CONWAY PRIMARY SCHOOL

E-safety Policy

Approved by:		**Date:** 02nd September 2020
Last reviewed on:	August 2020	
Next review due by:	September 2023	

Conway Primary E–SAFETY POLICY

Conway School believes that the use of information and communication technologies by children brings great benefits. Recognising the e-Safety issues and planning accordingly will help to ensure appropriate, effective and safer use of electronic communications. This Policy will help raise awareness of how we can keep children safe.

Table of Contents

Teaching and learning

Why is Internet use important?

We use the internet for a number of reasons:
Internet use is part of the statutory curriculum and a necessary tool for learning.
The Internet is a part of everyday 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 need to learn how to evaluate Internet information and to take care of their own safety and security.
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.
Benefits of using the Internet in education include:

access to worldwide educational resources including museums and art galleries;
inclusion in the National Education Network which connects all UK schools;
educational and cultural exchanges between pupils worldwide;
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 networks of schools, support services and professional associations;
improved access to technical support including remote management of networks and automatic system updates;
exchange of curriculum and administration data with KCC and DCSF;
Access to learning wherever and whenever convenient.

How can Internet use enhance learning?
The school's Internet access will be designed to enhance and extend education.
Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
The schools will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and maturity.
Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

How will pupils learn how to evaluate Internet content?
Because the quality of information received via radio, newspaper and telephone is variable and information received via the Internet, email or text message requires even better information handling and digital literacy skills. In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read:
Pupils should be made aware of the materials they read and shown how to validate information before Accepting its accuracy.
The evaluation of online materials is a part of teaching/learning in every subject.

Managing Information Systems
How will information systems security be maintained?
The security of the school information systems and users will be reviewed regularly.
Virus protection will be updated regularly.
Personal data sent over the Internet or taken off site will be encrypted.
Portable media may not used without specific permission followed by a virus check.
Unapproved software will not be allowed in pupils' work areas or attached to email.
Files held on the school's network will be regularly checked.
The ICT coordinator/network manager will review system capacity regularly.

How will email be managed?
Whole class or teacher email addresses will be used in Conway for communication outside of the school by children.
Pupils may only use approved email accounts.
Pupils must immediately tell a teacher if they receive offensive email.
Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
Access in school to external personal email accounts may be blocked.
Email sent to external organisations should be written carefully and authorised before sending, in the same
Way as a letter written on school headed paper.
The forwarding of chain messages is not permitted.
Staff should only use school email accounts to communicate with pupils as approved by the senior

Leadership Team.
Staff should not use personal email accounts during school hours or for professional purposes

How will published content be managed?

We have created an excellent websites that inspires pupils to publish work of a high standard.
We use it to celebrate pupils' work, promote the school and publish resources for projects.
Publication of information should be considered from a personal and school security viewpoint.
Material such as staff lists and a school plan are published in the school handbook and on a secure part of the website which requires authentication.
The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate and editorial guidance will help reflect the school's requirements for accuracy and good presentation.
The website will comply with current guidelines for publications including respect for intellectual property rights and copyright.

Can pupil's images or work be published?

Still and moving images and sounds add liveliness and interest to a website, particularly when pupils can be
included. Nevertheless the security of staff and pupils is paramount. Although common in newspapers, the
publishing of pupils' names with their images is not acceptable. Published images could be reused, particularly if large images of individual pupils are shown.
Strategies include using relatively small images of groups of pupils and possibly even using images that do
not show faces at all. "Over the shoulder" can replace "passport style" photographs but still convey the
educational activity. Personal photographs can be replaced with self portraits or images of pupils' work or of a team activity. Pupils in photographs should, of course, be appropriately clothed.
Images of a pupil should not be published without the parent's or carer's written permission. Pupils also need
to be taught the reasons for caution in publishing personal information and images online (see section 2.3.6).
Images that include pupils will be selected carefully and will not provide material that could be reused.
Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
Written permission from parents or carers will be obtained before images of pupils are electronically published once per year.
Pupils work can only be published with their permission or the parents.

How will social networking, social media and personal publishing be managed?

