

E-Safety Policy

Effective	31 August 2026
Author	Linda Elder
Reviewer	Tyler Lawrance
Approver	Karen McCord, Executive Principal
Due for review	31 August 2027
Version number	2.0

Board Approval: _____

Date: ____ / ____ / ____

Australian International School Dubai (AISD) will monitor the impact of the policy using:

- Logs of reported incidents
- Surveys of reported incidents:
 - Students
 - Parents/Caregivers
 - Staff

Scope of the Policy

This policy applies to all members of AISD (including staff, students, volunteers, parents/carers, visitors and community users) who have access to and are users of school ICT systems, both in and out of our school.

AIS Dubai will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/caregivers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within AISD:

Executive Principal

The Executive Principal is responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by receiving regular information about e-safety incidents and monitoring reports. The Executive Principal has appointed an E-Safety Coordinator, who will:

- Regularly monitor the e-safety incident logs
- Regularly monitor the filtering/change control logs
- Report to relevant Executive Principal meetings

Executive Principal and Senior Leaders:

- Have a duty of care for ensuring the safety (including e-safety) of members of our school community.

- Is aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- Are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- Will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support those colleagues who take on important monitoring roles.

E-Safety Coordinator:

- Leads the e-safety committee
- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing AISD e-safety policies/documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Provides training and advice for staff
- Liaises with the KHDA/relevant body
- Liaises with school technical staff (IT Department)
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments as outlined in our Incident Report Policy
- Meets with the Executive Principal to discuss current issues, review incident logs and filtering/change control logs
- Attends relevant meetings
- Reports regularly to Senior Leadership Team

IT Manager/Technical staff:

The IT Manager is responsible for ensuring that:

- AISD's technical infrastructure is secure and is not open to misuse or malicious attack

- AISD meets required e-safety technical requirements and any KHDA/other relevant body E-Safety Policy/Guidance that may apply.
- Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- The filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- They keep up to date with e-safety technical information in order to effectively carry out their e- safety role and to inform and update others as relevant
- The use of the network/internet/Google workspace/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the appropriate person.

Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring they:

- Have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- Have read and understood the [Information Communication Technology Policy \(Staff\)](#) and have signed the online Internet Access & Acceptable Use Agreement for Staff (presented as part of the new staff induction program)
- Report any suspected misuse or problem as per AISD's Responsible Behaviour Plan for Students (regarding students) *currently being updated* and [Professional Code of Conduct Policy](#) (regarding employees) for investigation/action/sanction.
- All digital communications with students/parents/carers will be on a professional level and only carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other activities
- Students understand and follow the e-safety and acceptable use policies
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- 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
- In lessons where internet use is pre-planned, pupils will 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.

Child Protection/Safeguarding Designated Safeguarding Lead (e.g. Wellbeing Team)

Will 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
- Cyber-bullying

Students:

- Are responsible for using AISD digital technology systems in accordance with the Student [Internet Access and Mobile Phone Acceptable Use Agreement \(Parents and Students\)](#)
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They will also know and understand policies on the taking/use of images and on cyber-bullying.
- Will understand the importance of adopting good e-safety practice when using digital technologies out of school, and realise that AISD's E-Safety Policy covers their actions out of school.

Parents/Caregivers:

Parents/Caregivers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. AISD will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, parent learning lounge, website and information about national/local e-safety campaigns/literature.

Parents and caregivers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

Education: Students

Whilst regulation and technical solutions are very important, their use should be balanced by educating students to take a responsible approach. The education of students in E-safety is therefore an essential part of our school's e-safety provision. Children and young people need the help and support of our school to recognise and avoid e-safety risks and build their resilience.

E-safety will be a focus in all areas of the curriculum and staff will reinforce e-safety messages across the curriculum. The e-safety curriculum will be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum is provided as part of our lessons, and will be regularly revisited
- Key e-safety messages will be reinforced as part of a planned program of wellbeing assemblies and the Moral Education/Australian curriculum.
- Students will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students will be helped to understand [Internet Access and Mobile Phone Acceptable Use Agreement \(Parents and Students\)](#) and encouraged to adopt safe and responsible use both within and outside school

- Staff will act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils will 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
- Where students are allowed to freely search the internet, staff will be vigilant in monitoring the content of websites the young people visit
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT Department (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, will be auditable, with clear reasons for the need

Education: Parents/Caregivers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

AISD will provide information and awareness to parents and caregivers through:

- Curriculum activities
- Letters, newsletters, AISD website
- Parents/Caregivers evenings/sessions
- High profile events/campaigns e.g. Cyber Safety week.
- Reference to the relevant websites/publications

Education: The Wider Community

AISD will provide opportunities for local community groups/members of the community to gain from our school's e-safety knowledge and experience. This may be offered through the

following:

- Providing family learning courses in use of new digital technologies, digital literacy and e-safety
- E-Safety messages targeted towards grandparents and other relatives as well as parents
- AISD website and social media platforms will provide e-safety information for the wider community
- Supporting community groups to enhance their e-safety provision

Education & Training: Support Staff/Non Teaching Staff/Volunteers/Visitors

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A program of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the Annual Performance Review (APR) process
- All new teaching staff will receive e-safety training as part of their induction program, ensuring that they fully understand the [Information Communication Technology Policy \(Staff\)](#) and have signed the online Internet Access & Acceptable Use Agreement for Staff.
- The E-Safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events, and by reviewing guidance documents released by relevant organisations
- This E-Safety policy and its updates will be presented to and discussed by staff in appropriate forums.
- The E-Safety Coordinator (or other nominated person) will provide advice/guidance/training to individuals as required

