



## **E-Safety Policy**

### **Vision**

ICT in the 21<sup>st</sup> Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Owler Brook Primary School we understand the responsibility to educate our pupils on e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, webcams, whiteboards, digital video equipment etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

### **Aims**

We aim to ensure that all pupils are kept safe when using any form of ICT.

### **e-Safety skills development for staff**

- Our staff will receive information and training on e-Safety issues through the coordinator at staff meetings.
- All staff will be made aware of their responsibilities relating to the safeguarding of children within the context of e- Safety and know what to do in the event of misuse of technology by any member of the school community report to one of the above working party members.
- New staff receive information on the school's acceptable use policy as part of their induction.
- All staff are encouraged to incorporate e-Safety activities and awareness within their lessons.

### **Managing the school e-Safety messages**

- We endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-safety policy will be introduced to the pupils on a regular basis.
- E-safety posters will be prominently displayed.
- E-safety information is available on the school website.

### **e-Safety in the Curriculum**

- The school provides opportunities within a range of curriculum areas to teach about e-Safety.
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.

- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button.

### **e-Safety information for parents/carers**

- The school will send out relevant e-safety information for parents/carers through newsletters and the school prospectus.
- The school website contains useful information and links to sites like Thinkuknow, Childline, YHdFL parents' page and the CBBC Dingle the rabbit safety page.
- The school will offer information sessions for parents/carers.

### **Password Security**

- All users must read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety policy. This includes teaching and non-teaching staff as well as school Governors.
- Adult users are provided with an individual network and email. (Also Learning Platform log-in username in future.)
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- If you think your password may have been compromised or someone else has become aware of your password report this to Jo Farrell, Office Manager.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems/ SIMs.net (and/or Learning Platform,) including ensuring that passwords are not shared.
- In our school, all ICT password policies are the responsibility of Jo Farrell and all staff and pupils are expected to comply with the policies at all times.

### **Managing the Internet**

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the Yorkshire & Humberside Grid for Learning (YHGfL) is logged and the logs are randomly but regularly monitored. Whenever any

inappropriate use is detected it will be followed up.

The school maintains students will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology.

- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils. The use of google should be avoided as it is an adult search engine and the results may not be suitable. You could direct them to search engines specifically designed for children and young people. For instance [www.bbc.co.uk/cbbc/find](http://www.bbc.co.uk/cbbc/find) can be used with younger pupils, or for older pupils BBC Search (<http://search.bbc.co.uk>), Ask Kids ([www.askkids.com](http://www.askkids.com)) and Yahoo Kids (<http://kids.yahoo.com>) are alternatives, which also provide image search facilities.
  - Hector (screen blocker) is used on all PCs for children to use if inappropriate images get through the firewall.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

### **E-mail**

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive any 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.

### **Publishing pupil's images and work**

- Written permission from parents or carers will be obtained before photographs of pupils are

published on the school web site.

- Pupils' names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Parents will be asked for consent when photographs are to be used or taken by the press because their circulation and coverage may be local, national and sometimes international.
- Pupil's work can only be published with the permission of the pupil and parents and will not enable them to be individually identified.

### **Photographs taken by parents/carers for personal use**

In the event of parents/carers wanting to take photographs for their own personal use the school will demonstrate their protective ethos by announcing that photographs taken are for private retention and not for publication in any manner including use on personal websites (e.g. school plays).

### **Social networking and personal publishing**

- The school will block/filter access to social networking sites.
- 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.
- School staff should not add children as 'friends' if they use these sites.  
(Staff Code of Conduct)

### **Community use of the Internet**

- The school will liaise with local organisations / Children's Centre to establish a common approach to e-safety, for example if it is used for adult or family learning courses.
- The after school clubs will be required to follow the school's e-safety policy and staff must sign the acceptable use agreement.

### **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 Sheffield City Council can 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 its implementation is effective.

Sept 15

Review Sept 15

### **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 senior member of staff.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

### **Roles and Responsibilities**

All staff within school have a responsibility for e-Safety. This will be monitored by the members of the ICT working party: Sue Bridges, Laura Wardell and Jakki Rhodes.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home-school agreements, and behaviour (including the anti-bullying) policy and PHSE.

### **Review**

Date: Sept 14

Date for review: Sept 15