

E-Safety Policy

2022 - 2023

Next review date: August 2023



This policy has been read and adopted by AAESS Board of Directors and Executive Principal:

Signed:



For and on behalf of AAESS Board of Directors

Date: August 2022

Signed:



Mr Andrew Thomas, Executive Principal

Date: August 2022

Policy Statement

The Board of Trustees are working with staff, pupils and parents / carers to create a school community which values the use of new technologies in enhancing learning, encourages responsible use of ICT, and follows agreed policies to minimise potential e-safety risks.

The Board of Trustees will:

- Discuss, monitor and review the E-safety and related policies on an annual basis.
- Support staff in the use of ICT as an essential tool for enhancing learning and in the embedding of e-safety across the whole curriculum.
- Ensure that students are aware, through e-safety education, of the potential e-safety risks associated with the use of ICT and mobile technologies, that all e-safety concerns will be dealt with sensitively and effectively; that pupils feel able and safe to report incidents; and that pupils abide by the School's E-Safety Policy.
- Provide opportunities for parents/carers to receive e-safety education and information, to enable them to support their children in developing good e-safety behaviour. The School will report back to parents / carers regarding e-safety concerns.
- Seek to learn from e-safety good practice elsewhere and utilise the support of the Trust and relevant organisations when appropriate.

Background / Rationale

New technologies have become integral to the lives of young people in today's society, both within the School and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

The requirement to ensure that young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in the School are bound. An E-safety Policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Principal and Board of Trustees to the Leadership Team and classroom teachers, support staff, volunteers, parents, members of the community and the students themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement. However, the use of these new technologies can put young people at risk within and outside the School. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to / loss of / sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge

- Inappropriate communication / contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video / internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this E-safety Policy is used in conjunction with other School policies, such as anti-bullying and Child Protection policies.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build students' / pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The School must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The E-safety Policy that follows explains how the School intends to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development / Monitoring / Review of this Policy

Scope of the Policy

This Policy applies to all members of the School community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of School ICT systems, both in and out of School.

ADEK & Headteachers, to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the School site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the School.

The School will deal with such incidents within this Policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

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

Board of Trustees:

The Board of Trustees are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Board of Trustees Safeguarding Committee receiving regular information about e-safety incidents and monitoring reports.

Principal and Leadership Team:

- The Principal is responsible for ensuring the safety (including e-safety) of members of the School community, though the day to day responsibility for e-safety will be delegated to the Designated Safeguarding Lead and Assistant Principal i/c ICT.
- The Principal / Assistant Principal i/c ICT / Designated Safeguarding Lead are responsible for ensuring that relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Principal, Deputy Principals, Assistant Principal i/c ICT and Designated Safeguarding Lead should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

Network Manager:

The Network Manager is responsible for ensuring:

- that the School's ICT infrastructure is secure and is not open to misuse or malicious attack;
- that the School meets the e-safety technical requirements outlined in the Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance;
- that users may only access the School's networks through a properly enforced password protection policy, in which passwords are regularly changed;
- the School's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- that he keeps 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;
- that the use of the Network, Virtual Learning Environment (VLE), remote access, email is regularly monitored in order that any misuse or attempted misuse can be reported to the Principal i/c ICT for investigation;
- that monitoring software / systems are implemented and updated as agreed in School policies.

Teaching and Administration Staff:

Teaching and Administration staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current School E-Safety Policy and practices;
- they have read, understood and signed the School Staff/Governor Acceptable Use Policy / Agreement;
- they report any suspected misuse or problem to the Principal i/c ICT for investigation;
- digital communications with students / pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official School systems;
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current School policies with regard to these devices.

Designated Person for Safeguarding / Child Protection Officer:

Should be trained in e-safety issues and be aware of the potential for serious child protection 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 the School ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to School systems;
- should 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 School policies on the use of mobile phones, digital cameras and hand held devices, they should also know and understand School policies on the taking / use of images and on cyber-bullying;
- 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.

Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The School will therefore take every opportunity to help parents understand these issues through a range of mediums. These could include; parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns.

POLICY STATEMENTS

Education – students:

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

E-Safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of ICT: this will cover both the use of ICT and new technologies in School and outside School.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.
- Students / pupils should 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.

Education – parents / carers:

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 experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

"There is a generational digital divide". (Byron Report).

The School will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, VLE.
- Parents' Evenings and training events.

Education and Training – Staff:

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 planned programme of formal e-safety training will be made available to staff. 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 performance management process.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the School e-safety policy and Acceptable Use Policies.
- The Principal i/c ICT and Designated Safeguarding Lead will receive regular updates through attendance at / the Trust / other information / training sessions and by reviewing guidance documents released by BECTA / ADEK and others.
- The Assistant Principal i/c ICT and Designated Safeguarding Lead will provide advice / guidance / training as required to individuals as required.

Training – Board of Trustees:

Board of Trustees should take part in e-safety training / awareness sessions, with particular importance for those who are members of any committee / group involved in ICT / e-safety / health and safety / child protection. This may be offered by participation in School training / information sessions for staff or parents.

Technical – infrastructure / equipment, filtering and monitoring:

The School will be responsible for ensuring that the 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 ICT systems will be managed in ways that ensure that the School meets the e-safety technical requirements outlined in the Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance.
- There will be regular reviews and audits of the safety and security of School ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to School ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the E-Safety Committee.
- All users will be provided with a username and password by the network manager who will keep an up to date record of users and their usernames. Users will be required to change their password every term.
- The “master / administrator” passwords for the School ICT system, used by the Network Manager must also be available to the Principal or Assistant Principal i/c ICT and kept in a secure place (eg School safe).
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. This extends to access for CIE, Edexcel support sites or any other software package purchased by the school.

