# E-Safety Policy

| | |
|---|---|
| Last Reviewed: | September 2021 |
| Next Review Due: | September 2022 |
| Reviewed By: | Zoe Wiles |

## Introduction

At The London Acorn School we believe that we have a duty to provide pupils with Internet access for our older pupils as part of their learning experience across all curricular areas. The use of the Internet is an invaluable tool in the development of lifelong learning skills.

We believe that when used correctly, Internet access will not only raise standards, but it will support teachers' professional work and it will enhance the school's management information and business administration systems.

We acknowledge that the increased provision of the Internet inside and outside of school brings with it the need to ensure that learners are safe. We need to teach pupils how to evaluate Internet information and to take care of their own safety and security.

E-safety, which encompasses Internet technologies and electronic communications, will educate pupils about the benefits and risks of using technology and provide safeguards and awareness to enable them to control their online experience.

## Aims

● This is a whole school policy to ensure all members of the school community make use of the internet and other technologies for appropriate professional and educational purposes. In considering the scope of the school's e-safety strategy, the School will take a wide and purposeful approach to considering what falls within the meaning of technology, networks and devices used for viewing or exchanging information including communications technology (collectively referred to in this policy as Technology).

● To ensure that Internet use and use of related technologies is monitored and managed appropriately.

● To provide a mechanism by which staff and pupils are protected from sites, information and individuals that could undermine the principles and aims of the school.

● To provide rules which are consistent and in agreement with the Data Protection Act and with acceptable procedures commonly used on the internet, including those associated with Netiquette.

## The Governing Body has:

● appointed the Headteacher to be the Coordinator for E-Safety.
● delegated powers and responsibilities to the Head Teacher to ensure all school personnel and visitors to the school are aware of and comply with this policy.
● responsibility for ensuring funding is in place to support this policy.
● responsibility for ensuring this policy is made available to parents.
● nominated a link governor to communicate with the school regularly, to liaise with the Headteacher/ coordinator and to report back to the Governing Body.
● agreed to undertake training in order to understand e-safety issues and procedures.
● responsibility for the effective implementation, monitoring and evaluation of this policy.

## The Headteacher will:

● ensure all school personnel, pupils and parents are aware of and comply with this policy.
● work with the Governing Body to create a safe ICT learning environment by having in place:
    - an effective range of technological tools
    - clear roles and responsibilities
    - safe procedures
    - a comprehensive policy for pupils, staff and parents.
● monitor the effectiveness of this policy.
● annually report to the Governing Body on the success and development of this policy.

## The E-Safety Coordinator will:

● ensure that all Internet users are kept up to date with new guidance and procedures.
● have editorial responsibility for the school website and will ensure that content is accurate and appropriate.
● monitor the implementation of this policy and its effectiveness.
● monitor the e-safety incident log that is kept in the school office to ensure that any reported problems with the filtering system are dealt with appropriately.
● safeguard the wireless encryption key known only to Safeguarding Team.
● ensure all Anti- Virus software is updated on all devices.

## The Link Governor will:

● work closely with the Headteacher and the E-Safety Coordinator.
● ensure this policy and other linked policies are up to date.
● ensure that everyone connected with the school is aware of this policy.
● report to the Governing Body every term.
● annually report to the Governing Body on the success and development of this policy.

## School Staff will:

● comply with all the aforementioned aspects of this policy.
● accept the terms of and sign the staff 'Acceptable Use Staff Agreement Form' (see Appendix B).
● be responsible for promoting and supporting safe behaviours with pupils and e-safety procedures.
● ensure that the use of Internet derived materials complies with copyright law.
● undertake appropriate training.
● ensure mobiles are only used in designated areas (staffroom or offices).

## Pupils will be made aware of, and expected to comply with this policy, and will be taught to:

● be critically aware of the materials they read.
● validate information before accepting its accuracy.

● acknowledge the source of information used.
● use the Internet for research.
● respect copyright when using Internet material in their own work.
● report any offensive email.
● ensure all mobile phones are given in to the school office and not taken into class.

## Parents/carers will:

● be aware of and comply with this policy.
● be asked to support the e-safety policy and to sign 'Parental Consent for Use of ICT in school' form (see Appendix A) allowing their child to have Internet access.
● make their children aware of the e-safety policy.
● when in school, turn off mobiles or have them on silent.

## The school Internet access will:

● be designed for pupil use.
● include appropriate filtering.
● include filtering appropriate to the age of pupils.
● be reviewed and improved at regular intervals.

## Authorisation of Internet Access:

● Before using any school ICT resource, all staff must read and sign the 'Acceptable Use Staff Agreement Form' (see Appendix B).
● Parents must read and sign 'Parental Consent for Use of ICT in school' form (see Appendix A) before their child has access to the Internet.
● Before using any school ICT resource, pupils must read and sign 'Pupil E-Safety Agreement Form' (see Appendix C).
● All up to date records will be kept of all pupils and school personnel who have Internet access.

