Online e-Safety Policy

Policy Name	Online e-safety policy
Date	12-04-2021
Last reviewed on	12-04-2021
Next review due by	January 2022

Introduction:

- The policy is updated and reviewed by the School IT-Supervisor who will report to the SMT of Al Ansar International School.
- The Policy will be subjected to review annually by the SMT in the event of any major changes in circumstances, to ensure those controls remain effective.

Scope

Al Ansar International School, Sharjah recognizes that the Internet, and access to it via a range of technologies, is an attractive and increasingly integral feature of children's learning and it is the duty of the school management to ensure that every child in their care is safe in every possible way, and that the same safeguarding principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect the Al Ansar community - the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks. The E-Safety Policy relates to other policies including those for safeguarding, ICT, Distance-Learning, bullying and child protection.

Research has proven that use of technology carries enormous benefits to learning and teaching. However, as with many technological developments, there is an element of risk here. While it is unrealistic to eliminate all risks associated with technology, the implementation of an effective E-Safety Policy will help children develop the skills and confidence to manage potential risks and considerably reduce their impact.

Al Ansar E-safety Policy, as part of the wider safeguarding agenda, outlines how we ensure safety of our students and that they are prepared to deal with the safety challenges that the use of technology brings.

Aims and Objectives

E-safety is an integral part of safeguarding the Al Ansar Community. This policy is written in line with 'Keeping Children Safe in Education'.

The school recognizes too that in enabling access to this invaluable resource it has a duty to ensure students are:

- safe from inappropriate content in a range of forms and across technologies
- safe from bullying and harassment of any kind
- safe from crime and anti-social behaviour in and out of school
- secure, stable and careful while online

Help the Al Ansar community working with students to understand their roles and responsibilities to work safely and responsibly with technology and the online world:

- for the protection and benefit of the children and young people in their care.
- for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice.
- for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession.

How will this policy be communicated?

- Posted on School Website
- Sent to parents and students via Al Ansar Smart App
- Available on the internal staff network/drive
- Available in paper format in the staffroom

Legislation and guidance

This policy is based on the MOE statutory safeguarding guidance, Keeping Children Safe in Education, and advice for schools on:

- Teaching online e-safety in school.
- Preventing and tackling bullying and cyber-bullying: advice for Educational Supervisor and school staff.

Key people

Designated Online e-safety Officer	Mr. Mustafa Junaid (IT Administrator)
The designated Child protection Officer	
Designated Safeguarding Lead (DSL) team	Principal, Vice Principals and the Quality Office. Administrative Section Supervisors IT-Supervisor & the IT-Support Team Educational Supervisor – Computers Computer Science & ICT-Teachers
Online Safety Group	Principal, Vice Principals and the Quality Office. Administrative Section Supervisors & their assistant. IT-Supervisor & the IT-Support Team Educational Supervisor – Computers Computer Science & ICT-Teachers Student representative from each section / grade. (E-Monitor)

Roles and responsibilities

Principal, Vice Principals and Quality and Development Officer. (SMT)

The **Principal, Vice Principals and Quality and Development Officer** is responsible for ensuring that the Al Ansar community understand this Online e-safety policy, and that it is being implemented consistently throughout the school.

The Administrative Section Supervisors

The Administrative Section Supervisors take lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with School SMT (Principal, Vice Principals and the Quality Office), IT-Supervisor / IT-Support-Team and other Al Ansar community members, as necessary, to address any online safety issues or incidents.
- Ensuring that any online safety incidents are documented and dealt with appropriately in line with this policy
- Ensuring that any incidents of online safety incidents and cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.

