Tweedmouth Community

Middle School

Schools e-Safety

Internet Policy Document Created: 25 May 2016

What is the scope of this policy?

This policy is NOT intended to be an exhaustive checklist of appropriate and inappropriate usage of technology in school. It is designed to be as brief as possible to ensure usability while still giving guidelines in usage. The underlying intent and strength in online safety is ensuring that the community, both students and staff, have the training and confidence to use existing and emerging technologies and to deal with any incident that occurs.

Who will write and review the policy?

- 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 Leadership Team and approved by governors and the PT.
- The e-Safety Policy and its implementation will be reviewed annually.
- When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.

Why is Internet use important?

- 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.

How can Internet use enhance learning ?

- The schools will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

How will pupils learn how to evaluate Internet content ?

- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

How will information systems security be maintained ?

- Virus protection will be updated regularly.
- The security of the school information systems and users will be reviewed regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- The school Internet access will be designed to enhance and extend education.

How will e-mail be managed ?

- Pupils may only use approved e-mail accounts.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Whole-class or group email addresses will be used in primary schools for communication outside of the school, controlled by the teacher.

How will published content be managed ?

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.

Can pupil's images or work be published ?

- 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.

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

- The schools will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- 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 e-mail addresses, full names of friends, specific interests and clubs etc.

How will filtering be managed ?

- The school will work with NCC 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 will include filtering appropriate to the age and maturity of pupils.

How will videoconferencing be managed?

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.

How can emerging technologies be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Staff will be issued with a school phone where contact with pupils is required.

How should personal data be protected ?

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

How will Internet access be authorised?

- 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' or Acceptable Use Policy before using any school ICT resource.
- KS2 and KS3 students must apply for Internet access individually by agreeing to comply with the eSafety Rules.

How will risks be assessed ?

- The school should audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.
- The school 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 NCC can accept liability for the material accessed, or any consequences resulting from Internet use.

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.
- All e–Safety complaints and incidents will be recorded by the school — including any actions taken.

How will Cyberbullying be managed ?

- 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 will be clear procedures in place to support anyone affected by Cyberbullying.

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 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.

How will the policy be introduced to pupils?

- An e–Safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.
- All users will be informed that network and Internet use will be monitored.

How will the policy be discussed with staff?

- The e–Safety Policy will be formally provided to and discussed with all members of staff.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use both professionally and personally will be provided.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.

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.

Tweedmouth Community Middle School Declaration

We confirm that this document is the school's official policy on e-Safety.

Headteacher:

Name:

Governor:

Name:

Date:

This document was produced by the e-Safety Policy Document Generator designed for Kent
County Council (KCC) by EIS, Maidstone a business unit of KCC