



## **Sandbank Nursery School and Playcare Project E-Safety Policy**

### **Writing and reviewing the e-safety policy**

The e-Safety Policy relates to other policies including those for Anti bullying and for Safeguarding.

The school's named e-Safety Coordinator is: Lauren Turner

Our e-Safety Policy has been written by the school, building on advice received and government guidance. It has been agreed by senior management and approved by governors.

The e-Safety Policy was devised by:

It was approved by the Governors on: May 2010

It was reviewed:

The next review date is:

## **Teaching and learning**

### **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 necessary tool for staff and pupils.

### **Internet use will enhance learning**

- The school Internet access will be designed expressly for pupil use.
- children will be taught what Internet use is acceptable and what is not. children will also be given clear guidance when using the Internet.
- Children will be given experience of the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

### **Pupils will be taught how to evaluate Internet content**

- The school will follow copyright law when Internet derived materials are used by staff and children
- Children will be taught to report unpleasant Internet content to a safe adult.

## **Managing Internet Access**

### **Information system security**

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies are in place in line with Local Authority policy.

### **E-mail**

- Children's access to email will be with direct adult supervision only.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The forwarding of chain letters is not permitted.

### **Published content and the school web site**

- Staff or pupil personal contact information will not generally be published. Contact details for the school are on the school website.
- The headteacher or their delegated representative will take overall editorial responsibility and ensure that content is accurate and appropriate.

### **Publishing Childrens images and work**

- Photographs that include children, will be selected carefully so that individual pupils cannot be identified or their image misused. Where suitable the school will use group photographs rather than full-face photos of individual children.
- Childrens full names will not be used anywhere on a school web site or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school web site.
- Work can only be published with the permission of the parents/carers.

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

- Children and staff will not be allowed to access social networking sites.
- Staff will highlight the safe usage and dangers of social networking sites if children refer to using these outside of school.

### **Managing filtering**

- The school will work with Walsall Children's Services to ensure systems to protect children are reviewed.
- If staff come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator.

### **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.
- School staff should be aware 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.
- The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- Staff will not use personal devices to capture images of pupils.

### **Protecting personal data**

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation 2018.

## **Policy Decisions**

### **Authorising Internet access**

- All staff must read and agree to the Staff Acceptable User Policy for ICT before using any school ICT resource.
- All staff and pupils are granted access to school ICT systems.
- Access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.
- Any person not directly employed by the school will be asked to sign an acceptable use of school ICT resources before being allowed access to school ICT resources.

### **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. Neither the school nor Local Authority can 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 the e-safety policy is appropriate and effectively implemented.

### **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 headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school safeguarding procedures.  
Parents will be informed of the complaints procedure.

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

- The school will liaise with local organisations to establish a common approach to e-safety.
- All community users will be required to have read and agreed to the school Acceptable Use Policy which applies to them.

## **Communications Policy**

### **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
- e-Safety training will be embedded within our work with the children.

### **Staff and the e-Safety policy**

- All staff will be given the School e-Safety Policy and its importance explained.
- All staff will be made aware of e-Safety training when they join the school.
- Staff must be informed that network and Internet traffic will be monitored and can be traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.
- Staff will be informed of e -Safety issues in regard to school equipment being used off the premises

### **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 publish a list of e-safety resources for parents/carers. This will be given to parents as children transfer to their next school.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school as part of the induction process.

### **Appendix 1: Useful resources for teachers**

BBC Stay Safe	<a href="http://www.bbc.co.uk/cbbc/help/safesurfing/">www.bbc.co.uk/cbbc/help/safesurfing/</a>
---------------	--

Becta	<a href="http://schools.becta.org.uk/index.php?section=is">http://schools.becta.org.uk/index.php?section=is</a>
Chat Danger	<a href="http://www.chatdanger.com/">www.chatdanger.com/</a>
Child Exploitation and Online Protection Centre	<a href="http://www.ceop.gov.uk/">www.ceop.gov.uk/</a>
Childnet	<a href="http://www.childnet-int.org/">www.childnet-int.org/</a>
Cyber Café	<a href="http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx">http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx</a>
Digizen	<a href="http://www.digizen.org/">www.digizen.org/</a>
Kidsmart	<a href="http://www.kidsmart.org.uk/">www.kidsmart.org.uk/</a>
Think U Know	<a href="http://www.thinkuknow.co.uk/">www.thinkuknow.co.uk/</a>
Safer Children in the Digital World	<a href="http://www.dfes.gov.uk/byronreview/">www.dfes.gov.uk/byronreview/</a>
WMNet	<a href="http://www.wmnet.org.uk">www.wmnet.org.uk</a>
Getsafe online	<a href="http://www.getsafeonline.org">www.getsafeonline.org</a>

## Appendix 2: Useful resources for parents

Care for the family	<a href="http://www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf">www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf</a>
"Know It All" CD	<a href="http://publications.teachernet.gov.uk">publications.teachernet.gov.uk</a>
Family Online Safe Institute	<a href="http://www.fosi.org">www.fosi.org</a>
Internet Watch Foundation	<a href="http://www.iwf.org.uk">www.iwf.org.uk</a>
Get safe online	<a href="http://www.getsafeonline.org">www.getsafeonline.org</a>
Think U Know	<a href="http://www.thinkuknow.co.uk/">www.thinkuknow.co.uk/</a>
BBC Stay Safe	<a href="http://www.bbc.co.uk/cbbc/help/safesurfing/">www.bbc.co.uk/cbbc/help/safesurfing/</a>

Reviewed: March 2021

Next review date: March 2023

Passed by: \_\_\_\_\_

Date: \_\_\_\_\_