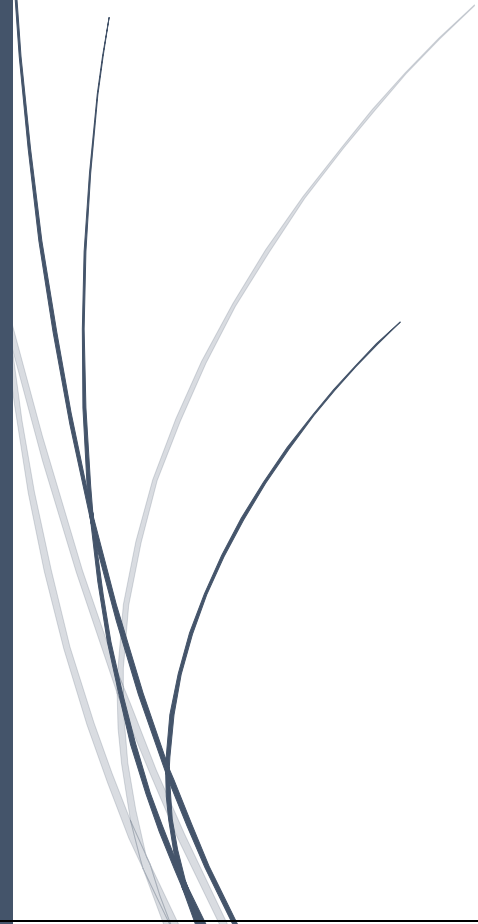September 2021

E-Safety and Distance Learning Policies & Procedures - Teachers

Al Murooj Scientific Private School

Next Review - September 2022

1. **Overview –**

The IT Department's intention for publishing Policies and Procedures is to provide clear guidelines and expectations aligned with an established mission of providing users with the best resources possible to educate every student.

The IT Department is committed to Al Murooj Scientific Private School (AMS) users from illegitimate or harmful actions by individuals, either knowingly or unknowingly. Network related systems, including but not limited to computer equipment, software, operating systems, storage media, mobile devices, network accounts providing electronic mail and or resources, web browsing, and FTP, are the property of AMS. These systems are to be used for educational and school business-related purposes with the intent of serving the interests of the students, teachers, and other staff members of AMS.

It is the responsibility of every computer user to know these guidelines, and to govern themselves accordingly.

2. **Aim –**

Our aim is to educate our school community about the potential dangers of utilizing technology and how to stay safe online. Students and staff should not be afraid of cyberbullying from anyone, known or unknown, and they should be able to spot it. They should be able to handle it properly and evolve into responsible citizens as an outcome.

3. **Scope –**

This policy applies to students, employees, consultants, temporary employees, authorized guests, and other workers at AMS, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by AMS including all future purchases.

4. **Teaching and Learning – Why Internet use is important?**

- The internet is an essential component for education, business and social interaction. The school is responsible to provide pupils with good quality internet access as part of their learning experience.

- The use of the internet is a prerequisite of the UK curriculum and a crucial learning tool for both teachers and students.
- The motivation behind Internet use in school is to build learning standards, to elevate student's accomplishment, to support teacher's area of expertise, and to upgrade the school's administration capacities.
- Access to the internet can act as a catalyst who demonstrate responsible and mature use of the internet. Internet use will improve learning. The school's internet access is designed for student use and includes standardised filtering which is appropriate to student's age.

5. **School Responsibilities**
- Students will be trained what Internet use is acceptable and what is not given clear objectives for internet use.
- Students will be educated in the effectual practise of the internet in research, including the competences of knowledge location, retrieval and evaluation.
- The school will certify that the use of Internet derived materials by teaching and non-teaching staff and students. act in accordance with copyright law.
- Students should be instructed to be significantly aware of the resources they read and shown and understand the methods to validate information before accepting its accuracy.
- Staff should direct students to online activities that will encourage the learning outcomes planned according to the age and ability of the individual.
- Students will be trained to acknowledge the source of information used and to respect copyright when using Internet in their own work.

6. **Managing Internet Access**
- The security of the school information systems and users will be revised regularly.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of the students.
- Files uploaded on the school's network will be reviewed on a regular basis.

- Unauthorised software will not be allowed in work areas or attached to email.

