have visited the offending site and left comments, for example.
- If the bullying was not carried out on the school system, was it carried out on a mobile or a particular internet service (e.g. IM or social networking site)?
- If the bullying was via mobile phone, has the bully withheld their number?
- If so, it is important to record the date and time of the message.
- If the number is not withheld, it may be possible for the school to identify the caller.

- For example, another student may be able to identify the number or the school may already keep records of the mobile phone numbers of their pupils.
- Content shared through a local wireless connection on mobile phones does not pass through the service providers' network and is much harder to trace. Similarly text messages sent from a website to a phone also provide difficulties for tracing for the internet service or mobile operator.
- Has a potential criminal offence been committed?
- If so, the police may have a duty to investigate.
- Criminal offences here include harassment and stalking, threats of harm or violence to a person or property, any evidence of sexual exploitation (for example grooming or inappropriate sexual contact of behaviour. It can be a very serious matter and can constitute a criminal offence.
- Although bullying or cyberbullying is not a specific offence in Egyptian law, there are criminal laws that can apply in terms of harassment, for example, or threatening behaviour, or indeed – particularly for cyberbullying –threatening and menacing communications.

Student Acceptable Use Policy and Internet Guidelines:

- Never make, reproduce or distribute videos, images, sound recording, or other mediums that show behaviour prohibited by the AUP or the School Behaviour Policy on school property or at school events, including using school-owned or personal electronic devices.
- Never post depictions of prohibited behaviour on social networking sites such as Facebook, Google Plus, YouTube, Instagram, Snapchat or any other similar Websites.
 - Any depictions of prohibited behaviour must be immediately turned over to the School Staff.
- Never post personal information, such as full name, address, telephone number, bank or credit card numbers, etc.
- Consider not posting photographs of yourself.
- Never post sensitive or inappropriate photos.
- Assume that everything you post is on the Internet permanently.
- Do not agree to meet in person someone you know only from a social networking site or chat room.

Basic Internet/Network Etiquette & Safety Rules:

- The ASE Code of Conduct and ASE policies on “Plagiarism/Cheating,” “Bullying and Other Forms of Aggressive Behaviour,” and “Bullying – Harassment – Intimidation — Sexting” apply to Internet/network conduct.
- The ASE will monitor and filter all student email and Google Apps content. Inappropriate or flagged messages will be blocked and sent to an administrator.
- Be polite. Use appropriate language and graphics.
- Do not use network or Internet access to make, distribute or redistribute jokes, stories or other material based on slurs or stereotypes relating to race, gender, ethnicity, nationality, religion or sexual orientation.
- Teachers may allow individual students to use email, electronic chat rooms, instant messaging, social networking sites and other forms of direct electronic communications, including Gmail and Google Hangouts, for educational purposes only and with proper supervision.
- Student Photos/Student Work - Publishing student pictures and work on websites promotes learning, collaboration and provides an opportunity to share the achievements

of students.

- Parents/guardians must indicate their written consent to publish their child's photo or school work on any school-related website before the item is published to the web.
- Privacy - Network and Internet access is provided as a tool for your education.
- The ASE reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage.
- All such information files shall be and remain the property of the ASE, and no user shall have any expectation of privacy regarding such materials.

Copyright - Do not download copyrighted material or software without permission of the owner. Please note that under no circumstances will K-12 students' photos or work be identified with first and last names on ASE, school or teacher websites.

- Do not sell or buy anything over the Internet.
- Do not transmit or access obscene or pornographic material; notify your teacher if you receive such material.
- Do not subscribe to list services, bulletin boards, or on-line services shall be reviewed by a ASE administrator and must be approved by the teacher prior to any such usage.
- Do not access the network or Internet by any means or device other than those approved by the teacher.
- Do not post inappropriate speech on any blogs, podcasts, Google Applications, or other web 2.0 tools. Such tools are considered an extension of your classroom, and any speech that is considered inappropriate in the classroom is also inappropriate in all uses of these Web tools
 - This includes, but is not limited to, profanity and racist, sexist or other discriminatory remarks.
 - Comments made on blogs will be monitored and, if they are inappropriate, deleted. Any student violating this rule will be subject to disciplinary action.
- Do not use the network or Internet for any illegal activity, including:
 - tampering with computer hardware, software or data.
 - unauthorised entry into computers and files (hacking/cracking),
 - knowledgeable vandalism or destruction of equipment,
 - deletion of computer files.
- Do not use the network or Internet to send messages relating to or in any way supporting illegal activities; make threats, intimidation or harassment of any other person.
- Do not attempt to log on as a system administrator. This action will result in cancellation of privileges.
- Do not use anonymous proxies to circumvent ASE-implemented content filtering.
- Do not knowingly or inadvertently load or create a computer virus or load any software that destroys files and programs, confuses users, or disrupts the performance of the system.
-
- Do not install third-party software without the consent of your assigned administrator.
- Do not share your passwords or use another person's accounts or passwords.
- Technology protection measures may be disabled by an authorised person.
- Do not participate in hacking/cracking activities or any form of unauthorised access to other computers, networks, or information systems. If an Internet/network security issue is identified, the user must notify an adult, such as a teacher, who will in turn notify a system administrator.

ASE Responsibilities:

- Will provide developmentally appropriate guidance to students as they make use of telecommunications and electronic information resources to conduct research and other studies related to the ASE's curriculum.
- All students will be informed of their rights and responsibilities as users of the ASE's network prior to gaining access to that network, either as an individual user or as a member of a class or group.
- Use of networked resources will be in support of educational goals.
- Treat student infractions of this AUP according to the CPS Code of Conduct.
- Provide alternate activities for students who do not have network and Internet privileges.