Tweedmouth West First School

Respect Responsibility Resilience

E-Safety Policy 2020/2021

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 Anti-Bullying, Curriculum, Data Protection and Security.

Good Habits
E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.

- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.

- Safe and secure broadband from the Northumberland Grid for Learning including the effective management of content filtering.

- National Education Network standards and specifications.

School e-Safety Officers
The school has appointed Mrs Robertson and Julie Newton as e-safety officers; Mrs Robertson is also the Designated Safeguarding Lead as the roles overlap.
Julie Newton is the online safety assistant in school.

Why is Internet Use Important?
The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.
Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality internet access
Pupils will use the internet outside school and will need to learn how to evaluate internet information and to take care of their own safety and security.

How does the Internet Use Benefit Education?
Benefits of using the internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;

  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 Local Authority and DCSF;
- 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 includes filtering appropriate to the age of pupils. See 'Safe use of the internet' policy.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support 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.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted internet access.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised internet access.
- Each user will have an individual log in to use the internet
- All internet access is monitored using Futures Cloud software, a weekly report is sent to the headteacher who is alerted to any inappropriate activity.

Unsuitable sites

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Local Authority help desk via the e-safety coordinator.

- School will ensure that the use of internet derived materials by pupils and staff complies with copyright law.

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

Email

- Whole class or group email addresses should be used in school

- Pupils must immediately tell a teacher if they receive an offensive email.

- 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.

- The forwarding of chain letters is not permitted.

Social Networking

- We will only allow access to social networking sites (School Facebook Page) from Mrs hodgson's (School Secretary) school equipment/mobile phone.

Remote Learning

- Children will access the online platform Seesaw to complete work -set by their teacher during a local lockdown/quarantine period or for homework activities
- Children will access this using their own devices at home.

Filtering

- The school will work in partnership with the Local Authority and the Internet Service Provider to ensure filtering systems are as effective as possible.

Video Conferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the internet.

- Videoconferencing will be appropriately supervised for the pupils' age. Google Meet will be used for our virtual assemblies. These are managed in school no outside links are accessed.

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.

- Mobile phones will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Published Content and the School Website

- 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 headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

- Photographs 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 Web site in association with photographs.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

- See 'Safe use of children's photograph's policy'

Information System Security

- School ICT systems capacity and security will be reviewed regularly.

- Virus protection will be installed and updated regularly.

- Security strategies will be discussed with the Local Authority.

Protecting Personal Data

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

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Northumberland County Council can accept liability for the material accessed, or any consequences of internet access.

- 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.

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 headteacher.
- 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.
- Discussions will be held with the Police to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils

- Rules for internet access will regularly be reinforced (i.e. during lessons involving the use of the internet).
- Pupils will be informed that internet use will be monitored.

Staff

- 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.

Parents

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

To be reviewed by the COMPUTING team in September 2021

Key Stage 1

Think then Click

These rules help us to stay safe on the Internet



We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.





We can search the Internet with an adult.

We always ask if we get lost on the Internet.





We can send and open emails together.

We can write polite and friendly emails to people that we know.



Key Stage 2

Think then Click

e-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.

These e-Safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or internet access.
- All network and internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Signed on behalf of the governing body: .....

Date: .....