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks
which allow individuals to publish unmediated content. Social networking sites can connect people with
similar or even very different interests. Users can be invited to view personal spaces and leave comments,
over which there may be limited control.
Although primary age pupils should not use Facebook, pupils should be encouraged to think about the ease
of uploading personal information, the associated dangers and the difficulty of removing an inappropriate
image or information once published.
No member of staff should use social networking sites or personal publishing sites to communicate with
students.
Staff need to be aware of the importance of considering the material they post, ensuring profiles are secured
and how publishing unsuitable material may affect their professional status.
Examples include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming,

chatrooms, instant messenger and many others.
The school will control access to social media and social networking sites.
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 email addresses, full names of friends/family, specific interests and clubs etc.
Pupils will 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.
Staff are advised not to run social network spaces for pupil use on a personal basis.
Pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

How will filtering be managed?
The school will work with Greenwich LA, Becta and the Schools Broadband team to ensure that systems to protect pupils are reviewed and improved.
If staff or pupils discover unsuitable sites, the URL must be reported to the e–Safety Coordinator.
The school's broadband access includes filtering appropriate to the age and maturity of pupils.
Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
Any material that staff believe is illegal must be reported to the headteacher who will inform the appropriate agencies such as IWF or CEOP.

How can emerging technologies be managed?
We recognise that many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools.
A risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom use to be developed. The safest approach is to deny access until a risk assessment has been completed and safety established.
Virtual online classrooms and communities widen the geographical boundaries of learning.
Approaches such as mentoring, online learning and parental access are becoming embedded within school systems.
The safety and effectiveness of virtual communities depends on users being trusted and identifiable.
This may not be easy, as authentication beyond the school may be difficult as demonstrated by social networking sites such as Bebo and MySpace The registering of individuals to establish and maintain validated electronic identities is essential for safe communication, but is often not possible.
Video conferencing introduces new dimensions; webcams are increasingly inexpensive and, with faster Internet access, enable video to be exchanged across the Internet. The availability of live video can sometimes increase safety — you can see who you are talking to — but if inappropriately used, a video link could reveal security details.
New applications are continually being developed based on the Internet, the mobile phone network, wireless, Bluetooth or infrared connections. Users can be mobile using a phone, games console or personal digital assistant with wireless Internet access. This can offer immense opportunities for learning as well as dangers such as a pupil using a phone to video a teacher's reaction in a difficult situation.
We keep up to date with new technologies, including those relating to mobile phones and handheld devices,
and be ready to develop appropriate strategies.
There are dangers for staff however if personal phones are used to contact pupils or families and therefore a
school owned phone should be used.
The inclusion of inappropriate language or images is difficult for staff to detect. Pupils may need reminding
that such use is inappropriate and conflicts with school policy. Abusive messages should be dealt with under
the school's behaviour and/or anti-bullying policies.

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. The sending of abusive or inappropriate
text, picture or video messages is forbidden.

How should personal data be protected?

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can
be very useful in improving services, data could be mishandled, stolen or misused.
The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes
openness in the use of personal information. Under the Act every organisation that processes personal
information (personal data) must notify the Information Commissioner's Office, unless they are exempt.
The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held
About them. The eight principles are that personal data must be:
Processed fairly and lawfully
Processed for specified purposes
Adequate, relevant and not excessive
Accurate and up-to-date
Held no longer than is necessary
Processed in line with individual's rights
Kept secure
Transferred only to other countries with suitable security measures.
This section is a reminder that all data from which people can be identified is protected.
Personal data will be recorded, processed, transferred and made available according to the Data Protection
Act 1998.

Policy Decisions

How will Internet access be authorised?

We allocate Internet access for staff and pupils on the basis of educational need. It should be clear who has
Internet access and who has not. Authorisation is as individuals and usage is fully supervised.
Normally all pupils will be granted Internet access, we keep a lists of those who are denied access. Parental
permission is required for Internet access in all cases as new pupils join Fox field.
The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT
resource.
At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised
access to specific, approved online materials.
Parents will be asked to sign and return a consent form for pupil access.
Parents will be informed that pupils will be provided with supervised Internet access.

How will risks be assessed?

Conway will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Greenwich LA can accept liability for the material accessed, or any consequences resulting from Internet use.We will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.
The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
Methods to identify, assess and minimise risks will be reviewed regularly and after every breech of this policy.

How will e–Safety complaints be handled?
Complaints of Internet misuse will be dealt with under the School's Complaints Procedure.
Any complaint about staff misuse must be referred to the headteacher. If the complaint is about the headteacher this should be reported to the chair of governors through the school office.
All e–Safety complaints and incidents will be recorded by the school — including any actions taken.
Pupils and parents will be informed of the complaints procedure.
Parents and pupils will work in partnership with staff to resolve issues.
Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguards Unit to establish procedures for handling potentially illegal issues.
Any issues (including sanctions) will be dealt with according to the school's disciplinary and child protection procedures.

