St. Andrew's C.P. School

Kirk Ella

eSafety Policy

Date of last Review: September 2020
Review in: September 2021 or
sooner if new technology emerges

Kirk Ella St Andrew's CP School
E-Safety Policy

Background

Every school must have an e-safety policy and ours relates to other policies including those for ICT, Positive Behaviour/Anti-bullying and Child Protection.

Our school ICT Co-ordinators, in conjunction with the Head Teacher, will also assume responsibility for e-safety.

Our e-Safety Policy has been written in accordance with the ERYC's Internet Safety Policy which has been adopted by our Governing Body as well as government guidance. It has been agreed by senior management and approved by governors. The E-Safety Policy and its implementation will be reviewed on an annual basis.

Teaching and Learning

The role of internet usage in learning

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 a part of the statutory curriculum and a necessary tool for staff and pupils.

The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection is updated regularly.
- Advice on security strategies will be monitored on the School's ICT web page and clarification sought as necessary.

E-mail

- Pupils may only use approved e-mail accounts on the school system and email usage should be supervised and monitored by a staff member.
- 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.
- Staff should use their school email account and not personal accounts for professional use.
- E-mails sent to an external organisation by pupils should be written carefully and authorised before sending.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully
- Pupils' full names will not be used anywhere on the Website, particularly in association with photographs.
- Permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Pupils will be advised never to give out personal details of any kind that may identify them or their location.
- Pupils and parents will be advised regularly in school newsletters that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing filtering

- The school will work with the LEA, The One Point and the 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 ICT Co-ordinators & Head Teacher.

- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing video conferencing

- Video conferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils will be required to gain permission from the supervising teacher before making or answering a video conference call.
- Video conferencing will be appropriately supervised 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.
- To ensure that abusive or inappropriate text messages are not sent, mobile phones are not allowed in school. If pupils need to bring one to school because it is essential for contact with parent after school sessions, it may be given to one of the Admin staff who will place it in the safe until the end of the day.
- As Kindles cannot be kept safe within school, children cannot bring their home kindles into school.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 (see also our school's Data Protection Policy 2018)

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- The school will keep a record of all 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 a pupil's access be withdrawn.
- For Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.

Assessing risks

- 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. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

Communications Policy

Introducing the e-safety policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and 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.

Enlisting parents' support

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

Date of review of policy: September 2021