Osborne Primary

Believe to achieve

E-SAFETY POLICY

Consultation with Staff: 24.9.14

Adopted by Governing Body: 29.9.14

Review date: Annually

Teaching and learning

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 so that they can build upon their previous knowledge in an independent manner.

The use of the Internet is a part of the statutory curriculum and an important tool for staff and pupils to both support and enhance learning.

Internet use to enhance learning

1. The school Internet access is designed expressly for pupil use and includes filtering (currently provided by Surfprotect) appropriate to the age of pupils.

2. Pupils are taught; what Internet use is acceptable; what is not and given clear objectives for Internet use.

3. Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

    1. When planning the use of the internet in KS1 adults will setup links, which have been checked, for children to use so that any risks are minimised
    2. In KS2 children will be able to search a topic independently using a suitable search engine (Google, Yahoo, Bing etc)

Pupils will be taught how to evaluate Internet content

1. The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
2. By taking part in regular E-Safety Lessons (every half term) through discrete teaching or through the ICT topic.
3. The school will take part in an Internet Safety Day and an annual Anti-bullying Week using resources provided and additional resources where possible (PCSO visits etc)
4. Pupils by the end of KS2 will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Pupil e-Safety curriculum

The school e-safety curriculum is an integral part of being safe online whether pupils are at home or school. It provides clear messages to the children and all staff **MUST** explain to the children what to do both at home and school if a problem does occur.

The e-safety curriculum plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas. It is a progressive e-safety programme that is built within the school computing curriculum and has additional discrete lessons that are also taught. It is built on SWGfL scheme of work and is reviewed regularly due to the ever changing technologies.

All pupils will be taught a range of skills and behaviours appropriate to their age and experience, including:

- STOP and THINK before they CLICK
- understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- understand why they must not post pictures or videos of others without their permission;
- know not to download any files without permission;
- have strategies for dealing with receipt of inappropriate materials;
- understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
- ensure staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;

Managing Internet Access

1 Information system security

1. School ICT systems capacity and security will be reviewed regularly.
2. Virus protection will be updated regularly on all electronic devices that it is available for.
3. **STRONG** passwords to protect data both on the network and other systems such as e-mail should be used.
4. Encrypted memory sticks used by staff to transfer restricted access files
5. Security strategies will be discussed with Surfprotect.

2 E-mail

1. Pupils may only use approved e-mail accounts on the school system.
2. Pupils must immediately tell an adult if they receive offensive e-mail.
3. If pupils receive an email from an unknown source they must tell an adult who will follow the school procedure on reporting.

4. Pupils **must not** reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission. If there are any reports that children have, all members of staff should refer to the Senior Leadership Team urgently.
5. E-mails 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.
6. The forwarding of chain letters is not permitted.
7. Attachments from unknown senders should not be opened at any time to prevent the spread of viruses, which could compromise data or equipment within the school network

3 Published content and the school website

1. 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.
2. The Head will delegate overall editorial responsibility to the Deputy Head to ensure that content is accurate and appropriate.
3. The publishing of photographs for the school website will be regularly reviewed to protect those children and staff who are no longer at Osborne Primary School (Permission will be sought if the school requires the photographs to remain on the website.)

4 Publishing pupil's images and work

1. Photographs that include pupils will be selected carefully.
2. Pupils' full names will not be used anywhere on the Web site particularly in association with photographs.
3. Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

5 Use of Ipads

The Deputy Head is responsible for regulating the behaviour of pupils when both on and off school site on IPads, following the school procedure on reporting.
The Deputy Head, governors and pupil monitors will undertake regular and random spot checks to ensure the equipment is being used appropriately.
The Head Teacher and Deputy Head will deal with any inappropriate incidents using the procedures outlined in this policy, the school behaviour, child protection and anti-bullying policies and will inform parents / carers of incidents of inappropriate e-safety behaviour.

Social networking and personal publishing

1. The school will block/filter access to social networking sites.
2. Pupils will be advised never to give out personal details of any kind which may identify them or their location.
3. Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

4. Staff will be told they **MUST NOT** publish personal information or information relating to the school community on social networking sites. They will be told they **MUST** set privacy settings and **NOT** to communicate with pupils.

Managing filtering

1. The school will work with the EXA, Office365 and Surfprotect to ensure systems to protect pupils are reviewed and improved.
2. If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Leader and ICT Network Manager as soon as possible.
3. The school uses a strong monitoring system which identifies any incidents. If the incident is not reported then the Deputy Head will investigate as stated in the procedure below.
4. Surfprotect will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

1. IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
2. Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
3. Videoconferencing will be appropriately supervised for all pupils.