The IT Department

The IT-Supervisor along with the IT-Support-Team is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis to keep students safe from potentially harmful and/or inappropriate content and contact online while at school.
- Ensuring that the school's IT-infrastructure systems (School Network, School Servers, Data, etc.) are all secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's IT-infrastructure systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Updating and conducting staff training for online safety

Educational Supervisors - Computers

- Maintaining and understanding of this Online e-safety policy.
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's IT-infrastructure systems and the internet and ensuring that Students follow the school's terms on acceptable use
- Working with the Administrative Section Supervisors to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

Computer Science & ICT Teachers

- Maintaining and understanding of this Online e-safety policy.
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's IT-infrastructure systems and the internet and ensuring that Students follow the school's terms on acceptable use
- Working with the Educational & Administrative Section Supervisors to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy

All staff – Al Ansar community

Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never assume that someone else will pick it up

✔ **All staff are responsible for:**

- Maintaining and understanding of this Online e-safety policy.
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's IT-infrastructure systems and the internet and ensuring that Students follow the school's terms on acceptable use
- Working with the Administrative Section Supervisors to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

✔ **Parents are expected to:**

- Notify the School Administrative Section Supervisors of any concerns or queries regarding this policy.
- Parents can seek further guidance on keeping children safe online from the non-educational websites.

4. Teaching and learning

Internet and digital communication play a key role in our remote learning and is a part of the statutory curriculum and a necessary tool for staff and students. The school provides the complete Al Ansar community with quality Internet access as part of their learning experience.

IT infrastructure systems & ICT tools will be used across the school to enhance and extend learning, to engage in interesting and vibrant learning activities and to empower learners so that they play a more active role in managing their own learning experiences.

Internet use will enhance learning

- The school's internet access will be designed expressly for student use.
- Access to the internet is enabled through the Firewall and where appropriate, the school will request changes to this filter.
- Students will be educated in the effective use of the internet which will have particular emphasis on what information they can and cannot share.
- When accessing remote learning (see remote learning policy), via online learning platforms, students will have access to their Goole Classrooms where resources are clear and easily accessible for students and parents.
- Teachers can upload a range of resources for learning at home including links to websites, pre-recorded lessons, interactive worksheets, visuals and printable materials.

Students will be taught how to evaluate Internet content

The school will ensure that the use of internet derived materials by staff and students complies with copyright law. Students will be taught the importance of cross-checking information before accepting its accuracy.

Educating Students about online safety

Students will be educated about online e-safety as part of the curriculum:

Students will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the
- internet or other online technologies
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- The safe use of social media and the internet will also be covered in relevant subjects.

Educating parents about online safety

- The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website and our online learning platform, Firefly.
- This Online e-Safety Policy will also be shared with parents.
- If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Section Administrative Supervisor.

Acceptable use of the internet in school

- All staff are expected to sign an agreement regarding the acceptable use of the school IT infrastructure systems and the internet.
- Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.
- Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.
- We will monitor the websites visited by the Al Ansar community - Students, staff, and visitors (where relevant) to ensure they comply with the above.

Managing Information Systems

Information system security

- School IT-infrastructure systems security will be reviewed regularly.
- Sophos Antivirus and Malwarebytes Antispam software updates will be ongoing.
- Security strategies will be discussed with the School SMT (Principal, Vice Principals and the Quality Office)

E-mail

- Students may only use the official school E-mail accounts on the school system.
- The school will consider how e-mail from Students to external bodies is presented and controlled.

Published Content and the School Website

- The contact details given on the website will be the school address, e-mail and telephone number.
- Staff or Student personal contact information will not be published.
- The IT Department Supervisor will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Student's Images and Work

- Written permission will be sought from parent/carers before photographs of Students are published on the school web site.
- Students' full names will not be used anywhere on a school website or other on-line space, particularly in association with photographs.
- Work can only be published with the permission of the Student and/or guardians.
- Student image file names will not refer to the student by name.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic platforms.

Social Networking and Personal Publishing

- Social Network sites and newsgroups will be filtered unless a specific use is approved.
- Students will be advised never to give out personal details of any kind which may identify them, their friends or
- their location.
- Students and parents will be advised that the use of social network spaces outside school brings a range of
- dangers for children and young people.
- Parents will be invited to attend e-safety workshops aimed at raising their awareness of how to manage online content at home.

Settings

Managing Filtering

- The school will work with appropriate agencies and partners to ensure systems to protect Students are reviewed and improved.
- If staff or Students come across unsuitable on-line materials, the site must be reported to the school SMT/ Section Administrative Supervisor, IT-Supervisor / IT-Support-Team.
- SMT will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The SMT (Principal, Vice Principals and the Quality Office) have noted that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones are not permitted to be used in school unless agreed with the SMT (Principal, Vice Principals and the Quality Office).
- The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- The use by Students of cameras in mobile phones will be kept under review.
- The use of webcams can only be used with the permission of the headteacher or other senior management.
- Games machines including the Sony Play station, Microsoft Xbox and others potentially have Internet
- access.
- At school, these devices will only be available ‘offline’.
- Administrative Section Supervisor will supervise Students who access such devices.

Protecting Personal Data

- The IT Team will be responsible for protecting & misuse of the Al Ansar community Personal data & information.

Remote Communications

- We allow staff to access the school’s Network & their data remotely.
- Staff accessing the school’s IT-infrastructure systems facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site.
- Staff must be particularly vigilant if they use the school’s IT-infrastructure systems facilities outside the school and take such precautions as the IT-Department may require from time to time against importing viruses or compromising system security.
- Our IT-infrastructure systems facilities contain information which is confidential and / or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

Remote Meetings and Training

- When it is necessary for parent, staff and professional meetings (such as annual reviews) or trainings to be held remotely, these must be conducted through Google Meet in line with our safeguarding policy.
- The IT-Department will manage the setup of accounts for relevant staff to host meetings through this channel.
- Al Ansar Int. School, recommends that staff set up an appropriate space for working remotely and ensure:
    - Appropriate dress code
    - Appropriate background
    - SMT are made aware of scheduled meetings / trainings
    - Meetings and trainings are scheduled in appropriate rooms, not accessed by students

Remote Online Learning

- Students can access remote learning through Google Meet / Google Classroom and other online learning platform.
- Teachers and relevant staff have received relevant training in this programme.
- Google Classroom is a secure channel through which a range of resources for learning at home can be uploaded including links to websites, pre-recorded lessons, interactive worksheets, visuals and printable materials.
- Staff must ensure that content is appropriate and follows safeguarding and guidelines by:
  - ✓ Using school-approved channels (Google-Classroom & Google meet)
  - ✓ Notifying SMT of 'live' sessions
  - ✓ Ensuring appropriate dress code by staff and students
  - ✓ Ensuring that lessons are taking place in an appropriate space/environment
  - ✓ Content of links and videos are checked before being shared/uploaded
  - ✓ Recordings of lessons are in line with safeguarding and data protection policies

Staff using work devices outside school

- All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:
  - ✓ Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
  - ✓ Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the
  - ✓ files stored on the hard drive by attaching it to a new device
  - ✓ Making sure the device locks if left inactive for a period of time
  - ✓ Not sharing the device among family or friends
  - ✓ Installing anti-virus and anti-spyware software
  - ✓ Keeping operating systems up to date – always install latest updates
  - ✓ Staff members must not use the device in any way which would violate the school's terms of acceptable use.
  - ✓ Work devices must be used solely for work activities.
  - ✓ If staff have any concerns over the security of their device, they must seek advice from SMT (Principal, Vice Principals and the Quality Office)

How the school will respond to issues of misuse

- Where a staff member misuses the school's ICT / IT-infrastructure systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct.
- The disciplinary action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
- The school Senior Management Team will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

- All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues.
- All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, memos and staff meetings).
- The Section Administrative Supervisor, will undertake child protection and safeguarding training, which will include online safety, at least once every 2 years.
- They will also annually update their knowledge and skills on the subject of online safety at regular intervals.
- More information about safeguarding training is set out in our child protection and safeguarding policy.

Monitoring arrangements

- The Administrative Section Supervisor logs behaviour and safeguarding issues related to online safety.
- This policy will be reviewed every year by the SMT (Principal, Vice Principals and the Quality Office).
- At every review, the policy will be shared with the Al Ansar community.

