Boxgrove Lane, Guildford, Surrey GU1 2TD
Interim Co-Headteachers: Mrs Alison Fitch BA (Hons) QTS
                             Mrs Rebecca Stacey BA (Hons) QTS

e-Safety Policy

The E-safety Policy relates to other policies including those for Anti-bullying, PSHEC and for Child Protection and Safeguarding.

Aims and objectives

Technology is embedded in every classroom and innovative use of new technologies has the capacity to inspire and scaffold learning, motivate learners and create opportunities to support and challenge at all levels. However, technology must be used safely, securely and responsibly to protect all members of our community. The measures and procedures detailed within this policy allow children and adults to use, learn through and enjoy technology in a safe environment.

Teaching and learning

Why Internet and digital communications are 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 Computing experiences as part of their learning.
- ➢ The school Internet access is provided by Surrey County Council through the Unicorn contract and includes filtering appropriate to the age of pupils.
- ➢ Pupils are taught what Internet use is acceptable and what is not and are given clear objectives for Internet use.
- ➢ Pupils are educated in safe searching when using the Internet, and will be directed to safe and age appropriate digital resources.
- ➢ Pupils are shown how to publish and present information appropriately to a wider audience.
- ➢ Pupils are taught how to use online communication tools effectively and safely.

Pupils will be taught how to evaluate Internet content

- ➢ The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- ➢ Where possible, pupils are encouraged to verify the information they find online with other sources, e.g. books
- ➢ Pupils will be taught how to report content that concerns them to a member of teaching staff.

Managing Internet Access

Information system security

- ➢ School Computer systems security is reviewed regularly.
- ➢ Virus protection is updated regularly.
- ➢ Security strategies are discussed with the Local Authority.

E-mail

- ➢ Pupils and staff may only use approved e-mail accounts on the school system. (@boxgrove.surrey.sch.uk)
- ➢ Incoming e-mail, where the author is unknown, will be treated as suspicious and attachments not opened.

Published content and the school website

- ➢ 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 Headteacher has overall editorial responsibility and ensures that content is accurate and appropriate.

Publishing pupils' images and work

- ➢ Written permission from parents or carers is obtained before photographs of pupils are published on the school Website.
- ➢ Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. The school will look to seek to use group photographs rather than full-face photos of individual children.
- ➢ Pupils' full names will not be used on the school website, particularly in association with photographs.
- ➢ ***Parents are clearly informed of the school policy on image taking and publishing.***

Managing filtering

- ➢ The school works in partnership with Surrey County Council to ensure systems to protect pupils are reviewed and improved.
- ➢ If staff or pupils come across unsuitable on-line materials, the site must be reported to the E-safety Coordinator (Peter Wright).
- ➢ Staff will ensure that regular checks are made so that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

- ➢ Videoconferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.
- ➢ Videoconferencing will only take place through appropriate teacher supervision.

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 and associated cameras will not be used during lessons or formal school time.
- ➢ Staff will use a school phone where contact with parents or pupils is required.

Protecting personal data

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

Policy Decisions

Authorising Internet access

➢ All staff must read and sign the 'Boxgrove Staff Acceptable Use Policy' before using any school Computing resource. This is presented at annual Inset days and to other staff individually if they join the staff team mid academic year.

➢ The school will maintain a current record of all staff and pupils who are not granted access to school Computing systems.

➢ Teaching staff demonstrate effective use of the internet and access to the Internet is by direct adult supervision using approved on-line materials.

➢ Parents will be asked to sign and return an internet consent form.

➢ Any person not directly employed by the school will be asked to sign an 'Boxgrove Staff Acceptable Use Policy' before being allowed to access the Internet from the school site.

Assessing risks

➢ The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the nature of the internet, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor GEP can accept liability for the material accessed, or any consequences of Internet access.

The school audits Computing use and emergence of new technologies to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective.

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.

➢ Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet

➢ All use of the school Internet connection by community and other organisations shall be in accordance with the school E-safety policy.

Sanctions and disciplinary measures

➢ Children who do not adhere to the e-safety policy, through inappropriate use of software or hardware, will be prohibited from using the equipment for a period of time, at the discretion of the Computing Coordinator and senior staff.

- ➢ In the event of an adult not adhering to the e-safety Policy, through inappropriate use of software, hardware, internet browsing or sensitive data stored on any device, an immediate meeting will be held with the individual(s), the Computing Coordinator and the Headteacher. This meeting will ascertain the severity of the misdemeanour before cautions or sanctions can be put in place.

- ➢ The inappropriate use of software, hardware, internet browsing or sensitive data by an adult, could result in the termination of the adult's contract, with the school, and criminal proceedings.

Communications Policy

Introducing the E-safety policy to pupils

- ➢ Appropriate elements of the E-safety policy are shared with pupils.
- ➢ E-safety rules are posted in all school learning areas where the internet is accessed.
- ➢ Pupils are informed that network and Internet use will be monitored.
- ➢ The school uses the Surrey E-safety scheme of work in order to teach children about relevant E-safety issues and instil a set of safe behaviours when accessing the internet. E-safety lessons are taught regularly throughout the school and links to the PSHE policy.

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.
- ➢ Staff that manage filtering systems or monitor Computing use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' support

- ➢ ***Parents' and carers' attention will be drawn to the School E-safety Policy.***
- ➢ On an annual basis, the school will hold E-safety information sessions for parents and carers to attend. At other events, a rolling presentation of information and resources about keeping children safe online will be shown, e.g. at parents' evenings and information evenings.
- ➢ The school will maintain a list of recommended E-safety resources for parents/carers to use in reinforcing messages of online safety outside of school.
- ➢ The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.