ICT and E-SAFETY POLICY

ICT and e-safety policy statement

This policy is written to help provide an environment in which students are protected from exposure to illegal, offensive or otherwise inappropriate material online without adversely affecting the learning experience

This policy is written in conjunction with the school rules and other safeguarding policies and is applicable to all students, staff, leaders and visitors who access the school's internet provision

Internet Access

The entire building and grounds of Anglotec are wireless enabled, and every classroom and office has at least one computer with internet access.

Staff may use the school's computer systems in the conduct of their duties. If preparing lessons, they must ensure that any material accessed is appropriate for use with their class, taking into account the age and cultural sensitivities of the students.

Students themselves may use the school's computer room or library to access websites to assist them in their studies, either with or without the guidance of a teacher. Students may also use their own devices, to access the internet using the school's WiFi.

However, staff and students are forbidden from accessing or transmitting any material which is deemed inappropriate or illegal, either on the school system or their own networks. This includes:

- exposure to inappropriate content, including online pornography, extremism, violent games, etc
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- racist, homophobic or other hate sites
- grooming
- cyber-bullying in all forms
- receiving or transmitting sexually explicit images or messages (sexting)
- breaching copyright

Firewalls are in place on the school's own networks, but all staff must be aware that students will have their own networks which may not have the same protection.

While the school accepts that it is impossible to control what a student's personal device with its own network accesses, it is nonetheless the responsibility off all staff to be alert and ensure, as far as humanly possible, that students do not access any websites which may be prohibited by this policy.

Managing the ICT infrastructure and Network

- Firewalls in place on the school's networks prevent the user accessing websites in the above categories, on the grounds that they are illegal, potentially illegal, inappropriate or offensive
- Sophos antivirus on all computers prevents access that is potentially threatening to the security of the school's systems

- Storage of all data within the school conforms to the UK Data Protection requirements
- Dual servers ensure that students do not have access to the network containing any confidential information
- Passwords are in place on all computers and students only have access to the passwords for the computer room and library
- The WiFi is password protected
- Data is backed up on a regular basis in the event that the system needs to be restored
- Classroom computers are to be locked by the teacher when leaving the classroom to prevent unauthorised access by students
- Any device loaned by the school to an employee must be used solely to help them in their work
- The hardware is maintained to ensure there is no health and safety risk
- Access to the school's network resources from remote locations is restricted and only approved in rare circumstances for purely work related matters
- No outside agencies, except our IT management organisation, are allowed to access Anglotec's network

Personal mobile phones and other mobile devices

- In class time student mobile phones and devices should only be used for learning purposes if requested by the teacher. They should be in airplane mode or silent at all times
- Personally owned mobile phones and devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for their loss, theft or damage
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside a professional capacity.
- Teachers are permitted to use their own mobile phones or devices in a teaching context, such as checking things on the internet for a class, but they must not disclose their personal number, email etc to the students
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.
- During work time mobile phones and personally-owned devices will be switched off or on 'silent mode' except where needed for work purposes
- Staff should never use their own photographic equipment (including mobile phones) to take images of students. If they plan to film or take photos of any under-18s on school equipment, they need to make sure that the student is happy for them to do so and check with the office that the parents have given their consent. Any images should be deleted immediately after use

Personal use of school systems

- The school permits the incidental personal use of school IT and other equipment provided that:
    - use must be minimal and take place out of normal working hours (that is, during lunch hour, before or after standard work hours)
    - it does not interfere in any way with the user carrying out his/her duties

    - it does not commit the school to any marginal costs
    - it complies with the school's policies including this policy
- Misuse or abuse of school equipment in breach of this policy will be dealt with in accordance with our disciplinary procedure. Serious breaches may amount to gross misconduct which can lead to summary dismissal. Misuse can, in certain circumstances, constitute a criminal offence and may result in a report to the police.

Responsibilities

The Principal
- has overall responsibility for ICT and e-safety, including the updating of firewalls as needed

The Principal will
- investigate and record all reported incidents of a breach of this policy
- make recommendations to the Principal based on their findings
- notify the Designated Safeguarding Lead if any incident involved an under-18 student

The Designated Safeguarding Lead will
- follow up on any incident involving an under-18
- liaise with agents/leaders/families of any under-18 involved
- notify the appropriate authorities if the incident is potentially criminal

Staff will
- read, understand and help promote the school's e-safety policy and guidance
- be aware of e-safety issues related to the use of mobile phones and other devices and monitor their use in classes and as far as is possible outside classes on activities etc.
- report any suspected misuse, abuse or access to inappropriate materials to the Principal
- model safe, responsible and professional behaviour in their own use of technology
- ensure any digital communications with students should be on a professional level and only through school based systems, never through personal email, texts etc

Students will
- understand the importance of reporting abuse, misuse or access to inappropriate
- know and understand that cyber bullying will not be tolerated
- understand the importance of adopting good e-safety practice, particularly in relation to under-18s

Homestays will
- understand the importance of adopting good e-safety practice in their own homes, especially when hosting under-18s
- report any suspected misuse, abuse or access to inappropriate materials to the Accommodation Manager, who will report it to the Principal

E-safety for Under-18s

Access to the internet is a wonderful way for young people to stay in touch with their friends and family but it also provides opportunities for abuse and inappropriate behaviour. In particular, there are risks to young people through cyber bullying (possibly by their peers), grooming by adult sexual predators, and illegal downloading of illegal or

copyrighted materials, and possibly also IT viruses. Anglotec has therefore established the following guidelines:

- Staff (excluding homestays) should not give out their personal mobile number, email address, social media contact details to students, especially those under 18
- Inappropriate access to websites should be reported to the Principal. Most inappropriate sites are blocked by the school firewall, but may be accessed by students in a home setting or through the internet on their own devices. Therefore, all staff are asked to be vigilant regarding use of the internet by under-18s, and if there are concerns they should notify the Principal
- Students are made aware of the school's IT policies at induction and these are displayed in the school and in particular in the computer rooms. Under-18s have a guide to safe internet use in their welcome pack