- The School maintains and supports the managed filtering service.
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Principal (or other nominated senior leader). Any filtering issues should be reported immediately to the Network Manager.
- School ICT technical staff regularly monitor and record the activity of users on the School ICT systems and users are made aware of this in the Acceptable Use Policy.
- Personal data can not be sent over the internet or taken off the School site unless safely encrypted or otherwise secured.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that students 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.
- Where students are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Students should 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 should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images - Photographic, Video

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 and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The School 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 should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow School policies concerning the sharing, distribution and publication of those images.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute.
- Students must 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 will comply with good practice guidance on the use of such images.
- 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 the School website.
- Students' work can only be published with the permission of the student and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must 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.

Staff must ensure that they:

- At all times take care to ensure the safe keeping 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.
- No personal data is stored on any portable computer system, USB stick or any other removable media.
- Transfer data using encryption and secure password protected devices.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the School currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

Communication Technologies	STAFF & OTHER ADULTS				STUDENTS			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to School	✓				✓			
Use of mobile phones in lessons		✓					✓	
Use of mobile phones in social time	✓						✓	
Taking photos on mobile phones or other camera devices		✓						✓
Use of hand held devices eg PDAs, PSPs	✓					✓		
Use of personal email addresses in School, or on School network	✓							✓
Use of School email for personal emails	✓							✓
Use of chat rooms / facilities				✓				✓
Use of instant messaging		✓						✓
Use of social networking sites		✓						✓
Use of blogs	✓					✓		

When using communication technologies the School considers the following as good practice:

- The official School email service may be regarded as safe and secure and is monitored.
- Users must immediately report to the Line Manager / Head of Year / Pastoral Manager, in accordance with the School policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) School systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Personal information should not be posted on the School website and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate activities

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from School and all other ICT systems. Other activities eg Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a School context, either because of the age of the users or the nature of those activities.

The School believes that the activities referred to in the following section would be inappropriate in a School context and that users, as defined, should not engage in these activities in School or outside School when using School equipment or systems.

Responding to incidents of misuse

It is hoped that all members of the School community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (see following page) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a “clean” designated computer.

School policy restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images					✓
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					✓
	adult material that potentially breaches the Obscene Publications Act in the UK/UAE					✓
	criminally racist material in UK/UAE					✓
	pornography					✓
	promotion of any kind of discrimination					✓
	promotion of racial or religious hatred					✓
	threatening behaviour, including promotion of physical violence or mental harm					✓
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the School or brings the School into disrepute				✓	
Using School systems to run a private business					✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by and / or the School					✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					✓	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					✓	
Creating or propagating computer viruses or other harmful files					✓	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					✓	

On-line gaming (educational)		✓			
On-line gaming (non educational)			✓		
On-line gambling					✓
On-line shopping / commerce		✓			
File sharing		✓			
Use of social networking sites		✓			
Use of video broadcasting eg Youtube		✓			

It is more likely that the School will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the School community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Students	Actions / Sanctions								
	Refer to class teacher / tutor	Refer to Head of Centre / Head of Faculty / Head of Year /	Refer to Principal	Refer to Police	Refer to technical staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓	✓	✓	✓		✓
Unauthorised use of non-educational sites during lessons		✓			✓			✓	
Unauthorised use of mobile phone / digital camera / other handheld device	✓	✓						✓	
Unauthorised use of social networking / instant messaging / personal email	✓	✓						✓	
Unauthorised downloading or uploading of files		✓			✓			✓	
Allowing others to access School network by sharing username and passwords		✓			✓			✓	
Attempting to access or accessing the School network, using another student's / pupil's account		✓			✓	✓	✓		

		<i>'Achieving Excellence'</i>							
Attempting to access or accessing the School network, using the account of a member of staff		✓	✓		✓	✓	✓		✓
Corrupting or destroying the data of other users		✓			✓		✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓					✓		✓
Continued infringements of the above, following previous warnings or sanctions		✓	✓		✓	✓	✓		✓
Actions which could bring the School into disrepute or breach the integrity of the ethos of the School			✓		✓	✓			✓
Using proxy sites or other means to subvert the School's filtering system		✓			✓	✓	✓		✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓			✓	✓			✓
Deliberately accessing or trying to access offensive or pornographic material		✓	✓	✓	✓	✓			✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act					✓	✓		✓	

Staff	Actions / Sanctions							
Incidents:	Refer to Line Manager	Refer to Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓				
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✓					✓		
Unauthorised downloading or uploading of files	✓					✓		
Allowing others to access School network by sharing username and passwords or attempting to access or accessing the School network, using another person's account	✓				✓	✓		

Careless use of personal data eg holding or transferring data in an insecure manner					✓	✓		
Deliberate actions to breach data protection or network security rules		✓			✓		✓	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓	✓	✓		✓		✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓			✓	✓	✓	✓
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	✓				✓	✓		✓
Actions which could compromise the staff member's professional standing	✓					✓		✓
Actions which could bring the School into disrepute or breach the integrity of the ethos of the School		✓			✓	✓	✓	✓
Using proxy sites or other means to subvert the School's filtering system		✓			✓		✓	✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓				✓			
Deliberately accessing or trying to access offensive or pornographic material		✓	✓		✓	✓	✓	✓
Breaching copyright or licensing regulations		✓			✓	✓		
Continued infringements of the above, following previous warnings or sanctions		✓	✓				✓	✓