CHESHIRE ALTERNATIVE PROVISION SCHOOL E-SAFETY POLICY & USER AGREEMENT

Date of Policy	January 2019
Date of Review	January 2022
Person/s Responsible	Shane Mahon/Lana Wild

General Introduction

1.The e-Safety Policy works in conjunction with Cheshire Alternative Provision School's other policies including those for bullying and for child protection.
Our e-Safety Policy has been written by the school, and has been agreed by the Senior Leadership Team and approved by the school's Governors.

2. Teaching and learning
2.1 Why the Internet and digital communications are important
   The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with high-quality Internet access as part of their learning experience.
   Internet use is a part of the statutory curriculum and a necessary learning tool for staff and pupils.

2.2 Internet use will enhance and extend learning
   The school Internet access is designed expressly for pupil use and will include filtering appropriate to the age of pupils.
   Clear boundaries are set for the appropriate use of the Internet and digital communications and discussed with both staff and pupils.
   Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

2.3 Pupils will be taught how to evaluate Internet content
   The e-Safety co-ordinator, where possible, will ensure that the use of Internet derived materials by both staff and by pupils complies with copyright law.
   Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

2.4 User names and passwords
   When joining the school, all students will be allocated a user name and password for access to the school network. It is each student's responsibility to ensure that nobody else becomes aware of their password(s), as well as ensuring that they are changed on a regular basis.

3. Managing Internet Access

3.1 Information system security
   School ICT system security will be reviewed regularly by the school's IT management operators.

Virus protection will be installed and updated regularly.
Security strategies will be discussed, where necessary, with the school's governing body.

3.2 E-mail
Students may only use approved e-mail accounts on the school system.
Students must immediately tell either the e-safety co-ordinator or their teacher if they receive offensive e-mail.
In e-mail communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known and the attachment is expected.
The school will regularly review how e-mail from students to external bodies is presented and controlled.
The forwarding of chain letters is not permitted.

3.3 Published content and the school web site
Staff or student personal contact information will not generally be published. The contact details given online should be the school office.
The e-Safety coordinator responsible for ICT will take overall editorial responsibility and ensure that published content is accurate and appropriate.

3.4 Publishing students' images and work
Photographs that include students will be selected carefully so that individual pupils cannot be identified or their image misused.
Students' full names will not be used anywhere on a school Website or other on-line space, particularly in association with photographs.
Written permission from parents or carers will be obtained before photographs of students are published on the school Website.
Work can only be published with the permission of the student and parents/carers.

3.5 Social networking and personal publishing
The school will control access to social networking sites, and will educate students in their safe use.
Newsgroups will be blocked 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 should not place personal photos on any social network space without considering how the photo could be used now or in the future.
Students should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Students should only invite known friends and deny access to others.

3.6 Managing filtering
The school will work with the Internet Service Provider to ensure that systems to protect pupils are reviewed and improved.
If staff or students discover an unsuitable site, it must be reported to the e-Safety Coordinator or a member SLT.
The e-Safety coordinator responsible for ICT will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

4. 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.
Mobile phones will not be used during lessons or formal school time unless under the direct

supervision of a member of staff. The sending of abusive or inappropriate text messages is forbidden.

The use by students of cameras in mobile phones will not be permitted in school.

Student Internet access via mobile phone is not permitted in school

5. Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

No student/staff personal data must be stored on any removable device unless encrypted / pass worded.

6. Policy Decisions

6.1 Authorising Internet access

All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource. Staff must ensure that a signed copy of the agreement is in the possession of the e-Safety co-ordinator.

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

All students must apply for Internet access individually by agreeing to comply with the Responsible Internet Use statement.

6.2 Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.

The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

6.3 Handling e-safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the headteacher.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Students and parents will be informed of the complaints procedure.

Discussions will be held with the Police to establish procedures for handling potentially illegal issues.

7. Communicating e-Safety

7.1 Introducing the e-safety policy to pupils

e-Safety rules will be posted in all rooms where computers are used and a summary of the rules will appear on each PC in school as a reminder to pupils before they log into the school's network.

Students will be informed that network and Internet use will be monitored.

A programme of training in e-Safety will be included in the IT Induction lessons at KS3 and KS4.

7.2 Staff and the e-Safety policy

All staff will be given the School e-Safety Policy and its importance explained.

Staff will be informed that network and Internet traffic can be monitored and traced to the individual user. The internet should only be used in school where the individual's specific use is necessary to enable them to carry out their work in school.

Staff that manage filtering systems or monitor ICT use will be supervised by senior

management and work to clear procedures for reporting issues.

   Staff should ensure that any IT equipment provided by the school remains the property of the school at all times and should only be used for the purpose(s) it is intended for.

   Staff should understand that phone or online communications with pupils can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship and should not communicate online with students in any way other than for school purposes – eg for the submission of assignments etc

   Staff should not use Facebook or any other social networking site to communicate with students. They must ensure that the use of Facebook etc is restricted so that pupils cannot gain access to their profile.

7.3 Enlisting parents' and carers' support

   Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters and on the school Website.

   The school will maintain a list of e-safety resources for parents/carers.