Churchill Park Academy

Winston Churchill Drive
King's Lynn
PE30 4RP

E- Safety Policy

Person responsible for the Policy	Headteacher
Date last reviewed	May 2022
Review Date	May 2023
Is this Policy to appear on the school website	Yes

The e-safety Policy is part of the School Development Plan and relates to other policies including ICT, Behaviour, Personal and Social Development and Safeguarding.

The school will appoint an e-Safety Coordinator. This may be the Designated Child Protection Coordinator as the roles overlap.

- Our e-Safety Policy has been written by the school, building on the NCC e-Safety Policy and government guidance. It has been agreed by the senior management and approved by governors.
- The e-Safety Policy and its implementation will be reviewed annually.
- The e safety Policy was approved by the Governors on

Teaching and Learning

- The Internet is an essential element in the 21st century life. The school has a duty to provide students 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 needs of the curriculum.

- 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 online activities that will support the learning outcomes planned for the pupil's 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.

Evaluation of Internet Content

- The school will endeavour to ensure that the copying and subsequent 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.

- The evaluation of online materials is a part of every subject

Information System security

- The school's ICT systems capacity and security will be reviewed regularly

- Virus and Spyware protection will be installed and updated regularly

- Users must take responsibility for their network use. Breaching the Staff Code of Conduct may result in disciplinary action

- All Internet connections must be arranged via the Norfolk County Council Children's services to ensure compliance with the security policy

- Decisions on Wider Area Network (WAN) security are made on a partnership basis between school and NCC.

- Personal data sent over the internet will be encrypted or otherwise secured.

- Portable media may not be used without specific permission followed by a virus scan.

- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.

- The network manager will review system capacity regularly.

E-mail

- Staff and pupils may only use approved email accounts

- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

- 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.

- E-mail will be filtered and monitored by the Network Manager.

Published Content and School Website

- All information published on the school website will already be publicly available and follow Ofsted guidance for school websites.

- Editorial decisions will be made by the Network Manager and the Officer Manager. Any more complex editorial decisions will be referred to a member of the Senior Management Team.

- The school website will be kept updated with pertinent information by the Office Manager and Network Manager.

- Pupil images will only be used on the school website with the permission of their parents/guardians.

Publishing Pupils' Images and Work

- Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

- Pupils' full names will not be used anywhere on the website or blog, particularly in association with photographs

- Written permission from parents or carers will be obtained before images of pupils are electronically published

Social Networking and Personal Publishing

- The school will block access to social networking sites, unless their unblocking is specifically requested by a member of staff to meet clear educational objectives.

- Pupils and staff will be advised never to give out personal details of any kind which may identify themselves or others and /or their location. Examples would include real names, addresses, full names of friends, specific interests etc.

- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary pupils and requires close monitoring with older pupils.

- Pupils will be taught how to use social networks in a safe and responsible way, including how to ensure their safety on social networks, how to find help and how to identify some of the dangers of social networking.

- All users should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.

- If staff become aware of any inappropriate or unsafe contact on social networks by a pupil, they will contact the pupil's parents/guardians and CEOP where appropriate.

- Staff are advised not to be 'friends' with students and ex-students on social networking media such as Facebook.

- All staff at Churchill Park School are directed not to post or store any images of students on their social media accounts.

Cloud Storage

- Some pupil data and images will be stored on the 'cloud' through 2Build a Profile and Classroom Monitor. Staff will ensure that their passwords for Classroom Monitor are kept secure.

- Staff will ensure that 2Build a Profile is only stored on Churchill Park School devices. These devices will have a password in order to open them.

- Whilst Churchill Park School still uses B-Squared Connecting Steps on the 'cloud' staff will ensure that they maintain the security of their passwords and therefore pupil summative assessment data (Connecting Steps is due to be phased out in July 2014).

Managing Filtering

- Churchill Park School will work with the LA, DfE and the Internet Services provider to ensure systems to protect pupils are reviewed and improved.

- Churchill Park School will manage its own filtering through the SWURL system. Filtering control will be devolved to the Network Manager and the Deputy Head Teacher. Whitelists will be reviewed every half-term.

- If staff or pupils discover an unsuitable site, it must be reported to the Network Manager.

- Any material that the school believes is illegal must be reported to appropriate agencies.

Emerging Technologies

- Emerging technologies will be assessed for educational benefit and a risk assessment will be carried out before use in school is allowed

- Pupil mobile phones will be handed into staff teams at the beginning of the day. They will be returned to pupils are the end of the day.

- Staff will be issued with a school phone where contact with pupils is required.

Protecting Personal Data

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

Policy Decisions

- 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 Code of Conduct for ICT’ and read the guidance before using any school ICT resource

- 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 NCC can 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.

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.