## When using e-mail, all pupils must:

● only use approved email accounts.
● report receiving any offensive emails.
● not divulge their own or others personal details.
● not arrange to meet anyone via the email.
● seek authorisation to send a formal email to an external organisation.

## The School Website

Contact details on the website will be:
● the school address,
● e-mail address and
● telephone number.

## The school website will not publish:

● staff or pupils contact details;
● the pictures of children without the written consent of the parent/carer;
● the names of any pupils who are shown;
● children's work without the permission of the pupil or the parent/carer.

## Social Networking

Pupils will not be allowed access:
● to social networking sites except those that are part of an educational network or approved Learning Platform;
● to newsgroups unless an identified need has been approved.

## Netiquette

Netiquette is a term referring to good behaviour while connected to the Internet. Netiquette is mainly referring to behaviour while using Internet facilities such as individual websites, emails, newsgroups, message boards, chat rooms or web communities. The following rules, for staff and pupils, will ensure that we are well-mannered when communicating electronically:

● Do not use someone else's name and pretend to be them.
● Do not try to obtain someone else's password.
● Do not call anyone names or threaten them with personal violence.
● Never forget that the person reading your mail is, indeed, a person, with feelings that can be hurt.
● Do not send anonymous messages.
● Write clearly and succinctly.
● Do not forward chain letters or unsolicited e-mails.
● Do not attach large files unless absolutely necessary.
● Do not use capital letters in messages (this is considered to be shouting).
● Proof read before you send.
● Check your emails regularly.
● Acknowledge that you have received a document.

## Adult Code of Conduct for Safe Use of Technology

**Mobile phone use**:
● Only use your phone during school breaks.
● Switch off your phone and store in your locker.
● Never phone parents or school agencies from your own phone.
● Never take photos of children with your phone.
● Never give your phone number to children or parents (accept for Class Representative).
● Never send text messages about children or their parents on your phone.

**Computer safety:**
● Never tell children your personal email address.
● Never communicate with children on social networking sites.
● Never send photos of children on the internet.

● Always send confidential information (i.e. with children's names) securely, in a manner consistent with agreed school policy.
● Never keep photos or films of children on s USB stick.
● Do not keep confidential information on a USB stick.
● Do not allow children in your care to have unsupervised access to computers.

**Camera use:**
● Always use a school camera to take photos of children.
● Never take a school camera home.
● Always remove past photos from a school camera before taking it on a trip.
● Do not allow non staff access to our photos without express permission from the parents, in writing and with the permission of the Head Teacher.
● Do not allow non staff to photograph our children without written permission from parents given through the Head Teacher.

## How complaints regarding E-Safety will be handled

The school will take all reasonable precautions to ensure e-safety. However, owing to the size and nature of the internet, the availability of mobile technologies and the speed at which technologies change, it is not possible to guarantee that unsuitable material will never appear on a school website. The school cannot accept liability for material accessed in school, nor any consequences of Internet access.
Our E-Safety Coordinator and the Head Teacher act as the first point of contact for any complaint. The Head Teacher will deal with all complaints of Internet misuse by school personnel.

**One or more of the following sanctions may be applied for Internet misuse:**
● Internet use only with adult supervision.
● A ban from using the Internet for a time.
● Email account withdrawn.
● Discussion with the Head Teacher.
● Informing parents or carers.
● Referral to police.

Complaints of cyberbullying are dealt with in accordance with our Behaviour Policy. Complaints related to child protection are dealt with in accordance with stated school procedures.

## Education in E-Safety

The London Acorn School will work to raise the awareness and importance of safe and responsible use of the internet and related technologies. The children will be taught rules that will help to protect them when using the Internet at school and at home. Children will be supported in making informed and appropriate choices if they encounter people and material online that may be challenging, prejudiced, inaccurate or that promote an extreme lifestyle or point of view.

## Inappropriate Material

Any inappropriate websites or material found by pupils or school personnel will be reported to the E-Safety Coordinator who in turn will report to the Internet Service Provider.

## Security of The London Acorn School Internet system

● New programs will be installed onto the network or stand alone machines by authorised personnel only.
● Personal memory sticks, CD's and other data recording devices may not be used in school.
● Everyone must be aware that under the Computer Misuse Act 1990, the use of computer systems without permission or for inappropriate use, could constitute a criminal offence.

## Reviewing this E-Safety Policy

The effectiveness of this policy will be reviewed by the E-Safety Coordinator, the Head Teacher and the Link Governor on an annual basis. In line with new technologies the necessary recommendations for improvement will be made to the governors.