Altwood
Church of England School

E-Safety Policy

Author:	Altwood School
Approver:	Local Governing Committee of Altwood School
Date:	Sept 2024
Next review:	October 2025
Category of policy:	

Changes history

Version:	Date:	Amended by:	Substantive changes:	Purpose:
1	**Sept 2025**	**Lead Governance Professional**	Split policy out from Safeguarding Policy	

What is E-Safety?

It is recognised by Altwood Church of England School that the use of technology creates great teaching and learning opportunities, whilst also presenting particular challenges and risks to children and adults both inside and outside of school related to their use.
The school recognises that it is its duty of care alongside that of parents and other members of the community to protect our children from these dangers and this can be achieved by many different mechanisms working together.

The school identifies that the issues classified within E-safety are considerable, but can be broadly categorised into three areas of risk:-

- **content:** being exposed to illegal, inappropriate or harmful material
- **contact:** being subjected to harmful online interaction with other users
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm

Student activities that can increase their risk of harm include:-

- Bullying via chat, text or email
- Obsessive gaming or internet use
- Accessing gambling or sexual content
- Illegal behaviour
- Sharing of nude or semi-nude images and videos

22.2 Purpose of E-Safety policy

The purpose of this e-safety policy is to outline what measures the school takes to ensure that students can work in an e-safe environment and that any e-safety issue is detected and dealt with in a timely and appropriate fashion.

22.3 General policy statement

The school will endeavour to ensure the e-safety of all school members. It will use education, technology, accountability, responsibility and legislation as the key ways to achieve this.

22.4 Whole school responsibilities for E-safety

Within the school, all members of staff and students are responsible for e-safety. Responsibilities for each group include:- Students:-

- Participating in and gaining an understanding of e-safety issues and the safe responses from e-safety training sessions.
- Compliance with a highly visible students' Acceptable Use Policy (AUP) which students must agree to each time they use school ICT equipment either in the school or remotely which connects to the internet.
- Reporting any e-safety issue to the teacher, Head of House or parent.
- Taking responsibility for their own actions using the internet and communications technologies.

All Staff:-

- Having a clear understanding of e-safety issues and the required actions from e- safety training sessions, of the expectations, applicable roles and responsibilities in relation to filtering and monitoring
- Reporting any e-safety issues to the DSL & IT Team as soon as the issue is detected
- Complying with a highly visible staff Acceptable Use Policy (AUP) each time they use school ICT equipment either in the school or remotely which connects to the internet
- Raise any concerns regarding PREVENT, extremism or safeguarding matters to the DSL or a deputy in line with this policy

Teaching Staff:-

- Educating students on e-safety through specific e-safety training sessions and reenforcing this training in the day to day use of ICT in the classroom
- Ensure that only school email is used to communicate with students past and present. Avoid use of social media or other communication channels with students past and present

Network Managers (Dan Capel & Gregor Pawlik):-

- Ensure that appropriate technological filtering and monitoring systems are in place when students and staff access school systems and internet provision. The school will be careful to ensure that these systems do not place unreasonable restrictions on internet access or limit what children can be taught with regards to online teaching and safeguarding.
- Monitoring the technology systems which track student internet use to detect e- safety breaches.
- Ensuring that all information captured using these systems is secure, accessible to the appropriate members of staff, and stored in a robust manner. In addition, securing and preserving evidence of any e-safety breach
- Checking and auditing all systems to ensure that no inappropriate data is stored or is accessible.
- Working with the Headteacher, review and advise on e-safety and acceptable use policies.
- Assisting in the resolution of e-safety issues with the Headteacher and Pastoral leadership.

ICT department:-

- Leading the development of the e-safety education programme for students and staff.
- Managing a parental awareness programme for e-safety.