Managing emerging technologies

1. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
2. **NOT** use mobile telephones in the classrooms when children are present.
3. Mobile phones will not be used in the classrooms or offices when children are present.
4. The sending of abusive or inappropriate text messages is forbidden.
5. Pupils are required to leave their mobile phones in the school office for the whole school day.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2010.

Policy Decisions

Authorising Internet access

1. All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
2. The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
3. At Key Stage 1, access to the Internet will be by adult demonstration with supervised access to specific, approved on-line materials.

Assessing risks

1. 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 Birmingham LEA can accept liability for the material accessed, or any consequences of Internet access.
2. The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

1. Complaints of Internet misuse will be dealt with by a Senior Leader using the following documents:
   - Response to incident of concern
   - E-safety screening tool
   - Incidents matrix
2. Any complaint about staff misuse must be referred to the Head Teacher.
3. Complaints of a child protection nature must be referred to a Designated Senior Leader and the Head Teacher.
4. Pupils and parents will be informed of the complaints procedure.

Community use of the Internet – By using the signing in book, all visitors agree to adhere to the school's e-safety policy. They will be reminded that the date, time and websites used on the premises are monitored for acceptable use.

Sanctions

There are times when incidents do occur, and these sanctions have been put in place to protect the welfares of those within the school community.

The following actions were agreed with both the School Leadership Team and all school staff.

Incident	Action
Deliberately Accessing or Trying to Access Material that could be considered illegal	Warning
Excessive or inappropriate Personal Use of internet/Social Networking Sites ETC	Refer to the Head
Unauthorised downloading and uploading of files	Refer to the Head
Allowing access to school network by sharing username and password or attempting to access using another person's account	Refer to appropriate line manager
Carless use of personal data	Warning
Deliberate actions to breach data protection or network rules	Warning
Corrupting or destroying data of others causing deliberate damage to hardware or software	Disciplinary Action
Sending an email, text message that is regarded as offensive, harassment or bullying	Warning
Using personal email, text messages, social media, instant message to contact students	Disciplinary Action
Actions which could compromise the staff members professional standing	Disciplinary Action
Actions which could bring school into disrepute or breach the integrity of the ethos of the school	Disciplinary Action
Subverting the schools filtering system	Disciplinary Action
Accidentally accessing offensive or pornographic material and failing to report it.	Refer to Line Manager
Deliberately accessing or trying to access offensive or pornographic material	Disciplinary Action
Breaching Copyright or licencing regulations.	Refer to Line Manager
Continued infringements of the above, following previous warnings or sanctions	Disciplinary Action

Communications Policy

Introducing the e-safety policy to pupils

1. E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each term.
2. Pupils will be informed that network and Internet use will be monitored.
3. All pupils will have half termly E-Safety Sessions to develop understanding of e-safety.
4. All Pupils will be read the acceptable use policy by a teacher, in which they will explain the policy to the children so that all children understand it.

Staff and the e-Safety policy

1. All staff will be given the School e-Safety Policy and its importance explained.
2. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
3. Staff should be aware that the school uses a strong monitoring system which identifies any incidents. If the incident is not reported then the Deputy Head will investigate the cause and issue the agreed sanctions, as stated below.

Enlisting parents' support

Parents' attention will be drawn to the School e-Safety Policy in newsletters and on the school Website.

All parents are invited to attend e-safety workshops to support the children's e-safety understanding in school and so they can build on this at home. They receive e-safety reminders and resources throughout the year.

Writing and reviewing the e-safety policy

The e-Safety Policy is part of the School Improvement Plan and relates to other policies including those for ICT, behaviour, anti-bullying and child protection.

The school will appoint an e-Safety Leader who will be supported by a committee composing of staff and pupils of the school.

Our e-Safety Policy has been composed by staff members, building on government guidance.

It has been agreed by all staff including senior leaders and approved by governors.

The e-Safety Policy and its implementation will be reviewed annually.

Osborne Primary School

Rules for Responsible Network and Internet Use

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- I will ask permission from a member of staff before using the Internet.
- I will not access other people's files.
- I will use the computers only for schoolwork and homework and will not try to access social network sites or games websites.
- I will not use inappropriate language on the school network or Internet.
- I will only e-mail people my teacher has approved.
- The messages I send will be polite and sensible.
- I will not give my home address or phone number on the Internet.
- To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy or uncomfortable with or I receive messages I do not like.
- I understand that the school may check my computer files and may monitor the Internet sites I visit.