BYOD and Cyber Safety Policy
2025-2026

Contents

The purpose of this BYOD and Cyber Safety policy is to ensure that all students use technology at school, home and elsewhere effectively, safely and responsibly.

School's responsibilities

The school is responsible for:

- Providing technological hardware/ software/ network access to promote teaching and learning within the school community.
- Maintaining the integrity, operation, and availability of its electronic systems for access and use.
- Providing a safe cyber environment for all users through firewalls and MDMs.
- The school does not guarantee user privacy or system reliability.

User Rights & Responsibilities:

It is expected that all users of the network digital resources will:

- Obey the laws and restrictions of the United Arab Emirates.
- Respect other users in the school community, which includes the strict prohibition of cyberbullying and harassment.
- Always use your own login account and password and not through any other individual's.
- Handle devices with care and be responsible for any loss or damage to individual devices
- Report on any problems with the equipment to the IT department.

Users are not expected to:

- Store commercial software, music, games or any hidden files and folders on their devices.
- Store parents' files and folders on their devices.
- Play games in school.
- Download unlicensed software.
- Repair, reconfigure, modify or attach any external devices to existing hardware without the permission of the IT department.
- Infringement or violation of U.A.E or international copyright laws or restrictions will not be tolerated.

Cyber-Bullying:

DEFINITION OF CYBER-BULLYING

Cyber-bullying is an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend himself/herself. By cyber-bullying, we mean bullying by electronic media:

• Bullying by texts or messages or calls on mobile phones

- The use of mobile phone cameras to cause distress, fear or humiliation
- Posting threatening, abusive, defamatory or humiliating material on websites, to include blogs, personal websites, social networking sites
- Using e-mail to message others
- Hijacking/cloning e-mail accounts
- Making threatening, abusive, and defamatory or humiliating remarks in chat rooms, to include Facebook, YouTube, WhatsApp, all social networking sites.

LEGAL ISSUES

Cyber-bullying is generally criminal in character. The law applies to cyberspace.

• It is unlawful to disseminate defamatory information in any media including internet sites.

• Section 127 of the Communications Act 2003 makes it an offence to send, by public means of a public electronic communications network, a message or other matter that is grossly offensive or one of an indecent, obscene or menacing character

Students will be held accountable for Cyber-Bullying, even if it occurs off-campus during the school year and negatively impacts the academic environment of the school. AL Maaref American School has a zero tolerance for Bullying, including Cyber-Bullying.

GUIDANCE FOR STAFF

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

• Ask the student to show you the mobile phone

• Note clearly everything on the screen relating to an inappropriate text message or image, including the date, time and names.

• Make a transcript of a spoken message, again record date, times and names.

• Tell the student to save the message/image.

• Go with the students and see the Supervisor / Head of Section, or in their absence, a member of the Senior Leadership Team Computers.

• Ask the student to get up on-screen the material in question.

• Ask the student to save the material.

• Print off the offending material straight away.

• Make sure you have got all pages in the right order and that there are no omissions

• Accompany the student, taking the offending material, to see the Supervisor.

• Normal procedures to interview students and to make statements will then be followed, particularly if a child protection issue is presented.

GUIDANCE FOR STUDENTS

If you believe you or someone else is the victim of cyber-bullying, you must speak to an adult as soon as possible. This person could be a parent/guardian, your tutor, your supervisor or the head of section.

• Do not answer abusive messages but log and report them.

• Do not delete anything until it has been shown to your Form Teacher, your supervisor, parents/guardian or the head of section (even if it is upsetting, the material is important evidence which may need to be used later as proof of cyberbullying).

• Do not give out personal IT details.

• Never reply to abusive e-mails.

• Never reply to someone you do not know.

• Stay in public areas in chat rooms.

GUIDANCE FOR PARENTS

It is vital that parents and the schoolwork together to ensure that all students are aware of the serious consequences of getting involved in anything that might be seen to be cyber-bullying.

• Parents can help by making sure their child understands the school's policy and, above all, how seriously the school takes incidents of cyber-bullying.

• Parents should also explain to their sons or daughters' legal issues relating to cyberbullying.

• If parents believe their child is the victim of cyber-bullying, they should save the offending

material (if need be by saving an offensive text on their or their child's mobile phone) and make sure they have all relevant information before deleting anything.

• Parents should contact the Head as soon as possible. A meeting can then be arranged with the principal, which may involve other relevant members of staff.

• If the incident falls in the holidays, the school reserves the right to take action against bullying perpetrated outside the school which spills over into the school.

Lost, Stolen, or Damaged Devices

Each user is responsible for his/her own device and should use it responsibly and appropriately. **MAS** takes no responsibility for stolen, lost, or damaged devices, including lost or corrupted data on those devices.

While school employees will help students identify how to keep personal devices secure, students will have the final responsibility for securing their personal devices.

MAS Administration