



## **INTERNET SAFETY POLICY**

### **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.

### **Internet use for pupils**

- 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
- 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.
- The school has an e safety policy created by pupils and this is on display in all classrooms and has been shared in assembly.

### **Managing Internet Access**

School ICT systems capacity and security will be reviewed regularly.  
Virus protection will be updated regularly.

### **E mails by children**

- An 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.

### **School web site**

- The Executive Head teacher and Head of School will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Pupils' full names will not be used anywhere on the Web site particularly in association with photographs. Parents are informed of the school website; they are given the opportunity to request their child's pictures not to be shown.

### **Safety Guidelines**

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- 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. If staff or pupils discover an unsuitable site, it must be reported to the ICT leader who is the e safety leader.

- The school recommends children use search engines which are child friendly. Searching using google (including images) is not advised for younger pupils. Also You Tube will not be used by pupils independently — unless the video clips have been selected/checked by the teacher first.

### **Use of the internet in after school club**

Pupils in after school club will be supervised at all times when in the ICT Suite. They may use Word or 2 Simple programmes. The children will be restricted to the following websites only:

- espresso/Discovery education
- BBC Bitesize
- Mathletics
- [thinkuknow.co.uk](http://thinkuknow.co.uk) (internet safety)

### **Enlisting Parent's Support**

Parents' attention will be drawn to the School e-Safety Policy in newsletters, and conversations.

If using the internet at home:

- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils must be made aware of how they can report abuse and who they should report abuse to.
- Pupils should be taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future.
- Pupils should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications.
- Pupils should only invite known friends and deny access to others.

### **How will Cyberbullying be managed?**

- Cyberbullying is defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007.
- It is essential that pupils, staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse.
- Promoting a culture of confident users will support innovation and safety. DCSF and Childnet have produced resources and guidance that will be used to give practical advice and guidance on cyberbullying: <http://www.digizen.org/cyberbullying>
- Cyberbullying (along with all forms of bullying) will not be tolerated in school. All incidents of cyberbullying reported to the school will be recorded.
- There are clear procedures in place to investigate incidents or allegations of bullying:
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify bullying behaviour, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Sanctions for those involved in Cyberbullying may include: The perpetrator will be asked to remove any material deemed to be inappropriate or offensive, a service provider may be contacted to remove content, Internet access may be suspended at school for the user for a period of time, parent/carers will be informed and the Police will be contacted if a criminal offence is suspected.

### **Other E-safety Issues**

**Sexting** — Children in Year 5 and 6 will be informed about the implications of sexting and how, once a picture has been sent, this image can never fully be removed from the world wide web.

**Pornography** — many children will come across some type of pornographic content when searching the Internet. Children are taught about what to do if they come across this type of material and who to speak to.

### **Handling e-safety complaints**

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

### **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 should not be using the internet for purposes other than school related, during the working day.

### **Social networking**

The following guidance on social networking is provided to protect members of staff:

Do NOT accept pupils as a friend on Facebook or any other social networking site (this also includes past pupils who are under the age of 18).

Do NOT accept parents on Facebook or any other social networking site (if you already have a close friend on Facebook who is also a parent please notify the e-safety leader and make this known).

Comments relating to school or their working lives should not be made on any social networking site.

Please be advised that if you have named the school as your workplace on any social networking site, **ANY** personal comment you make is a reflection of you as a professional.

If a member of staff has a social network account it is imperative that they regularly complete a privacy check.

If a message is received electronically from a parent or pupil please inform the e safety leader.

Staff need to be aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. Examples include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.

**e-safety leader: Mr D O'Regan**

**Policy updated: September 2015**