Oakfield House School

E-Safety Policy

Policy Document
(2014-2015)

Updated:	**September 2014**
Review date:	**September 2015**
Signed by:	

C O N T E N T S

Page

1. Introduction

The Green Paper '*Every Child Matters* and the provisions of the *Children Act 2004 Working Together to Safeguard Children* sets out how organisations and individuals should work together to safeguard and promote the welfare of children.
The 'staying safe' outcome includes aims that children and young people are:

· safe from maltreatment, neglect, violence and sexual exploitation
· safe from accidental injury and death
· safe from bullying and discrimination
· safe from crime and anti-social behaviour in and out of school
· secure, stable and cared for.

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.
This Policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks
Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective eSafety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.
Our eSafety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our pupils are prepared to deal with the safety challenges that the use of technology brings.
The e-Safety Policy relates to other policies including those for safeguarding, ICT, bullying and for child protection. It is been agreed by senior management and approved by Acorn Care and Education

· The school's e-Safety Coordinator is Ms Angela Clark

· The designated senior person for Child Protection is Ms Paula Kitching

2. Teaching and learning

2.1 Why the 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 pupils 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. ICT will be used across the school to enhance and extend learning, to engage in interesting and vibrant learning activities and to empower learners so that they play a more active role in managing their own learning experiences.

2.2 Internet use will enhance learning

The school's 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

Pupils will be shown how to publish and present information to a wider audience.

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 will be taught the importance of cross-checking information before accepting its accuracy.

Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or Hector Protector.

3 Managing Information Systems

3.1 Information system security

School ICT systems security will be reviewed regularly.

Virus protection will be updated regularly.

Security strategies will be discussed with the Local Authority. 3

3.2 E-mail
Pupils may only use approved e-mail accounts on the school system.
Pupils must immediately tell a teacher if they receive offensive e-mail.
In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
The forwarding of chain letters is not permitted.
Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
The school will consider how e-mail from pupils to external bodies is presented and controlled.
3.3 Published content and the school web site
The contact details given on the Web site will be the school address, e-mail and telephone number. Staff or pupil personal contact information will not be published.
The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
3.4 Publishing pupil's images and work
Written permission will be sought from parent/carers before photographs of pupils are published on the school web site.
Pupils' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.
Work can only be published with the permission of the pupil and parents/carers.
Pupil image file names will not refer to the pupil by name.
Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.
3.5 Social networking and personal publishing
Social Network sites and newsgroups will be filtered unless a specific use is approved.
Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for children and young people. 4

3.6 Managing filtering

The school will work with appropriate agencies and partners 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.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

3.7 Managing videoconferencing & webcam use

Pupils must ask permission from the supervising teacher before making or answering a videoconference call.

Videoconferencing and webcam use will be appropriately supervised for the pupils' age.

3.8 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.

The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Mobile phones are not permitted to be used in school useless agreed with the Head or the Deputy Head Teacher. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden and pupils are expected to hand in their phones on arrival to school.

The use by pupils of cameras in mobile phones will be kept under review.

Games machines including the Sony Play station, Microsoft Xbox and others have Internet access which may not include filtering. Staff will supervise pupils who access the internet via such devices.

The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

3.9 Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. 5

4 Policy Decisions

4.1 Authorising Internet Access

All staff must read and sign the Acceptable Use Policy for ICT before using any school ICT resource.

All pupils must read and sign the Acceptable Use Policy for ICT before using any school ICT resource. Parents will be asked to sign and return a consent form.

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

Any person not directly employed by the school will be asked to sign an acceptable use of school ICT resources before being allowed to access the internet from the school site.

4.2 Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. The school can not accept liability for any material accessed, or any consequences of Internet access.

The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

4.3 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 SLT

Complaints of a child protection nature must be dealt with in accordance with the school's child protection procedures.

Pupils and parents are informed of the complaints procedure.

Pupils and parents will be informed of consequences for pupils misusing the Internet. This may include the loss of internet privelges. 6

5 Communications Policy

5.1 Introducing the e-safety policy to pupils

E-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.

Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

A programme of training in e-Safety will be developed.

E-Safety training will be embedded within the ICT scheme of work and the PSHCE curriculum.

5.2 Staff and the e-Safety policy

All staff will be given the School e-Safety Policy and its importance explained.

Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.

Staff will always use a child friendly safe search engine when accessing the web with pupils.

5.3 Enlisting parents' and carers' support

Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.

The school will maintain a list of e-safety resources for parents/carers.

The school will ask all new parents to sign the parent /pupil agreement when their child is admitted to the school.

Created June 2011

Revised March 2013

Revised September 2014