ANGLO EUROPEAN SCHOOL

E-SAFETY POLICY

Ratified by:	Full Governing Body
Date:	01/12/2021

E-safety Policy Rationale:

The purpose of this policy statement is to:

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
- provide staff and volunteers with the overarching principles that guide our approach to online safety
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

The policy statement applies to all staff, volunteers, children and young people and anyone involved activities linked to The Anglo European School.

E-safety encompasses internet technologies and electronic communications such as laptops, tablets, mobile phones and wireless technology. It highlights the need to educate students about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences. The purpose of internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and administration systems. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for students who show a responsible and mature approach to its use. Our school has a duty to provide students with quality internet access. Students will use the internet outside school and will need to learn how to evaluate internet information and to take care of their own safety and security.

We recognise that:

- the online world provides everyone with many opportunities; however it can also present risks and challenges
- we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
- we have a responsibility to help keep children and young people safe online, whether or not they are using our network and devices
- all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse
- working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

Policy Links:

The school's e-safety policy will operate in conjunction with other policies including those for Behaviour, Anti Bullying, Child Protection, Curriculum, IT and Data Protection. E-safety depends on effective practice at a number of levels:

- Responsible IT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband for learning including the effective management of content filtering.

E-safety considers the following technologies: PCs, laptops, tablets, webcams, digital video equipment, mobile phones, portable media players, games consoles and personal digital assistants. All persons either using technology or supervising the use of technology are required to abide by this policy.

E-safety requirements relate to school-owned technology and also to personal technologies. E-safety requirements are applicable during the times whereby the school is opened and the use of any school equipment outside of normal working hours. As well as extended school events, lettings for community use. It is also relevant to residential/off-site events e.g. school trips and visits.

Internet: The Benefit to Education

Benefits of using the internet in education include:

- Fully supports the school's implementation and delivery of a broad and balanced, international Curriculum to enhance learning opportunities
- Access to world-wide educational resources
- Educational and cultural exchanges between students world-wide
- Access to experts in many fields for students and staff
- Professional development for staff through access to national developments, educational materials and effective curriculum practice
- Collaboration across support services and professional associations
- Improved access to technical support including remote management of networks and automatic system updates
- Exchange of curriculum and administration data with the Local Authority and Department for Education DfE.
- Access to learning wherever and whenever convenient.

The school internet access will be designed expressly for student use and includes filtering appropriate to the age of students.

- Students will be taught what internet use is acceptable and what is not and given clear objectives for Internet use
- Internet access will be planned to enrich and extend learning activities
- Staff should guide students in on-line activities that will support learning outcomes planned for the students' age and maturity.
- Students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation

Authorised Internet Access:

Our school will comply with copyright law. All students must read and sign the 'Acceptable IT Use Agreement' before using any school IT resource. Parents will be informed that students will be provided with supervised internet access. Parents will be asked to sign and return a consent form for student access.

Safeguarding Children and Child Protection:

This policy is an extension of the child protection policy. Caution is expressed to the whole school community as regards child safety in the virtual world as well as the real world. Social networking sites, the uploading of inappropriate web content and cyber-bullying are issues that adults must ensure vigilance and ensure appropriate means are put in place to safeguard and educate our students. It is expected that students are able to develop their own protection strategies for when adult supervision and technological protection are not available.

World Wide Web:

If staff or students discover unsuitable sites, the URL (address), time, content must be reported to the network manager and RM who are likely to be the most readily available. School will ensure that the use of internet derived materials by students and staff complies with copyright law. Students should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email:

Students may only use approved e-mail accounts on the school system. Students must immediately tell a teacher if they receive offensive e-mail. Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission. Great care must be taken to ensure personal passwords remain confidential. If it is felt that a student has obtained a teacher's password, or if a student's password has been obtained by another student, this should

be reported to RM so that they can change it. Teachers are able to re-set passwords for students; please contact RM if you are unable to do this.