Links with other policies

This online safety policy is linked to our:

- BYOD policy
- Distance Learning Policy
- Child protection policy
- Child welfare policy
- Al Ansar Occupational Health and Safety Policy
- Digital Wellbeing policy
- Safeguarding policy
- Behaviour policy

Acceptable Use of Technology - Agreement

Policy Name:	Acceptable Use of Technology - Agreement
Date:	12-04-2021
Last reviewed on:	12-04-2021
Next review due by:	January 2022

Appendix 1: Acceptable Use Agreement (Al Ansar Staff-members)

Write your Name in Full	
Department / Section	
Year / Grade – Section *(Only if required – for example: 5/4B – where 5 is the Year and 4B is the Grade & section)*	

When using the school's IT-infrastructure systems and accessing the internet in school, or from outside school on a work device / task:

Part-1: I WILL NOT:

1.1: Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or immoral nature (or create, share, link to or send such material).

1.2: Use them in any way which could harm the school's reputation.

1.3: Access social networking sites or chat rooms using the school Internet.

1.4: Use any improper language when communicating on the School Internet, including in Emails or other messaging services.

1.5: Install any unauthorised software, or connect unauthorised hardware or devices to the school's network.

1.6: Share my school-related password with others or log in to the school's network using someone else's details.

1.7: Take photographs of Students / Classmates / Colleagues without checking & approval, of the concerned Section Head / Vice Principal / Principal / Quality Office.

1.8: Share confidential information about the school, its students or staff, or other members of the school community.

1.9: Access, modify or share data I am not authorised to access, modify or share.

1.10: Promote private businesses.

Part-2: I WILL:

2.1: I will only use the school's IT-infrastructure systems and access the internet, school domain and school platforms in or outside school on a work device / task, for educational purposes or for the purpose of fulfilling the duties of my role.

2.2: I agree that the school will monitor the websites I visit in school and my use of the school's ICT facilities and systems.

2.3: I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

2.4: I will not share the school-related passwords with anyone else.

2.5: I will let the Administrative Section Supervisor and IT-Support-Team, know if I see any misuse of the school internet services

2.6: I will also inform the Administrative Section Supervisor and IT-Support-Team, if I encounter any such material which might upset, distress, hurt or harm them or others while using the internet in school.

2.7: I will always use the school's IT-infrastructure systems and internet responsibly, and ensure that students in my care do so too.

Signed by Al Ansar Staff-Member:		
	Signature	**Date** (dd/mm/yyyy)

Acceptable Use of Technology - Agreement

Policy Name:	Acceptable Use of Technology - Agreement
Date:	12-04-2021
Last reviewed on:	12-04-2021
Next review due by:	January 2022

Appendix 1: Acceptable Use Agreement (Al Ansar Students / Parents)

Select One	**□ Student □ Parent**
Write your Name in Full	
Year / Grade – Section *(Example: 5/4B – where 5 is the Year and 4B is the Grade & section)*	

When using the school's IT-infrastructure systems and accessing the school domain from within or outside the school, then:

Part-1: I WILL NOT:

1.1: Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or immoral nature (or create, share, link to or send such material).
1.2: Use them in any way which could harm the school's reputation.
1.3: Access social networking sites or chat rooms using the school Internet.
1.4: Use any improper language when communicating on the School Internet, including in Emails or other messaging services.
1.5: Install any unauthorised software, or connect unauthorised hardware or devices to the school's network.
1.6: Share my school-related password with others or log in to the school's network using someone else's details.
1.7: Take photographs of Students / Classmates / Colleagues without checking & approval, of the concerned Section Head / Vice Principal / Principal / Quality Office.
1.8: Share confidential information about the school, its students or staff, or other members of the school community.
1.9: Access, modify or share data I am not authorised to access, modify or share.

Part-2: I WILL:

2.1: I will only use the school's IT-infrastructure systems and access the school domain and school platforms in or outside school for educational purposes or for school tasks.
2.2: I agree that the school will monitor the websites I visit in school and my use of the school's ICT facilities platforms and systems.
2.3: I will take all reasonable steps to ensure that devices are secure and password-protected when using them in school, and keep all data securely stored in accordance with this policy and the school's data protection policy.
2.4: I will not share the school-related passwords with anyone else.
2.5: I will let the Administrative Section Supervisor know if I see any misuse of the school internet services.
2.6: I will also inform the Administrative Section Supervisor, if I encounter any such material which might upset, distress, hurt or harm them or others while using the internet in school.

