The School Acceptable Use Policy

Updated on January 2021

Reviewed and approved by:

OSG TEAM

AL AMEER ENGLISH SCHOOL, AJMAN

ACCEPTABLE USE POLICY

USER GUIDELINES

(With Expectations)

I.   TEACHERS

are responsible for ensuring that:

1. they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.

2. they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP).

3. they report any suspected misuse or problem to the Supervisor / Principal /Vice Principal/ Academic Co-Ordinator/ Curriculum Head; E-Safety Coordinator / Officer for investigation / action / sanction.

4. all digital communications with students / pupils / parents / guardians should be on a professional level and only carried out using official school systems.

5. e-safety issues are embedded in all aspects of the curriculum and other activities.

6. students / pupils understand and follow the e-safety and acceptable use policies.

7. students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

8. they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.

9. in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

10. Of the safe keeping of personal data, minimizing the risk of its loss or misuse.

11. Transfer data using encryption and secure password protected devices.

12. Use sensible email addresses and username. Use privacy settings and strong passwords.

13. Don't put anything online you wouldn't want your colleagues, family and friends to see.

14. Carefully consider if you want to connect with students or parents on social media.

15. Teachers should create an awareness on good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

16. Teachers have to select a digital ambassadors and techno Savvy, have to maintain a logbook of incidents during e-learning classes.

II.   STUDENTS / PUPILS:

are responsible-

1. for using the school digital technology systems in accordance with the Student / Pupil Acceptable Use Policy.
2. have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
3. need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
4. will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
5. should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's   E-Safety Policy covers their actions out of school, if related to their membership of the school.
6. Students may not post personal information such as their home address, telephone number or the name and location of their school without teacher's permission.
7. Students are prohibited from making prejudicial, harassing, threatening, obscene or hateful remarks and other anti-social behaviour.
8. Students are prohibited from using the Internet to access or process inappropriate text files, information that advocates illegal acts, or information that lacks any educational value.
9. Students should immediately tell a teacher or other school employee about any material that you feel is not appropriate or that makes you feel uncomfortable.

10. Students should be aware that no communications are guaranteed to be private. School portal use is monitored. Illegal activities may be reported to the authorities.
11. Students should note that plagiarism is the taking of material created by others and presenting it as if it were one's own. It will not be acceptable to plagiarize material from the Internet or from the portal.
12. Students should note that all communications and information accessible via the school portal should be assumed to be private property.
13. Students may not use the google classrooms or school portal for commercial purposes or product advertisement. Products or services may not be purchased or offered. The student and his/her parents will be responsible for any liabilities stemming from such unauthorized uses of the portal.
14. Student username and passwords are confidential. All passwords shall be protected by the user and not shared or displayed. Individual users shall, at all times, be responsible for the proper use of accounts issued in their name.
15. Students may not send broadcast email or broadcast voicemail without prior permission from the Teacher.
16. Students are expected to check their email on a frequent and consistent basis in order to stay current with school related communications.
17. Students who violate school policy or administrative procedures will be subject to suspension or termination of system/network privileges and will be subject to appropriate disciplinary action and/or prosecution.
18. Students should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from Sharing of personal data, access to illegal / inappropriate materials inappropriate on-line contact with adults, strangers, potential or actual incidents of grooming, Cyberbullying.

III. PARENTS / GUARDIANS

Parents / Guardians play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. Parents and guardians will be encouraged to support the school in promoting good e-safety practice and to follow guidelines:

1. on the appropriate use of digital and video images taken at school events.

2. Usage of access to parents' sections of the website / VLE and on-line student / pupil records.

3. Place the computer or laptop in a common area in your home within your supervision. This will allow you to indirectly monitor your child.

4. Frequently check the information being exchanged between your child their peers and the school on the third entity.

5. If you witness any inappropriate activity on an online platform, report immediately.

6. Install parental control software to block inappropriate content and websites that are not required for distance learning.

7. Follow the virtual timetables for your child.

8. Maintain regular family routines including bed time.

9. Student username and passwords are confidential. All passwords shall be protected by the user and not shared or displayed. Individual users shall, at all times, be responsible for the proper use of accounts issued in their name.

10. Parents may not send broadcast email or broadcast voicemail without prior permission from the Teacher.

11. Parents are expected to check their child's email on a frequent and consistent basis in order to stay current with school related communications.

12. Parents must be aware that if the child violates school policy or administrative procedures will be subject to suspension or termination of system/network privileges and will be subject to appropriate disciplinary action and/or prosecution.

13. Parents should monitor e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from Sharing of personal data, access to illegal / inappropriate materials inappropriate online

contact with adults, strangers, potential or actual incidents of grooming, cyber-bullying.
14. Parents should be free to contact and acknowledge the issues faced by their ward if any during e-learning to the teacher concerned.