BURROUGH GREEN CofE PRIMARY SCHOOL
E-SAFETY Policy

The e-safety policy that follows explains how we intend to provide the necessary safeguards to help ensure everything that can reasonably be expected of us to manage and reduce risks associated with the use of new technologies.

1. Writing and reviewing the E-Safety policy

The e-Safety Policy relates to other policies including those for Positive Behaviour (incorporating anti-bullying), Acceptable Use and for Child Protection.

- Our E-Safety Policy has been written by the school, building on the Cambridgeshire E-Safety and government guidance. It has been agreed by staff and approved by governors.
- The E-Safety co-ordinator is: Esther Street.
- The Designated Safeguarding Lead for Child Protection is Keith Archer.
- The E-Safety Policy and its implementation will be reviewed every three years.
- The E-Safety Policy was revised by: Keith Archer and Esther Street.

2 Teaching and learning

2.1 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.

2.2 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. This is provided across the county by E2BN. All pupil laptops are set to the primary filter. Staff laptops will be set to the staff filter.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge, location, retrieval and evaluation.

2.3 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 aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught how to recognise unsuitable material and bring this to the attention of a trusted adult, usually the class teacher when in school.

2.4 Pupils will be taught about the dangers of the Internet

- Pupil will learn about cyberbullying. How to recognise, report and avoid it, as well as their social responsibility to act on seeing another being cyberbullied.
- Pupils will be made aware of inappropriate or dangerous online relationships and how to report any communications which they are uncomfortable about.
- Pupils will be made aware of sites that promote extreme views which do not value people with different beliefs and cultures, and to report these to the E-Safety Coordinator.
- The forwarding of chain letters is not permitted within our school.

- Pupils or their parents should inform the school as soon as possible if they or their child has received 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.

- Pupils will be given sites where they can seek further information and report inappropriate behaviour from home (CEOP)

3 Managing Internet Access

3.1 Information system security

- School ICT system's capacity and security will be reviewed regularly.
- Virus protection is updated regularly. All computers use the anti-virus protection by Sophos.

3.2 Published content and the school web site

- The contact details on the website should be 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.

3.3 Publishing pupil's images and work (see also Acceptable Use Policy)

- Photographs that include pupils will be selected carefully and will not have a pupil's name published with it.
- Pupils' full names will not be used anywhere on the website or on Twitter, 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.
- Pupil's work can only be published with the permission of the pupil and parents which will form part of a content form sent home to parents.

3.4 Social networking and personal publishing

- The E2BN filter will block access to ALL social networking sites. Staff alone have access to the school Twitter account.
- 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. Parents to be informed that the legal age for pupils to use social networking sites is 13 years old.

3.5 Managing filtering

- The school will work with the E2BN to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Coordinator.
- If children find an unsuitable internet site they will be encouraged to tell an adult immediately and the adult will pass this information on to the E-Safety Coordinator.
- The EdIT team will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

3.6 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 during lessons or formal school time, unless used to take and post images for the school's Twitter account. Any images must be deleted from the user's phone immediately once the image has been posted (see Acceptable Use Policy). The sending of abusive or inappropriate text messages is forbidden.
- Staff will be issued with a school phone where contact with parents is required.

4 Policy Decisions

4.1 Authorising Internet access

- All staff must read and sign the 'Acceptable Use Agreement' before using any school IT resource.
- All teaching staff will be informed of any child for whom internet access has been withdrawn, or children whose parents wish them not to use the internet.
- 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 and return a consent form.

4.2 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. Neither the school nor E2BN can accept liability for the material accessed, or any consequences of Internet access.

4.3 Reporting of E-safety concerns and complaints.

- The E-Safety Co-ordinator will keep a log of any known 'extreme' or 'unusual' actions that a pupil may be undertaking online.
- Concerns of a child protection nature must be dealt with in accordance with school child protection procedures. Any concerns must be passed on to the Designated Safeguarding Lead for Child Protection immediately.
- Pupils or parents may wish to raise concerns about internet/email use which should be passed on to the E-Safety Coordinator who may also share these with the Headteacher. Staff will determine the most appropriate course of action which may follow procedures laid down in related policies e.g. Disciplinary Procedure, Acceptable Use Policy, Positive Behaviour Policy. The person raising the concern will be informed of the proposed course of action.

5 Informing staff and pupils of E-safety policy

5.1 Introducing the E-safety policy to pupils

- Pupils will be informed that network and Internet use will be monitored.
- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year and reminded regularly during ICT sessions.
- Rules relating to safe use of the internet will be discussed with pupils at the start of every term.

5.2 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.

5.3 Enlisting parents' support

- Parents' attention will be drawn to the School E-Safety Policy in newsletters, the school prospectus and on the school Web site.
- A dedicated area of the school website will be given to E-safety, with tips and advice about E-safety for parents and pupils. A link is provided to the CEOP website for this purpose.

6 Disposal of ICT Equipment

- All hard drives on Computers/Laptops will be destroyed so as to prevent confidential data entering the public domain.

Policy was reviewed: Autumn 2015

Policy Ratified by Governors Health and Well-Being Committee: 25th January 2016

Next review: Autumn 2018