Swarland E-Safety Policy
"The Best That We Can Be"

What is E-Safety?

E-Safety encompasses the safe use of new technologies, internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. Swarland School's e-safety policy will operate in conjunction with other policies including those for Behaviour, Curriculum, Anti-bullying, Data Protection (GDPR) and Security.

End to End E-Safety

E-Safety at Swarland depends on effective practice at all levels:

- Responsible ICT use by all staff and children; 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 connections including filtering and monitoring.

Writing and reviewing the e-safety policy

The e-Safety Policy relates to other policies including those for ICT, anti bullying, child protection and PSHE.

- The school will appoint an e-safety Co-ordinator who will be the Designated Child Protection Coordinator as the roles overlap.
- Our e-safety policy has been written by the school, building on the Northumberland ICT Advisory Service support team and government guidance. It has been agreed by all staff and approved by governors.
- The e-safety Policy and its implementation will be reviewed biannually.
- The school will maintain an up to date e-safety audit to ensure we are meeting statutory requirements.

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 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.

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include Lightspeed 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.
- 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 will guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

Pupils will be taught how to evaluate Internet content

- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the Head teacher. Pupils can also access the Hectare safe button to block content that upsets them. Staff are then informed to assess the situation.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will 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

- The security of the school information systems are reviewed regularly with advice from NCC Advisory Service.
- Virus protection will be updated regularly.
- Security strategies will are discussed and reviewed with the County technician and Northumberland Grid for Learning.

E-mail

- Pupils may only use approved e-mail accounts on the school system using NORTLE.
- 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.
- E-mail sent to an external organisation should be written carefully and authorised by a member of staff before sending.
- The forwarding of chain letters is not permitted.
- Pupils have been advised to only open attachments from known and safe sources or to check with the teacher if in doubt.

Published content and the school website

- The contact details on the website are 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 and will not enable individual pupils to be clearly identified by name.
- 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 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 information of any kind that may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school IM address, e-mail address, names of friends, specific interests and clubs etc.
- Pupils and parents will be advised of the possible risks that the use of social network spaces outside school, primary aged pupils can be exposed to.

Managing filtering

- The school will work with the LA, DfE 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 an adult, who will inform the e-Safety Coordinator. The e-safety lead will then record the e-safety incident following procedures set out in the appendix flowchart.
- Northumberland IT Support, the ICT technician and ICT Co-ordinator 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 before use in school is allowed.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations 2018.

Policy Decisions

Authorising internet access

- All staff must read and sign the "Acceptable Use Agreement" before using any school ICT resource. They will be required to sign it on an annual basis.
- The school will keep a record of all staff and pupils who are granted Internet access with Lightspeed logins. The record will be kept up to date, for instance a member of staff may leave or a pupils access be withdrawn.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- At Key Stage 2, access should be restricted to websites identified in teachers planning and be supervised by an adult.

Assessing risks

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. 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 Head teacher will ensure that the e-Safety Policy is implemented, an e-safety audit is carried out annually and compliance with the policy monitored.
- Pupils will be taught when and how to use HECTAR should they find something upsetting on screen or report a concern via School 360.
- Parents as well as children will receive e-safety training. Children will have e-safety delivered through part of their broad and balanced curriculum. Parental workshops to be offered biannually with further information or guidance given on the school website.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff/head teacher.
- 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 the school child protection procedures.
- Any incident of cyber bullying will be dealt with following procedures in the Anti-Bullying Policy and Behaviour Policy.
- Any breech of the Acceptable Use Policy by children will be dealt with using our Behaviour Policy.
- Any breech of the Acceptable Use Policy by adults will be dealt with using the staff Disciplinary Policy and Code Of Conduct Policy.

Community use of the Internet

- The school will advise members of the community using the schools Internet that they will need to abide by the school e-safety rules as displayed in the suite. Any misuse and they will have access withdrawn. All visitors will need to receive an individual login from the Headteacher to access Lightspeed and monitor their activity.

Communications Policy

Introducing the e-safety policy to all pupils

- E-safety rules will be posted in the ICT suite and discussed with the pupils as appropriate.
- An E-Safety curriculum will be embedded to raise the awareness and importance of safe and responsible internet use.
- Any breach of the acceptable use policy will be dealt with according to our code of conduct behaviour policy.

Staff and the e-Safety policy

- All staff will be made aware of the School e-Safety Policy and its importance explained. A copy of reporting an e-safety incident will be available in the policy file and displayed in the staff room.
- Staff have signed up to an Acceptable Use Policy, Code of Conduct and Social Networking Policy.
- 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 links on the school website.
- Adults working with pupils using the Internet will be made aware of the School e-Safety Policy.

This policy is to be read alongside our
Disciplinary Policy
Code of Conduct Policy
Social Networking Policy
Anti-bullying Policy
Whistle blowing policy
Internet User Policy
Acceptable Use Policy
Behaviour Policy.
GDPR policy

Some useful links on e-Safety awareness can also be found on our website.

Revision Record of Issued Versions			
Author	**Creation Date**	**Version**	**Status**
Louise Fletcher	9.7.14	1.0	Final version for publication
Changed by	**Revision Date**		
School	17.11.15	2.0	Draft adapted version for consultation with staff and Governors. Revisions regarding links to Anti-Bullying and Behaviour Policy.
School	18.11.15	3.0	Final version for publication
	19.7.16	3.0	Reviewed with primary status amendments.
	19.9.18	3.1	Reference updates to GDPR 2018.