Discovery Schools Academy Trust

Greystoke Primary School

Enabling our children to reach their full potential

E –safety Policy

This Policy has been formally adopted by the Governing Body of Greystoke Primary School. It will be reviewed by the Governors, the Head Teacher and the staff every year from the date of the signature below.

Signed……Date……

Chair of Governors

1.Introduction

Greystoke Primary School recognises the Internet and other digital technologies provide a good opportunity for children and young people to learn. These new technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.

1.1 As part of our commitment to learning and achievement we at Greystoke Primary School want to ensure that new technologies are used to:

- Raise standards.
- Develop the curriculum and make learning exciting and purposeful.
- Enable pupils to learn in a way that ensures their safety and security.
- Enhance and enrich their lives and understanding.

1.2 We are committed to an equitable learning experience for all pupils using ICT technology and we recognise that ICT can give disabled pupils increased access to the curriculum to enhance their learning.

1.3 We are committed to ensuring that **all** pupils will be able to use new technologies safely. We are also committed to ensuring that all those who work with children and young people, as well as their parents, are informed about the risks that exist so that they can take an active part in safeguarding children.

1.4 The nominated senior person for the implementation of the School's e-Safety policy is Mr Andrew Hayes, Assistant Head Teacher.

2. Scope of Policy

2.1 The policy applies to:

- all pupils;
- all teaching and support staff (including peripatetic), school governors and volunteers;
- all aspects of the School's facilities where they are used by voluntary, statutory or community organisations.

2.2 Greystoke Primary School will ensure that the following elements are in place as part of its safeguarding responsibilities to pupils:

- a list of authorised persons who have various responsibilities for E-safety;
- a range of policies including acceptable use policies that are frequently reviewed and updated;
- information to parents that highlights safe practice for children and young people when using new technologies;
- audit and training for all staff and volunteers;

- close supervision of pupils when using new technologies;
- education that is aimed at ensuring safe and responsible use of new technologies;
- a monitoring and reporting procedure for abuse and misuse.

3. Teaching and learning

3.1 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.

3.2 Internet use will enhance learning

The school Internet access will be designed expressly for pupil use and will include 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

3.3 Pupils will be taught how to evaluate Internet content

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.

4. Managing Internet Access

4.1 Information system security

School ICT systems capacity and security will be reviewed regularly.

Virus protection will be updated regularly.

4.2 E-mail

Pupils may only use approved e-mail accounts on the school system.

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 before sending, in the same way as a letter written on school headed paper.

The forwarding of chain letters is not permitted.

4.3 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 headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

4.4 Publishing pupil's 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 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 Website or Twitter feed by way of signed Media Agreement.

Pupil's work can only be published with the permission of the pupil and parents.

4.5 Social networking and personal publishing

The school 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 or their location.

Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

4.6 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 the ICT Coordinator.

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

4.7 Managing videoconferencing

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

Pupils should ask permission from the supervising teacher before making or answering a videoconference call.

Videoconferencing & Skype will be appropriately supervised for the pupils' age.

Skype will be managed by the supervising adult who will connect using a protected password.

Use of video for teaching purposes; i.e.; IRiS – agreement is sought from the parents where media agreements have not been signed or where the material will be made public.

4.8 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.

4.9 Protecting personal data

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

5. Policy Decisions

5.1 Authorising Internet access

All staff, visitors, governors and trainees must read and sign the 'Acceptable Use of ICT Agreement' before using any school ICT resource.

The school will keep a record of all persons 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.

At 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 the pupil's acceptable use of ICT policy.

5.2 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 Discovery Schools Teaching Trust 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.

5.3 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 can use the complaints procedure.

6. Communications

6.1 Introducing the e-safety policy to pupils

E-safety will be taught at the beginning of each unit of work and displays will support the teaching.

Pupils will be informed that network and Internet use will be monitored.

6.2 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.

6.3 Enlisting parents' support

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

7.1.Review and monitoring

The e-Safety Policy and its implementation will be reviewed annually.

The policy will be monitored by the Senior Leadership Team and Advisory Board.