



Auckland College Independent School

Every Pupil Matters, Every Moment Counts

E-Safety Policy





Document Control

Owner:	Auckland College Independent School
Written by:	S.Livramento & L.Willis
Approved by:	A.Akaraonye – Chair of Governors
Applies to:	Whole School
Date effective from:	September 2026
Review period:	1 Year
Date of next review:	September 2027
Version:	V1



Table of Contents

E-Safety Policy	4
Rationale	4
Why is internet use important?	4
How does the internet benefit education?	4
Objectives	4
Members of staff responsible	5



E-Safety Policy

Rationale

E-Safety encompasses Internet technologies and electronic communications such as mobile phones. This policy highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experiences. This policy will operate in conjunction with other school policies including those for ICT, behaviour, bullying, PSHCE and child protection.

Why is internet use important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

- Internet use is a part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- 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 quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does the internet benefit education?

- Access to world-wide educational resources including museums and art galleries.
- Educational and cultural exchanges between pupils world-wide;
- Cultural, vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across support services, professional associations and between colleagues;
- Improved access to technical support including remote management of networks and automatic system updates;
- Access to tools of direct communication, including video conferencing and email.

Objectives

- Key Stage 2 and 3 pupils will take part in a project about e-safety where they will discuss chat rooms, social networking, and cyber bullying and acceptable use of the internet.



- Software will be used to monitor what websites pupils can access and most well-known websites containing social networking, blogging, peer-to-peer, chat rooms and explicit material will be blocked so that pupils have no access to these.
- The school ICT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Files held on the school's network will be regularly checked.
- Our IT provider will ensure that the system has the capacity to take increased traffic caused by Internet use.
- Images, which include pupils, will be selected carefully and only those children whose written parental permission has been sought will be identifiable.
- Pupils' full names will not be used on the Website when associated with photographs, or in any way which may be to the detriment of pupils.
- Pupil photographs will immediately be removed from the school Website/social media upon request from parents, or other appropriate request.
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or school.
- Pupils 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.

Members of staff responsible

Although any member of staff using ICT in their teaching has a responsibility to understand the requirements of the e-safety policy, the main responsibility will lie with the Head of ICT and the Headteacher. As the e-safety policy links in with safeguarding and anti-bullying there may also be extreme cases where Directors are involved because of a suspension or exclusion.