How is the Internet used across the community?
We recognise that children can access the internet outside of school and offer support and advice to parents on internet safety though regular information sent home with children and through advice on our website.
The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

How will Cyberbullying be managed?
Cyberbullying is defined as "The use of Information Communication Technology, particularly mobile phones
and the internet to deliberately hurt or upset someone" DCSF 2007
Many young people and adults find using the internet and mobile phones a positive and creative part of their
everyday life. Unfortunately, technologies can also be used negatively. When children are the target of
bullying via mobiles phones, gaming or the internet, they can often feel very alone, particularly if the adults
around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.
It is essential that young people, Foxfield staff and parents and carers understand how cyberbullying is
different from other forms of bullying, how it can affect people and how to respond and combat misuse.
Promoting a culture of confident users will support innovation and safety

DCSF and Childnet have produced resources and guidance that will be used to give practical advice and guidance on cyberbullying: http://www.digizen.org/cyberbullying
Cyberbullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's policy on anti-bullying.
There are clear procedures in place to support anyone affected by Cyberbullying through Place 2 Be and our e-Safety team.
All incidents of cyberbullying reported to the school will be recorded.
There are clear procedures in place to investigate incidents or allegations of Cyberbullying:
Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying

and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
Sanctions for those involved in Cyberbullying may include:
The bully will be asked to remove any material deemed to be inappropriate or offensive.
A service provider may be contacted to remove content.
Internet access may be suspended at school for the user for a period of time.
Parent/carers will be informed.
The Police will be contacted if a criminal offence is suspected.

How will Learning Platforms and learning environments be managed?
SLT and staff will monitor the usage of the LP by pupils and staff regularly in all areas, in particular message
and communication tools and publishing facilities.
Pupils/staff will be advised on acceptable conduct and use when using the learning platform.
Only members of the current pupil, parent/carers and staff community will have access to the LP.
All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or
transferred to their new establishment.
Any concerns with content may be recorded and dealt with in the following ways:
a) The user will be asked to remove any material deemed to be inappropriate or offensive.
b) The material will be removed by the site administrator if the user does not comply.
c) Access to the LP for the user may be suspended.
d) The user will need to discuss the issues with a member of SLT before reinstatement.
di)e) A pupil's parent/carer may be informed.

Communication Policy
How will the policy be introduced to pupils?
At Conway we teach about e–Safety as an ICT lesson activity and as part of every subject whenever pupils are using the internet.
All users are informed that network and Internet use will be monitored.
An e–Safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.
Pupil instruction in responsible and safe use should precede Internet access.
e–Safety training will be part of the transition programme across the Key Stages and when moving between establishments.
Safe and responsible use of the internet and technology will be reinforced across the curriculum.
Particular attention will be given where pupils are considered to be vulnerable.
We will use the following e–Safety programmes:
Think U Know: ***www.thinkuknow.co.uk***
Childnet: ***www.childnet.com***
Kidsmart: ***www.kidsmart.org.uk***
Safe Social Networking: ***www.safesocialnetworking.com***

How will the policy be discussed with staff?
The e–Safety Policy will be formally provided to and discussed with all members of staff.
To protect all staff and pupils, the school will implement Acceptable Use Policies.
Staff should be aware that Internet traffic can be monitored and traced to the individual user, Discretion and
professional conduct is essential.
Staff that manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and
have clear procedures for reporting issues.
Staff training in safe and responsible Internet use both professionally and personally will be provided.
How will parents' support be enlisted?
Parents' attention will be drawn to the School e–Safety Policy in newsletters, the school brochure and on the
school website.
A partnership approach with parents will be encouraged. This will include parent meetings with demonstrations and suggestions for safe home Internet use.

Parents will be requested to sign an e–Safety/internet agreement as part of the Home School Agreement.
Information and guidance for parents on e–Safety will be made available to parents in a variety of formats.
Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
Interested parents will be referred to organisations listed in section “e–Safety Contacts and References.”

Policy Management

Who will review the policy?

The school has an e–Safety panel made up of the ICT coordinator, Inclusion Manager and Headteacher.
The e–Safety Policy and its implementation will be reviewed annually by the panel.
Our e–Safety Policy has been written by the school, building on borough advice and government guidance. It has been agreed by the Senior Leadership Team and approved by governors.

Date when e-Safety policy was last reviewed: September 2020
Date when next review is due: September 2023

Signed Stephen Gatiss Date: September 2020

e-Safety Contacts and References

Becta: www.becta.org.uk/safeguarding
CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
Childline: www.childline.org.uk
Childnet: www.childnet.com
Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk
Cybermentors: www.cybermentors.org.uk
Digizen: www.digizen.org.uk
Internet Watch Foundation: www.iwf.org.uk
Kidsmart: www.kidsmart.org.uk
Teach Today: http://en.teachtoday.eu
Think U Know website: www.thinkuknow.co.uk
Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com