7. E-mail

- E-mail is the fundamental means of communication for both students and staff.
- Students must only use approved e-mail accounts on the school system for education purposes only.
- Students must immediately report to the teacher if they receive any type of offensive e-mail.
- Students must not reveal any personal details in e-mail communication or arrange to meet anyone without specific permission.
- School staff will only use official email accounts provided by the school to communicate among the staff, students and parents, as approved by the Senior Leadership Team (SLT).
- Access to external personal e-mail accounts in school may be blocked.

8. Acceptable use of school's internet, systems and technology for teachers –

School Systems –

- School devices are intended for educational use and not for personal matters.
- Do not change any device settings without permission from IT admin.
- Do not share your username and password with anyone and ensure that you change it at regular intervals
- Do not use the system if the previous user has not logged out. Either log out and use your credentials, or approach the IT admin for support.
- Do not save personal files or data on school systems.
- Do not download or install any program, software or hardware without permission.
- Lock the device once you are done working with it.

Internet and Technology –

- School network must for used for school matters only and not for personal interest.

- All staff members are accountable to report any unauthorized use of the school system or network.
- Social networking sites are forbidden to use.
- Use the email id provided by school to communicate about school related matters with students/parents/outside community.
- Ensure no one has access to your school account.
- Do not send, upload, download, or distribute offensive, threatening, obscene or religious materials.
- Do not save your personal username, passwords, bank details, contact information etc. over school network.
- Respect materials that have copyrights and think wisely before downloading or forwarding any such data.
- Advise and spread awareness among students and colleagues on how to be safe online.
- Share best practices involving ICT skills.
- Do not share school internet credentials with any visitor/outsider.
- Be responsible and ethical while communicating online.
- If you notice any unusual activity that seems suspicious, then report to the IT coordinator immediately.
- Scan your flash drives or any external devices on a regular basis.

Using MS Teams –

- Do not create any groups in MS Teams. If you need a group within MS Teams, contact IT admin for creating a new group.
- All the online sessions will be recorded and download the video.
- All the downloaded videos should be handed over to your respective Subject HOD's every week.
- Do not log out from class ID's from the class room.
- Create a back up for every material you upload in MS Teams for security purposes.
- Turn off the computers after the last period. Teachers who teach last periods are responsible to turn off the computers.

9. Teacher Guidelines for Distance Learning

- Teachers must not have one to one session with any student, a third-party Inclusion team member must be present when having a MS Teams(Principal, Vice principal, Head section). Teachers can record academic sessions only.

- During counselling or intervention sessions, according to child protection policy, a team member and one of the parents must be present during live sessions or interventions for the protection of the child and of the teacher or counsellor. Where the matter is of a child protection nature and it would be detrimental for the parent to be present, there must be two staff members.

- Students should turn on the cameras for the safety purposes of both teachers and students during the class live sessions (if capable).

- Record the class live sessions to safeguard the actions and words spoken during the distance learning for the protection of both students and teacher.

- When the child discloses any child protection issue or safeguarding concern, the teacher will write the exact words used (no paraphrasing) you may not record this. If possible, take the statement in the presence of a third party who may be a teacher or staff for safety and security purpose.

- Report the incident directly to Section Head.

Handling Confidential Data

Every employee of the organization is obliged to protect any confidential data. Some examples of confidential Data:

- Student Information
- Student Marks
- Question Papers
- Personal Details such (Passwords, PIN etc)

Consequences of Violation of Acceptable ICT Use Policy – Accountability Statement

The school reserves the right to take action depending on the severity of violation committed which may include warning, suspension, or expulsion but may not be limited to these and may also be involved with reporting the matter with higher authorities.

Terms and Conditions Agreement

To access the network through the school's computers/network, employees must sign and return this agreement on an annual basis to the school administration. The signed agreement will be archived in school's system as well as manual file.

Use of the network/internet is a privilege, not a right. The school's network/internet connection is provided for professional and educational purposes only. Personal files need to be saved on your own personal storage devices. DO NOT save any personal files on computers belonging to the school. Unauthorised or inappropriate use will result in cancellation of this privilege.

The staff member agrees to abide by ADEK and School Board Regulations.

As a staff member of Al Murooj Scientific Private School, understand that any misuse of equipment that results in the lost, damage or vandalism is to be paid for through the staff members expense.

I, hereby acknowledge that I have read and accept the terms and conditions mentioned in this document and also accept that I understand the significance of the terms and conditions of this policy. I understand that a disciplinary action will be taken by the administration if I violate these guidelines established by Al Murooj Scientific Private School.

Please complete the following information:

Staff Member's Full Name: _____

Staff Member's Signature: _____

Date: _____