Education: Executive Principal

The Executive Principal will take part in e-safety training/awareness sessions, with particular importance for those who are members of any subcommittee/group involved in technology/e-safety/health and safety/child protection. This may be offered in a number of ways:

- Attendance at training provided by the KHDA/Executive Principal Network meeting/or other relevant organisation
- Participation in school training/information sessions for staff

IT Department: Infrastructure/Equipment, Filtering and Monitoring

AISD is responsible for ensuring that our school infrastructure/network is as safe and secure as is reasonably possible, and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School technical systems will be managed in ways that ensure that our school/academy meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school academy technical systems.
- Servers, wireless systems and cabling should be securely located and physical access restricted.
- All users will have clearly defined access rights to school/academy technical systems and devices.
- The IT Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users.
- School technical staff regularly monitor and record the activity of users on AISD technical systems, and users are made aware of the online Internet Access & Acceptable Use Agreement for Staff.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. AISD infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto our school systems.
- Personal data cannot be sent over the internet or taken off our school site unless safely encrypted or otherwise secured.

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD will not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and our Bring Your Own Device (BYOD) Policy (*currently being updated*) is in place with references made within all relevant policies.

- AISD has a set of clear expectations and responsibilities for all users
- AISD adheres to the UAE Cybercrime Law ([Federal Law No. 5 of 2012](#))
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by our school's/academy's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Students receive training and guidance on the use of personal devices

- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the Bring Your Own Device (BYOD) Policy, *currently being updated*.
- Any user leaving AISD will follow the process outlined within the Bring Your Own Device (BYOD) Policy, *currently being updated*.
- AISD network administrators will install SSL certificates on BOYD devices to ensure adequate security and protection to devices whilst using our school network

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/caregivers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. AISD I will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff will inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they will recognize the risks attached to publishing their own images on the internet eg on social networking sites
- In accordance with guidelines, parents/caregivers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images will not be published/made publicly available on social networking sites, nor will parents/carers comment on any activities involving other students/pupils in the digital/video images
- Staff and volunteers are allowed to take digital/video images to support educational aims, but should follow school policies concerning the sharing, distribution and publication of those images. Those images will only be taken on

school equipment, the personal equipment of staff will not be used for such purposes

- Care will be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or our school into disrepute
- Students should not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and comply with our best practice guidance on the use of such images and parent media permission
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of students are published on our school website or any other media such as Parent Newsletters
- Students' work can only be published with the permission of the pupil and parents or carers

Data Protection (followed as guidelines)

Personal data will be recorded, processed, transferred and made available according to UAE law which states that personal data should be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

Our school will ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”.
- Responsible persons are appointed/identified (IT Manager)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage/cloud computing which ensure that such data storage meets the KHDA and Education Queensland requirements

Staff should ensure they:

- At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data
- Transfer data using encryption and secure password protected devices

- Do not use personal phones for taking photos of students, unless with specific permission from the Executive Principal.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies, AISD considers the following as good practice:

- AISD official school email service may be regarded as safe and secure and is monitored. Users will be aware that email communications are monitored. Staff and students will therefore use only AISD email service to communicate with others when in school, or on school systems (e.g. by remote access)
- Users should immediately report, to the nominated person (in accordance with AISD policy), the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should not respond to any such communication
- Any digital communication between staff and students or parents/caregivers' (email) should be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media should not be used for these communications
- Whole class/group email addresses may be used in Early Years, while student pupils in Prep to Year 12 will be provided with individual school email addresses for educational use
- Students will be taught about e-safety issues, such as the risks attached to the sharing of personal details. They will also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies
- Personal information will not be posted on AISD website and only official email addresses will be used to identify members of staff

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for

pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render our school or KHDA liable to the injured party. Reasonable steps to prevent predictable harm should be in place.

AISSD provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and our school community through limiting access to personal information:

- Training to include acceptable use, social media risks, checking of settings, data protection, reporting issues
- Clear reporting guidance including: responsibilities, procedures and sanctions, assessment and including legal risk

School staff will ensure that:

- No reference will be made in social media to pupils, parents/caregivers or school staff
- They do not engage in online discussion on personal matters relating to members of our school community
- Personal opinions will not be attributed to AISSD or KHDA
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

Parents will ensure that:

- No reference will be made in social media to pupils, parents/caregivers or school staff
- They do not engage in online discussion on personal matters relating to members of our school community
- Personal opinions will not be attributed to AISSD or KHDA

Our school's use of social media for professional purposes will be checked regularly by the

E-safety Coordinator, e-safety committee and the Marketing Team to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Responding to Incidents of Misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

Illegal Incident

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, this is to be immediately reported to the Executive Principal, and potentially then report immediately to the police.

Other Incidents

It is hoped that all members of our school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure will be followed:

- Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police if the need arises. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff will have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation.

These may be printed, signed and attached to the form (except in the case of images of child sexual abuse (see below).

- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Police involvement and/or action (as relevant)
- If content being reviewed includes images of child abuse then the monitoring will be halted and referred to the police immediately. Other instances to report to the police include:
 - Incidents of 'grooming' behaviour
 - Sending obscene materials to a child
 - Criminally racist material
 - Other criminal conduct, activity or materials

If such an incident occurs, isolate the computer in question as best you can. Any change to its state may hinder a future police investigation.

It is important that all of the above steps are adhered to, to provide an evidence trail for our school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form will be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is expected AISD may face more incidents related to inappropriate behaviour rather than illegal misuse. It's crucial to handle such incidents promptly and in a fair manner. It's also important to inform our school community that these incidents have been resolved.