John Randall Primary School and Nursery

Online Safety Policy

The e safety policy is part of the School Development Plan and relates to other policies including those for computing, bullying and for Child Protection.

The school's computing co-ordinator, ICT technician and Head teacher will act as the Online Safety team.

The school Online Safety team, building on the CEOP and government guidance, has written our Online Safety policy. It has been agreed by senior management and approved by governors. The Online Safety policy and its implementation will be reviewed annually.

Teaching and Learning:

Why Internet use is important
The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide children with quality Internet access as part of their learning experience. Internet use is part of the statutory curriculum and necessary tool for staff and pupils.

Pupils will be taught to use Internet to enhance learning
The school Internet access is designed expressly for pupil use and includes filtering of content. Online Safety will be promoted and developed through Key stage assemblies, computing lessons, PSHE and circle times within individual Year groups. With consideration and respect given to the pupils age, ability and developmental stage.
Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Managing Internet Access

Information system security
School ICT systems and usage, including security will be monitored and reviewed regularly by the Online Safety team. Virus protection is updated and monitored regularly by Telford and Wrekin borough council. All use of school computer systems is in accordance with the appropriate usage policy.

Email
Pupils may only use approved e-mail accounts on the school system and e-mail usage should be supervised and monitored by a member of staff.
Pupils must immediately tell a teacher if they receive any 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.
Staff sending e-mails to an external organisation should refer to the appropriate usage policy and the login/responsible use policy.

Published content and the school web site.
The contact details on the Web site should be the schools address, e-mail and telephone number. Staff or pupils' personal information will not be published.
Individual class teachers, the computing co-ordinator and technician, with the support and guidance of the Head teacher, will take editorial responsibility and ensure that content is accurate and appropriate.
Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. Pupil's full names will not be used anyway on the Web site, particularly in association with photographs. Written permission from parents or carers will be obtained for all pupils allowing the school to take photographs for education purposes and celebration on the schools Web site, please see appendix for copy of parent agreement forms.

Pupils' work may be published on the Web site with the acknowledgement of the pupil.

Social networking and personal publishing
The school will block/filter access to social network sites, as soon as knowledge of their existence is reported to the Online Safety team. Newsgroups and forums will be blocked unless a specific use is approved. Pupils will be advised never to give out personal details of any kind that may identify them or their location, as stated in the login/responsible use policy. Pupils and parents will be advised through meetings, parent's evenings and newsletters that the use of social network spaces outside school is inappropriate for primary aged children.
Pupils will complete annually the Child Exploitation and Online Protection Centre (CEOP) questionnaire appropriate for their age and year group. The results will be collaborated, analysed and suitable intervention programmes will be designed to support children in any area of concern highlighted by the questionnaire.

Managing filtering
The schools Online Safety team will work with the LEA and Internet service provider to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover an unsuitable site, it must be reported to the Online Safety team.
The Online Safety team will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies
Emerging technologies will be examined for educational benefit and risk assessment will be carried out before use in school is allowed.
Mobile phones will be left in the school office and are not allowed during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden in accordance with the pupil section within the login/responsible use policy.

Protection personal data
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998

Child Protection / Safeguarding Designated Person / Officer
The designated person is trained in e-safety issues and is aware of the potential for serious child protection / safeguarding issues to arise from:
- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Communication of the policy

Introduction of Online Safety policy to pupils
Online Safety rules will be posted in the ICT suite and discussed with the pupils throughout the computing curriculum in the Digital Literacy strand. Pupils will be informed that network and Internet use can be and will be monitored regularly.
Pupils are responsible for using our digital technology systems in accordance with the pupil acceptable use policy. They should also have;
~ a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
~ need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
~ will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.

~ should understand the importance of adopting good e-safety practice when using digital technologies out of school

Staff and the Online Safety policy
All staff will be given access to the Online Safety policy and a digital copy on the server will be available. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
Staff to be given up to date knowledge of current Online Safety issues ~ apps, social media trends etc

Enlisting parents support
Parent's attention will be drawn to the school Online Safety guidance in newsletters and the school prospectus. A copy of the schools Online Safety policy will be available on the schools Web Site. Internet Safety Day to be brought to parents attention via social media and website with a link to relevant information. Offer parents a contact (computing co-ordinator) to discuss any issues they may have.

Policy decisions

Authorising Internet access
All staff must read and sign a copy of the schools 'Acceptable ICT Use Agreement' before using any ICT equipment or resource. Every time staff and pupils log on to and access schools computers, they must read and click to agree or disagree with the login/reasonable use policy.
The school will keep a record of al staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance, a member of staff may leave or pupils' access be withdrawn.

Assessing risks
The school will take all reasonable precautions to ensure that users access only appropriate materials. However, due to the international scale and linked nature of the Internet content, it is not always possible to guarantee that material may never appear on a school computer. The school cannot accept liability for the materials accessed, or any consequences of Internet access.

Handling Online Safety complaints
A member of the schools management team will deal with complaints of Internet misuse. Any complaints of staff misuse must be reported to the head teacher. Complaints of child protection nature must be dealt within accordance with the child protection policy. Pupils and parents will be informed of the complaints procedure.
If necessary discussions will be held with West Midlands police youth crime reduction officer for advice, guidance or to establish procedures for handling potentially illegal issues.

Policy completed by

Zoe Smith: Computing Co-ordinator

February 2017

Policy Review: February 2018

John Randall Primary School and Nursery

ICT Login and Reasonable use policy

All staff and pupils accessing and attempting to log on to a computer at John Randall Primary must read and agree to the Login and reasonable use policy.
To successfully log on to a computer staff and pupils after entering their personal ID and password staff/pupils must read and click to either agree or disagree to the policy.
There are two versions of this policy, one for members of staff/adults and the second a simplified pupils version. Depending on the type of login ID and password entered into the computer will determine which policy appears.

Staff/adult policy

This computer system is owned by the school. This login and reasonable use policy helps to protect pupils, staff and the school by clearly stating what use of the ICT resources is acceptable and what is not. If any further clarification is required please contact the head teacher or the ICT team at Telford and Wrekin borough council.

- ✓ School computers and Internet connections must be for educational purposes.
- ✓ Network access must be made with your own authorised account and password, which must not be given to any other person. When temporarily leaving the workstation it should be locked (Ctrl-Alt-Del K) to prevent any unauthorised access.
- ✓ All staff are responsible for their own e-mails, which should be written in a responsible and professional manner.

- ✓ Any inappropriate content sent or received will be reported to the ICT services and the Head teacher.
- ✓ Anonymous messages and chain letters/messages are not permitted.
- ✓ Use for personal financial gain, gambling, political or advertising is not permitted.
- ✓ Any attempt to bypass security systems is a serious offence.

The school may exercise its right to monitor the use of all the schools computer systems, including access to web sites, the interception of e-mail and deletion of inappropriate materials where it believes unauthorised and inappropriate use of computers is taking place.

Pupils' policy

- School computers are for school work only and I will ask my teacher if I am unsure what is allowed
- I will only log on to a computer with my own login name and secret password.
- I will only send messages to people I know, or people my class teacher has approved.
- The messages I send will be kind, polite and sensible.
- From time to time I may see things which are unpleasant or I know that are wrong. If I see anything like this I will tell a member of staff as soon as possible.
- I understand that I must never give out my home address or phone number, or arrange to meet someone.
- I will ask permission before opening e-mails or an e-mail attachment sent by someone I do not know.
- I understand that the teachers in school may check my computer files, e-mails and Internet sites that I have visited.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or any school computer.