Headteacher:-

- Dealing with E-safety breaches from reporting through to resolution in conjunction with the ICT support team
- Working with ICT team to create, review and advise on E-safety and acceptable use policies
- Working with outside agencies including the police where appropriate
- Maintaining a log of all e-safety issues

SLT:-

- The DSL and Senior Leadership Team should read annex D regarding Online Safety within 'Keeping children safe in education' 2023

22.5 How the school ensures E-safety in the classroom:-

Educating students in e-safety

A clear objective of the school is to educate students in safe use of ICT and the internet. We feel this is one of the best ways to minimise the potential for any e-safety issues to occur. Students will receive specific e-safety lessons aimed at ensuring that:-

- Students know the e-safety risks that exist and how to identify risk
- Students know how to mitigate against e-safety risks by using e-safe practices whilst online
- Students know when, how and to whom, to report instances when their e-safety may have been compromised
- Students know that they are in an environment that encourages them to report e- safety issues without risk of reprimand, humiliation or embarrassment
- All members of staff will have a duty to reinforce e- safety practices wherever possible and will offer students advice and support in the classroom where minor e-safety incidents have occurred
- E-Safety education information has high visibility in the school
- The school ensures a comprehensive whole school curriculum response is in place to enable all students to learn about and manage online risks effectively and supports parents and the wider school community (including all members of staff) to become aware and alert to the need to keep children safe online
- Mobile phones are not permitted to be used on site by students at any point (other than Sixth Formers in the Sixth Form Centre). Mobile phone networks can be accessed easily, and each smart phone carries both a still and moving image camera, along with microphone. Thus, to safeguard young people and their privacy, any phones seen or heard being used will be confiscated for parents or carers to collect.

Acceptable Use Policies

All school members i.e. students, staff and parents must agree to an Acceptable Use Policy (AUP) before they can use school ICT systems. With respect to e-safety the AUP details:- •

The user's responsibilities

- Activities which are appropriate and inappropriate
- Best practice guidelines
- How the school will monitor e-safety
- What information is collected

Altwood Church of England School acknowledges that whilst filtering and monitoring is an important part of school's online safety responsibilities, it is only one part of its role. Children and adults may have access to systems external to the school control such as mobile phones and other internet enabled devices and technology. The school does not allow mobile telephones to be switched on or used by students on site. This reduces the risk of potential harm and / or abuse during the school day. 6th Formers may use their phones and "own devices" inside the 6th Form

Centre. Failure to abide by this element of the school's Behaviour for Learning policy will result in the confiscation of the telephone until parents can collect.

How E-safety is monitored

- The Behaviour Mentors and DSL, along with the Network Managers, will actively monitor students' ICT activity using a monitoring system which can flag potential e-safety issues. Issues with regard to safeguarding and extremist matters are alerted as an urgent alert by SENSO, the monitoring and filtering software. This will be investigated by Deputy DSLs and action taken as appropriate
- A weekly log is sent to DSL and Behaviour Mentors covering lower level concerns. Where these are of a behavioural nature, the class teacher is informed; where they are of a safeguarding nature, normal procedures are followed; where the matter occurred outside of school, parents and carers will be informed
- Deputy DSLs monitor and amend the lists of words and acronyms picked up by SENSO as appropriate
- Records are kept on SENSO regarding actions taken, and shared on to CPOMS as appropriate
- The ICT teaching staff will periodically review internet access logs to track any websites which could potentially present an e-safety issue
- The Network Managers will periodically review the E-Safety log to track and trends and use the information to look at ways of improving the student's e-safety
- Teaching staff will directly monitor the students' ICT and internet use in the classroom

How technology is used

The school will employ a variety of different technologies to help to ensure e-safety for all school members:-

- The school will use internet filtering to block inappropriate content and in addition block websites which are irrelevant to the student's programme of study and are considered time wasting
- The school will use a system which tracks all student activity on the school's computers. This system will automatically flag potential e-safety issues which will be monitored and then can be investigated by the ICT staff and pastoral teams. See above for details.
- The school will restrict which activities the students can perform using ICT and the internet through systems, security policy and access control
- Teaching staff will use control mechanisms to attempt to limit the applications and websites which the students can visit whilst using ICT within a lesson
- SENSO will be used to facilitate teaching staff to monitor and intervene on students' use of computers

22.6 How the school will respond to issues of misuse

The following are provided for the purpose of example only. Whenever a student or staff member infringes the E-Safety Policy, the final decision on the level of sanction will be at the discretion of the Headteacher.