Signed by Al Ansar Staff-Member / Student / Parent:		
	Signature	**Date** (dd/mm/yyyy)

اتفاقية الاستخدام الآمن للتكنولوجيا والأجهزة الإلكترونية .

اسم السياسة:	اتفاقية الاستخدام الآمن للتكنولوجيا والأجهزة الإلكترونية .
التاريخ :	2021-4-12
تاريخ آخر مراجعة:	2021-4-12
موعد المراجعة:	يناير 2022

الملحق 1: اتفاقية الاستخدام المقبول والآمن (طلاب / أولياء أمور مدرسة الأنصار)

قم بالاختيار:	**ولي أمر ☐ طالب ☐**
الاسم الكامل:	
السنة الدراسية \ الصف -الشعبة:	

عند استخدام أنظمة البنية التحتية لتكنولوجيا المعلومات بالمدرسة والوصول إلى الإنترنت في المدرسة ، أو من خارج المدرسة على جهاز خاص بالمدرسة:

الجزء الأول: لن أفعل التالي :

1.1: الوصول أو محاولة الوصول إلى مواد غير ملائمة ، بما في ذلك على سبيل المثال لا الحصر المواد ذات الطبيعة العنيفة أو الإجرامية أو غير الأخلاقية (أو إنشاء مثل هذه المواد أو مشاركتها أو نسخ رابطها أو إرسالها).

1.2: استخدمها بأي طريقة من شأنها الإضرار بسمعة المدرسة.

1.3: الوصول إلى مواقع التواصل الاجتماعي أو غرف الدردشة باستخدام الإنترنت المدرسي.

1.4: استخدم أي لغة غير لائقة عند الاتصال على الإنترنت بالمدرسة ، بما في ذلك رسائل البريد الإلكتروني أو خدمات المراسلة الأخرى.

1.5: تثبيت أي برنامج غير مصرح به ، أو توصيل أجهزة أو أجهزة غير مصرح بها بشبكة المدرسة.

1.6: مشاركة كلمة المرور الخاصة بي (المخصصة من المدرسة) مع الآخرين أو تسجيل الدخول إلى شبكة المدرسة باستخدام تفاصيل شخص آخر.

1.7: التقاط صورًا للطلاب / زملاء الدراسة / الزملاء والمعلمين دون التحقق وموافقة رئيس القسم المعني / نائب المدير / المدير / مكتب الجودة.

1.8: مشاركة المعلومات السرية حول المدرسة أو الطلاب أو الموظفين أو أعضاء آخرين في مجتمع المدرسة.

1.9: الوصول إلى البيانات غير مصرح لي بالوصول إليها أو تعديلها أو مشاركتها.

الجزء 2: سأفعل التالي :

2.1: أستخدم فقط أنظمة البنية التحتية لتكنولوجيا المعلومات الخاصة بالمدرسة والوصول إلى نطاق المدرسة والأنظمة الأساسية للمدرسة داخل المدرسة أو خارجها للأغراض التعليمية أو للمهام المدرسية.

2.2: أوافق على أن المدرسة ستراقب مواقع الويب التي **سأزورها في المدرسة** وستراقب وتتابع استخدامي لمنصات وأنظمة مرافق تكنولوجيا المعلومات والاتصالات بالمدرسة.

2.3: أتخذ جميع الخطوات المعقولة للتأكد من أن الأجهزة آمنة ومحمية بكلمة مرور عند استخدامها في المدرسة ، والاحتفاظ بجميع البيانات مخزنة بشكل آمن وفقًا لهذه السياسة وسياسة حماية بيانات المدرسة.

2.4: لن أشارك كلمات المرور المتعلقة بالمدرسة مع أي شخص آخر.

2.5: أخبر مشرف القسم الإداري إذا رأيت أي سوء استخدام لخدمات الإنترنت بالمدرسة.

2.6: أبلغ أيضًا مشرف القسم الإداري ، إذا واجهت أيًا من هذه المواد التي قد تزعجني أو تزعج زملائي أو تؤذيهم أو تضر بالآخرين أثناء استخدامنا الإنترنت في المدرسة.

توقيع الطالب\ ولي الأمر:	**التوقيع:**	**التاريخ (اليوم \ الشهر\ االسنة):**