Wyken Croft
Primary School

E-Safety Policy

Review:	Annually
Reviewed by:	Georgette Franklin and Kerry Webb
Agreed by Governors:	October 2021
Shared with Staff:	October 2021
Date for next review:	October 2022

Wyken Croft
Primary School

Wyken Croft Primary School

E-Safety Policy

Writing and reviewing the e-safety policy

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences. The school's e-safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Bullying, Curriculum, Data Protection and Security.

- The school will appoint an e-Safety coordinator. The e-Safety Coordinator will liaise with the Child Protection Coordinator and/or Phase Leaders where necessary.
- Our e-Safety Policy has been written by the Designated Safeguarding Lead (DSL), building on the Warwickshire ICT Development Service e-Safety Policy and government guidance. It has been agreed by the Headteacher and approved by governors.
- The e-Safety Policy will be reviewed annually.

Teaching and learning

Why Internet use is important?

- Internet use is part of the statutory curriculum and a necessary tool for learning.
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- The purpose of Internet use in school is to raise educational standards, to enhance other curriculum areas, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Internet access is an entitlement for pupils who show a responsible and mature approach to its use.
- 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 can Internet use benefit education?

- Access to world-wide educational resources including museums and art galleries;
- 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 and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Exchange of curriculum and administration data with the LA and DfES;
- Access to learning wherever and whenever convenient.

How can Internet use enhance learning?

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and will be given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line 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 how to evaluate Internet content

- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the school ICT Manager.
- School should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils will be taught strategies to ensure that they are able to deal with inappropriate Internet content.

Managing Internet Access

Information system security

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- The school uses the Coventry City Council Broadband with its firewall
- The school uses on-site web filter hardware and the council filter covering the entire network.
- The school will provide an additional level of protection through its deployment of Impero in partnership with Coventry City Council's Education and Learning Services (Impero is installed on all school desktops and laptops).
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- The ICT network manager will review system capacity regularly.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Use of words included in the Impero 'banned' list will be detected and logged.
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper. Confidential information must be password protected with the password sent in a separate email.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- Email addresses should be published carefully, to avoid spam harvesting.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The Website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

Publishing staff and pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified by name.
- 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 photographs of pupils are published on the school Website.
- Images of staff should not be published without consent.

Social networking and personal publishing

- Social networking sites and newsgroups will be blocked unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, 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 e.g. house number, street name, school or shopping centre.
- Teachers should be advised not to run social network spaces for students on a personal basis.
- 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.
- Pupils should be advised not to publish specific and detailed private thoughts.
- Schools should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

Managing filtering

- The school will work in partnership with the Coventry City Council to ensure filtering systems are as effective as possible.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school IT Team.
- Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP (addresses later).
- Access to sites that are filtered needs to be requested to the IT team where it will be assessed and either allowed or disallowed.

Managing videoconferencing

- If Microsoft Teams is used it must be with an authorised account linked to the school.
- Staff members have access to a Office 365 A1+ for Faculty account as part of their email account.
- Personal accounts are not to be used to video conference.

Users

- Pupils should ask permission from the supervising teacher before making or answering a video call.
- Video calls should be supervised appropriately for the pupils' age.

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.

Staff

- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Personal Mobile Devices should be turned off or put on silent. It is not permitted to use Personal devices during pupil contact time.
- Under no circumstances should a personal mobile device be used to take photographs or video of pupils, either on-site or off-site such as school trips.

Children

- Children must hand in personal mobile devices to the class teacher at the beginning of the day. They must be turned off as soon as they are in the school grounds and should not be used under any circumstances.
- If any child is found using a personal mobile device, it will be confiscated and the child will not be permitted to bring a personal mobile device into school again.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Staff should be mindful of the Data Protection act when accessing school data including, but not restricted to, SIMS, Online Subscriptions, creation of detail sheets for events or trips and transfer of data via memory stick.

Policy Decisions

Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All users must read and abide by the 'Acceptable ICT Use Policy' before using any school ICT resource.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to read and acknowledge the school's 'Acceptable ICT Use Policy'.

Assessing risks

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor Coventry City Council can accept liability for the material accessed, or any consequences of Internet access.

- The headteacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.
- 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.

Handling e-safety complaints

- Complaints of Internet misuse by pupils will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.

Community use of the Internet

- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

Communications Policy

Introducing the e-safety policy to pupils

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access in EVERY lesson.
- A module on responsible Internet use will be included in the PSHE, Citizenship or ICT programmes covering both school and home use.

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and will have its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- All staff should read and sign the Acceptable ICT Use Policy.

Parents

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school Web site.

Other Policies to be read in conjunction with the E-safety Policy:-

Child Protection & Safeguarding Policy
Remote Learning Policy
Staff Code of Conduct
Acceptable Use of ICT Policy
Data Protection Policy
School Confidentiality Statement