Students:-

Category A infringements

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) during the school day
- Use of unauthorised instant messaging / social networking sites.

[Possible Sanctions: **referred to Head of House/ Head of IT and Computing** / contact with parent / removal of Internet access rights for a period; if seen with phone between 8.45am and 3.10pm, phone will be confiscated and collected by parent]

Category B infringements

- Continued use of non-educational sites during lessons after having been warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile phone (or other new technologies) after first sanction
- Accidentally accessing offensive material and not notifying a member of staff of it

[Possible Sanctions: referred to Head of House/ Head of ICT / contact with parent / removal of Internet access rights for an extended period / exclusion / no longer allowed to bring phone to school]

Category C infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email that is regarded as harassment, intimidatory or of a bullying nature (one-off incident)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet
- Transmission of commercial or advertising material

[Possible Sanctions: referred to Head of House/ Head of ICT / Assistant Head (Pastoral) / Headteacher / contact with parents / removal of equipment / removal of Internet and/or Learning Platform access rights for an extended period / suspension / permanent exclusion / referral to police]

Category D infringements

- Continued sending of emails or e-messages regarded as harassment or of an intimidatory or bullying nature after previous sanction

- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, or hate based
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school's name into disrepute

[Possible Sanctions - Referred to Assistant Head with responsibility for Behaviour / Headteacher / parent informed / suspension / permanent exclusion / removal of equipment / referral to police]

Staff:-

Category A infringements (Misconduct)

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Misuse of first level data security, e.g. wrongful use of passwords
- Breaching copyright or license e.g. installing unlicensed software on network

[Sanction - referred to line manager / Headteacher / Warning given.]

Category B infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic, violent or hate based;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988; • Bringing the school into disrepute.

[Sanction - referred to Headteacher and follow school disciplinary procedures / Police / Governors]

Child Pornography:
In the case of child pornography being found, the member of staff will be immediately suspended and the school disciplinary procedures implemented.

Other safeguarding actions:

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop
- Instigate an audit of all ICT equipment to ensure there is no risk of students accessing inappropriate materials in school or via school equipment
- Identify the precise details of the material
- Where appropriate, involve external agencies as part of these investigations

How will staff and students be informed of these procedures?

- Procedures are included within the school's e-safety / Acceptable Use Policy. All staff are required to sign the school's E-safety Policy acceptance form;
- Students will be instructed about responsible and acceptable use and given strategies to develop 'safe behaviours' through ICT lessons. Students are required to sign an age appropriate e-safety / acceptable use form;
- The school's e-safety policy will be made available to parents who are required to sign an acceptance form when their child starts at the school.

22.7 Working with parents and the community

Clearly many school students will also have access to ICT and the internet at home, often without some of the safeguards that are presents within the school environment. Therefore parents must often be extra vigilant about their child's e-safety at home.

One of the goals of the school is to support parent's role in providing an e-safe environment for their children to work in outside the school. The school does this in several ways, including publishing esafety information and directing parents to external e-safety advisories via the school website.

22.8 Acceptable Use Policies

The school has the following acceptable use policies in place which must be agreed to before the relevant individuals will be able to access ICT systems and the internet:-

- Staff ICT and the Internet Acceptable Use Policy
- Students ICT and the Internet Acceptable Use Policy • Parents Acceptable Use Policy for Parents Portal Access.
- A copy of these policies is available on request. The school will regularly review and update these policies.