Staff must only communicate with students through their school email address. Staff should not contact parents from their work email address without specific approval; emails to parents should be sent via enquiries@aesessex.co.uk. E-mails sent to external organisations should be written carefully and professionally, in the same way as a letter written on school headed paper. In every case, e-mails should be confined to facts rather than giving judgements or criticisms. Our preferred form of communication with parents is Intouch and this is overseen by the Business Manager.

Social Networking:

The school will block/filter access to social networking sites and newsgroups unless a specific use is approved. Students will be advised never to give out personal details of any kind which may identify them or their location. Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.

Social Networking – guidance for Staff:

Before participating in any online community:

- staff must remember that anything posted online is available to ***anyone in the world***
- any text or photo placed online becomes the property of the site(s) and is completely out of our control the moment it is placed online – ***even if access to your site is limited***
- Staff are reminded of the need for discretion and professionalism when up-loading data which could potentially have a negative impact on the school or individual concerned. Such action could lead to disciplinary procedures being instigated.
- Staff ***should not*** add ***current students*** to or become members of students' social networking sites
- Staff have a duty of care to our young people and must not put themselves in situations which could potentially comprise their professionalism
- Staff must also be aware that ex-students may also have current students as members of their social networking sites. To this effect, staff are ***strongly advised*** not to post personal details such as address and telephone numbers etc. when setting up a social networking account
- Remember, photographs of you can be posted by others and tagged.
- Pornographic sites should not be accessed under any circumstances. Any teacher who uses school internet facilities to download pornographic materials is likely to be judged as committing an act of gross misconduct.
- Access to other offensive or inappropriate sites should also be avoided. There may be circumstances where access to such material is necessary to inform teaching and learning. In such cases, prior permission from the Designated Safeguarding Lead.

- No student or member of staff should post images or video footage of the school, staff, students or the school's name on any internet site, including social media platforms, without prior written consent from the Headteachers.

Use of webcams and / or video-conferencing:

The school is aware of the benefits which communicating using webcams can have. Webcams can be used in school for an approved education purpose. Webcams should only be used in scheduled lesson time and as part of the planned curriculum activity under teacher supervision.
In the event of school closure, we are unable to authorise the use of webcams from your own home in order to communicate with students as there are associated safeguarding risks.

Filtering:

The School has an extensive and effective filtering system which all staff and students go through. The system also tracks all users on computers in the school and keeps records of searches they have performed and a complete internet history over the year.

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 school supports staff CPD opportunities on the use of new and emerging technologies which promotes high quality teaching and learning.

Assessing Risks:

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access. The school will audit IT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate on a yearly basis.

Cyber bullying:

Cyber Bullying can take different forms such as: threats and intimidation; harassment or "cyber-stalking" (e.g. repeatedly sending unwanted texts or instant messages); vilification / defamation; exclusion or peer rejection; impersonation; unauthorised publication of private information or images and manipulation.

Students are not allowed to use their mobile phones during the school day. The School cannot be held responsible for any malicious communication that takes place between students via a mobile phone; communication on a mobile phone remains the responsibility of the bill payer. The School may be able to help in instances where restorative conversations need to take place to help manage an issue but parents

should report any incidents of cyber bullying to the Police if they consider that a crime has been committed.

Any cyber bullying that takes place via a school e-mail address or via a school computer should be reported to the class teacher, where appropriate, or Year Leader.

Promotion of e-safety:

The school will use the following strategies to raise awareness of e-safety:

- Internet Safety Week
- Assemblies
- Publication of the e-policy policy and additional guidance on the school website
- Information, advice and guidance is shared with parents
- New staff induction programme
- All our staff (teaching and non teaching) are trained as to how to recognise e-safety issues and how to report them,
- E-safety is addressed in the schools IT Acceptable Use Policy

Procedures for reporting a cause for concern:

If you feel that a student is in any way vulnerable then you must report this in accordance with our Child Protection Policy.

If a member of staff is in anyway subject to allegation, they must report this to the Headteachers in accordance with our Whistleblowing Policy.

Recommended reference sites:

https://www.ceop.police.uk/safety-centre/

https://www.nspcc.org.uk/keeping-children-safe/online-safety/

https://learning.nspcc.org.uk/research-resources/schools/e-safety-for-schools/