Otterham Primary School

E-Safety Policy

January 2016

E-Safety Policy

E-Safety encompasses **Internet technologies** and **electronic communications**, including handheld devices. This policy highlights the need to educate pupils about the benefits and risks of using technology, and provides safeguarding and awareness for users to enable them to control their online experience.

Otterham School has a designated e-Safety Coordinator (Claire Humber), who also works closely with Lin Caudle (child protection officer), as well as the link ICT governor, Julian Elson. Our School's e-Safety Policy reflects the need to raise awareness of the safety issues associated with electronic communications as a whole and operates in conjunction with other school policies, including those for ICT, behaviour, bullying, PSHE and safe guarding, child protection. E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; 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 internet provision by South West Grid for Learning (SWGfL).

TEACHING & LEARNING

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. The purpose of Internet use in school is to raise educational standards, to promote all pupil achievement, to support the professional work of staff and to enhance the school's management functions. Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Benefits of using the Internet in education include:

- Access to world-wide educational resources;
- Educational and cultural exchanges between pupils world-wide;
- Cultural, vocational, social and leisure use in libraries, clubs and at home;
- Collaboration across support services, professional associations and between colleagues, including the access of administration data;
- Access to technical support, including remote management of networks and automatic system updates;

Planning

Teacher planning ensures there are clear objectives for Internet use and that activities enrich and extend learning. All staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and ability. Specific PHSE and computing lessons will ensure pupils are made aware of potential risks online and ways in which they can keep themselves and others safe.

Learning

- Pupils are regularly reminded of potential dangers online and taught ways in which to stay safe.
- 'Think before clicking' – these key stage appropriate rules are shared with each class and displayed on each class' lapsafe as a reminder.
- Staying safe – Pupils are taught to follow 'SMART' rules when online: Safety, Meeting others, Accepting messages and files, Reliability, Telling an adult.

- Social Networking - Although Otterham School blocks access to all social networking sites, both pupils and staff are reminded of ways in which to keep safe if using these at home. For instance, pupils will be advised never to give out any personal details or upload personal photos. Similarly pupils and staff are advised on security (including setting appropriate passwords), how to deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

Misuse and Complaints

Any complaint about staff or pupil misuse must be referred to the Headteacher. Pupils and parents will be informed of the complaints procedure (see complaints procedure).

Filters

The school Internet access will include filtering of some material, including social media sites. It is the responsibility of all staff to check that the filtering methods selected are appropriate, effective and reasonable. Pupils will be taught what is/ is not acceptable, using the 'Thing before clicking' rules. If staff or pupils discover unsuitable sites, they are taught to alert an adult who will report it to the Internet Service Provider (TME).

Copyright Law

The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law. Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

MANAGING INFORMATION SERVICES

The school ICT systems will be reviewed regularly with regard to security. Virus protection are installed and updated regularly. Use of data storage facilities by pupils within school is prohibited to protect against virus transfer. Personal staff and pupil passwords are used to ensure tight security.

E-mails

Each class has access to their own school-based email account, which is specific to their own login. Children are able to send emails when supervised by an adult (refer to think before clicking rules).

Published content and the school's website

The point of contact on the school's website will be the school address, school e-mail and telephone number. The School Secretary will take overall editorial responsibility and ensure content is accurate and appropriate. Both staff and pupils' personal information will not be published and images which include pupils will be carefully selected so that only those with parental permission will be identifiable. Pupils' full names will not be used on the website when associated with photographs or school work, or in any way which may be to the detriment of pupils. Pupil photographs will immediately be removed from the school website upon request from parents, or other appropriate request.

Emerging technologies and mobile phones

Emerging technologies will be examined for educational benefit. Mobile phones will not be used during lessons or formal school time.

Videoconferencing

Videoconferencing should be supervised appropriately for the pupils' age with parental permission sought before children partake in videoconferences. Only key administrators will be given access to the videoconferencing system, web or other remote control page and unique log-in/ password details kept secure. Equally, recorded material will be stored securely.

Videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet. All videoconferencing equipment in the classroom must be switched off when not in use and external IP addresses should not be made available to other sites. Videoconferencing contact information will not be put on the school website.

COMMUNICATIONS POLICY

The parent and pupil agreement is reviewed yearly and is separated into key stage rules ('Think Before Clicking'). These rules are displayed near all computer systems in the classrooms and reinforced regularly in lessons.

Parents/carers' attention will be drawn to the School e-safety Policy in newsletters, which is on the school website. Parents/carers also have the opportunity to attend an open afternoon so they can be briefed about e-safety, thus ensuring they are vigilant at home too.

All staff will follow and apply the school e-safety Policy as discretion and professional conduct is essential. Staff training about safe and responsible Internet use will be provided as required, with reference made to the e-safety policy.

The policy has been agreed by the leadership team and approved by the Governing Body. It will be reviewed regularly. Changes will be made immediately if technological or other developments so require.

Policy Statements

Education – Pupils

E-Safety education will be provided in the following ways:

- A planned e-safety programme is provided as part of ICT / PHSE/ other lessons and is regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities, including annual involvement National E-Safety Day
- Pupils should be taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be helped to understand the need for the pupil Acceptable Use Policies and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet will be posted in all class rooms

- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – Parents / Carers

The school will provide information and awareness to parents and carers through:

- Letters, newsletters, website
- An open afternoon
- Reference to the appropriate websites

Education & Training – Staff

Staff training will be offered as follows:

- Regular E-Safety training will be made available to staff
- New staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies (AUP)
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days
- The E-Safety Coordinator will provide advice / guidance / training as required to individuals as required

Training – Governors

Governors will be invited to take part in e-safety training sessions, with particular importance for those who are members of the E-Safety committee and child protection.

Agreed by:
Ratified by Governors on:
Date for review: