Online Safety Policy

Consultation with Staff: September 18

Adopted by Governing Body: 01.10.18

Review date: Annually

Teaching and learning

Why Internet use is important

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. Using the internet has become an essential element in 21st century life for education, business and social interaction. This means that 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.

Internet use to enhance learning

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

2. In the event that inappropriate content does manage to be viewed/accessed in school, the Head Teacher will be notified to investigate using Securus Online Monitoring Tools.

3. Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use. In KS1 and KS2 this is done through the Rising Stars Online Safety scheme of work, whole school assemblies, enrichment days and when new issues are raised in the public domain. In EYFS, parts of the SWGfL digital literacy program is used alongside the national Internet Safety Day.

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

1. When planning to use the internet in KS1, adults will setup links in the children's zone of the school website for children to use. These should have been checked before the session to reduce any risks of seeing inappropriate content.
2. In KS2 children will be able to search a topic independently using a suitable search engine (Safesearch, Google SafeSearch and Kid Rex)

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 Online Safety Lessons which occur **every half term** through discrete teaching or through the e-safety topics in the computing curriculum.
3. The school will take part in an Internet Safety Day and Anti-Bullying Week. During these sessions all classes to complete cross-curricular activities relating to online safety 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.
5. Using the posters situated in each classroom to remind children how to act responsibly online.

Pupil Online Safety curriculum

The school Online Safety curriculum is an integral part of teaching children how to be safe online whether at home or at school. It provides clear messages and all staff MUST explain to the children what to do both at home and school if a problem does occur: telling an adult, use of CEOP /Report Abuse button and not sharing personal details.

At Osborne Primary School, the Online Safety curriculum plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for all curriculum areas. It is a progressive programme that is built alongside the 2014 National Curriculum computing curriculum and has additional discrete lessons that are also taught. It is built using Rising Stars Online Safety scheme alongside the SWGfL scheme of work. It is reviewed regularly due to the ever changing technologies and online safety issues that arise.

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;
- know some of the technical words (trolling, hacking, sexting etc)
- 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 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
- 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 (CEOP button);
- ensures that 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 (Surfprotect & ExaNetworks) will be reviewed regularly by the ICT Subject Lead and the School Network Manager.
2. Virus protection (ESET) will be updated regularly on all electronic devices, where possible, due to application development.
3. All staff and pupils will be encouraged to use STRONG passwords to protect data both on the network and other systems such as e-mail.
4. Encrypted memory sticks are used by staff to transfer restricted access files.
5. Staff are being encouraged to use Microsoft OneDrive to store all data for ease of access, but also to ensure all data is stored safely in case an encrypted memory stick is lost or destroyed.
6. Security strategies will be discussed with Surfprotect and Securus.

2 E-mail and Electronic Messaging

1. Pupils may only use approved accounts on the school system to send electronic messages via email. No other messaging is permitted on the school system.
2. Pupils **must** immediately tell an adult if they receive offensive e-mail or messages whether at home or school.
3. If pupils receive an email or message from an unknown source they must tell an adult who will decide whether to report it or not.
4. Pupils must not reveal personal details of themselves or others in communication, or arrange to meet anyone without direct permission. If there are any reports that children have, all members of staff should refer to the DSL and Senior Leadership Team urgently.
5. E-mails sent to an external organisation by children 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 messages, jokes, pictures or videos 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 web site

1. The contact details on the school website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published – this includes staff photographs or full name without explicit consent.
2. The Head Teacher and Computing Subject Lead will take overall editorial responsibility and ensure that content is accurate and appropriate.
3. The publishing of photographs for the school website will need to be regularly reviewed to protect those children and staff who no longer attend/work at Osborne Primary School

4 Publishing pupil's images and work

1. Photographs that include pupils will be selected carefully to ensure there are no safeguarding concerns related to the pupil. Any photos of pupils which are to be published need to be checked by the Computing Subject Lead and Senior Leadership Team.
2. Pupils' full names will not be used anywhere on the web site, and no names will appear alongside photographs to reduce pupils being identified.
3. Written permission from parents or carers must be obtained before photographs of pupils are published on the school website, in order to be in line with GDPR regulations.
4. Pupil's work can only be published with the permission of the pupil and parents and will use only the pupil's first name.

5 Use of School Social Media Platforms

The school now uses Marvellous Me to inform parent of their child's successes and on occasions, Twitter. This is a social media environment that can be accessed by parents, pupils and members of staff. To manage this, the following restrictions are to be put in place.

1. No images or videos of children will be published anywhere on Twitter without consent from parents and the Senior Leadership Team, and considerations will be made when posting to Marvellous Me.
2. Only the Computing Subject Lead or Network Manager will be able to add children's names to Marvellous Me.
3. The Computing Subject Lead or Network Manger will assign teachers and teaching assistants to the correct class at the beginning of each academic year.
4. Parents and pupils can access the system by receiving a unique code for their account which will be distributed on an annual basis.
5. Parents cannot message members of staff using Marvellous Me to protect staff working within the school.

6 Use of Tapestry Assessments in Foundation Stage

The school uses Tapestry Journal in both reception classes to assess children against the Early Learning Goals. This is a secure environment that can be accessed by parents and staff using secure login details. To consider the safeguarding of all pupils, the following has been put in place:

1. As Tapestry is online, any data added to the system is encrypted by the software. Also, any data given to Tapestry is owned by the school and will not be used by Tapestry staff unless permission is given. (Tapestry Data Management Policy)
2. Parents will receive a session on the use of Tapestry led by the Early Years Team. This will stress the importance of not sharing photos with others.
3. Only the Network Administrator will add children's names to the website.
4. The Computing Subject Lead will create teachers and teaching assistant's logins and assign them to the correct class at the beginning of each academic year.
5. Staff and volunteers can add observations to the system using IT in school. Where a volunteer has added an observation, approval by class teacher will be needed before publishing.
6. Parents can only access the system by giving the school their email.
7. Osborne Nursery has been given restricted access to the system for moderation purposes and data transfer.

7 Use of iPads

The Computing Subject Lead and Senior Leadership Team are responsible for regulating the behaviour of staff and pupils when they are on and off the school site using school IT equipment

(IPads, IPod Touch). The Senior Leadership Team will deal with any inappropriate incidents using the sanctions outlined in this policy, behaviour policy, safeguarding/child protection and anti-bullying policies, and will inform parents/carers of incidents of inappropriate online safety behaviour that may take place.

Social networking and personal publishing

1. The school will block/filter access to social networking sites (i.e. Facebook, Twitter etc).
2. As part of the new school website design the school now has a Twitter account. This will be used to post information that is important to parents by all staff. At no point should any pictures of children be posted without expressed consent from parents and the Senior Leadership Team.

3. Pupils will be advised never to give out personal details of any kind which may identify them or their location. As part of their online safety lessons they will also be taught to think about objects that are in their content which may identify a location.

3. Parents and pupils will be told of the age restrictions for social networking sites, as it is inappropriate that any primary aged school children access these. However, the school does understand children do have their own accounts and may have to deal with issues that occur on theses occasion, even if they are not posted about or in school.

4. Staff will be advised not to publish personal information or information relating to the school community on social networking sites. They will be advised to set privacy settings to the highest settings (i.e friends only or only me) and not to communicate with pupils or parents from school.

Managing filtering

1. The school will work with the EXA Networks, Office365, Surfprotect, and Securus 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 Online Safety Lead, and Network Manager as soon as possible. If the site has been accessed then staff should inform the Head teacher as soon as possible, so that this can be logged in the Online Safety incidents/monitoring folder.
3. The school uses a strong monitoring system (provided by Securus) which identifies any incidents and on many occasions, false positives. Weekly monitoring of online activity takes place and evidence is recorded in the Online Safety Incidents/Monitoring Folder of the incdents and subsequent actions. If the incident is not reported then the Head teacher or designated leader will investigate the cause and issue the agreed sanctions, as stated below.
4. Surfprotect and Securus 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 the pupils' age.

Managing emerging technologies

- **E**merging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Personal mobile phones **will not** be used during lessons or formal school time, and must be only be used at break times in designated areas and in the absence of children.
- The sending of abusive or inappropriate text messages is forbidden. Pupils are required to leave their mobile phones in the Phase Three Assistant Head's Office.

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 and pupils 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. In Key Stage 1, access to the Internet will be supervised by an adult at all times using approved on-line materials. In Key Stage 2 children will be shown how to access websites which children will follow whilst being supervised.

Assessing risks

1. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the scale and 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 Online ICT provision to establish if the current Online Safety policy is adequate and that its implementation is effective.

Handling Online Safety complaints

1. Complaints of Internet misuse will be dealt with by a member of the Senior Leadership Team using the following documents:
   - Response to incident of concern
   - Online Safety screening tool
   - Incidents matrix
2. Any complaint about staff misuse must be referred to the head teacher as soon as possible.
3. Complaints which involve Safeguarding/Child Protection must be dealt with in accordance with school Safeguarding/Child Protection procedures.
4. Pupils and parents will be informed of the complaints procedure.

Community use of the Internet

By using the signing in system, all visitors agree to adhere to the school's online safety policy which is onscreen for them to accept. Also, school staff will tell them that the date, time and websites used are monitored within the school premises.

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.

Sanctions for Pupils

The following actions were agreed with both the Head teacher and Online Safety Lead.

Incident	Action
Deliberately Accessing or Trying to Access Material that could be considered inappropriate for a child's age.	1st incident – talk to pupil from Online Safety Lead and warning given 2nd incident – CR and parents informed
Excessive or inappropriate Personal Use of internet/Social Networking Sites ETC	1st incident – talk to pupil from Online Safety Lead and warning given 2nd incident – CR and parents informed with short online safety settings session with Online Safety Lead
Unauthorised downloading and uploading of files	1st incident – talk to pupil from Online Safety Lead and warning given 2nd incident – CR and parents informed
Allowing access to school network by sharing username and password or attempting to access using another person's account	1st incident – talk to pupil from Online Safety Lead and warning given 2nd incident – CR and parents informed
Carless use of personal data	CR and parent informed
Corrupting or destroying data of others causing deliberate damage to hardware or software	CR and parent informed
Sending an email, text message that is regarded as offensive, harassment or bullying	1st incident – CR and parent informed 2nd incident – DSL informed. 3rd incident – Fixed Term Exclusion.
Using personal email, text messages, social media, instant message to contact adults	1st incident – CR and parent informed 2nd incident – DSL informed. 3rd incident – Fixed Term Exclusion.
Subverting the schools filtering system	1st incident – CR and parent informed 2nd incident – DSL informed. 3rd incident – Fixed Term Exclusion.
Accidentally accessing offensive or pornographic material and failing to report it.	1st incident – talk to pupil from Online Safety Lead and warning given 2nd incident – CR and parents informed 3rd incident – DSL Informed
Deliberately accessing or trying to access offensive or pornographic material	1st incident – CR and DSL informed. 2nd incident – Fixed Term Exclusion
Continued infringements of the above, following previous warnings or sanctions	Fixed term exclusion In rare circumstances Permanent Exclusion.

Sanctions for Staff

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 Online Safety policy to pupils

1. Pupils will be informed that network and Internet use will be monitored.
2. All pupils will have half termly online safety sessions, using the Rising Stars Online Safety Scheme in years 1 to 6, to develop understanding of how to behave when using technologies that access the internet.
3. 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. Alongside this, online safety rules will be posted in all networked rooms and discussed with the pupils at the start of each half term.

Staff and the Online Safety policy

1. All staff will be given the School Online Safety Policy and its importance explained at the start of each academic year. They will also be required to say they have read the policy and adhere to the acceptable usage of ICT.
2. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
3. If staff access websites which haven't been accessed before, they should do this without the Interactive Whiteboard showing the screen (i.e.turned off or on freeze).
4. Staff should be aware that the school uses a strong monitoring system which identifies any incidents. If the incident is not reported then the Senior Leadership Team will investigate the cause and issue the agreed sanctions, as stated below.

Enlisting parents' support

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

All parents are invited to attend online safety workshops to support the children's understanding in school so that this can built on at home. They also receive Online Safety reminders and resources throughout the year.

Writing and reviewing the Online Safety policy

The Online Safety Policy is part of the School Improvement/Enhancement Plan and relates to other policies including those for ICT, bullying and for child protection. Our Online Safety Policy has been written by the school, building on government guidance. It has been agreed by senior management and approved by governors. The Online Safety Policy and its implementation will be reviewed annually.

Rules for Responsible Network and Internet Use

The school has installed computers, tablets and internet access to support and enhance learning in all year groups. 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 and tablets only for schoolwork and homework.
- I will not try to access social network sites, games websites or applications which are inappropriate.
- I will not use inappropriate language on the school network or Internet.
- I will only send electronic messages people my teacher has approved.
- The messages I send will be polite and sensible.
- I will not give personal information on the Internet.
- To help protect other pupils and myself, I will tell an adult if I see anything I am unhappy or uncomfortable with or I receive messages I do not like.
- I will ask permission to record sounds, take photographs or film others and will not do so without consent of both the pupil(s) and adult in charge of my class.
- I will not attempt to change the settings on any computer or tablet.
- I understand that the school may check my computer files and may monitor the Internet sites I visit.
- I will regularly re-visit the online safety poster in my classroom to remind myself of the online safety rules.