Westbourne Primary School E-Safety Policy

"Everyone at Westbourne is committed to working together to give children the academic and life skills they will need to be successful." (Vision)

Rationale

At Westbourne Primary School, we give children the necessary life skills in remaining safe whilst using ever-changing technology. Similarly, we support children to fulfil their potential and aim to raise standards across the whole curriculum, in this instance, with ICT as the driver. The purpose of our E-Safety policy is to highlight the potential dangers in using ICT both in and out of school, and to provide staff, children and others with information on how to stay safe using technology.

Aims

This document, when coupled with the **Acceptable User Agreement**[1] (AUA), aims to ensure that all stakeholders have an understanding of how to manage E-Safety through set systems and protocols.

At Westbourne Primary School, we aim to ensure all children have appropriate access to ICT technologies for learning.

Introduction

See *Acceptable User Agreement* for more information.

Staff liaise with parents and children in order to provide information on safe use of technology in and out of school. An E-safety letter is sent home at the start of the year, explaining the dangers and terminologies parents may need to know. Teaching of E-Safety is fundamental to the ICT curriculum and should underpin every lesson where ICT is used.

E-Safety is embedded into the taught curriculum throughout all ICT in school. Westbourne Primary School identifies the five main aspects of E-Safety as:

- Obsessive use;
- Copyright infringement;
- Exposure to **inappropriate**[2] materials and content;
- Physical danger, sexual abuse, online safety;
- Data privacy and protection;

Breaches of E-Safety guidance will be dealt with by the E-Safety officer.

Governing Body

The Governing Body has the responsibility to review this policy every three years. Governors work with the Head Teacher and E-Safety Leader to establish and monitor the school arrangements for e-safety.

Obsessive Use

Staff teach children to have an awareness of technology overuse. They help children identify what obsessive use looks like and the implications of this upon social relationships and health. Where concerns are brought to the attention of the school, staff follow up with parents any concerns regarding a child's use of ICT at home.

Copyright Infringement

Children need to understand that data online belongs to someone and that certain copyright laws are attached to data such as images, videos and sound. Children are taught to reference data sources where appropriate, by providing the relative hyperlink and reference. They will begin to understand that certain data cannot be shared or distributed with others, and that some data (including music and film) must be purchased at a cost.

[1] The **Acceptable User Agreement** details specifically how stakeholders will use ICT inside and outside of school more specifically than the E-Safety policy.
[2] **Inappropriate** is defined to be something that is unsuitable for children to be exposed to.

Exposure to Inappropriate Materials and Content

The school firewall filters the majority of inappropriate content, though children still need to be taught what materials are inappropriate to them in relation to their age group. If an inappropriate image, video, sound, or message is displayed on their screen, they must know to turn their monitor off and inform a teacher immediately.

Westbourne Primary employs a smooth wall system installed on all devices, which provides weekly reports to the Headteacher on the content of its users.

Physical Danger, Sexual Abuse and Online Safety

See also Personal Content and Online Identity.

Children are taught to keep all of their personal information private online. They must not share any data with another and must only communicate with somebody if they are absolutely certain of their identity. They will know what content may put them in physical and/or sexual danger by engaging in open discussion with themselves and staff.

Children are taught that they should never arrange to meet someone through technology (i.e. e-mail, texting, etc.) if they are uncertain as to who they are communicating with. They must tell staff and/or parents if any concerns arise.

Data Privacy and Protection

Data Encryption

All data kept by staff on children is considered sensitive and must therefore be kept secure, through usernames, passwords and encrypted memory sticks. No sensitive information belonging to the school, or the children, may be kept on any device that is not secured with a password.

Password Protection

Children and staff all receive individual usernames and passwords for logging on to the school network and the e-mail system. Staff teach children the importance of password protection. Any incidents involving sharing or stealing of passwords will be logged and dealt with by the ICT Leader/Technician, the class teacher, or, where severe/repeat offences have occurred, the Head.

This is also applicable to parents and families, who receive their own unique usernames and passwords for home learning websites such as Bug Club and Education City. The ICT Leader, and other relevant adults, run workshops for parents and governors on safe use of these sites throughout the school year.

Cloud Storage

Westbourne Primary School uses OneDrive as its cloud storage solution. The ICT technician keeps the password to this and logs staff on who need it. Children and staff are able to use this in order to transfer information between handheld devices and the school network.

Updating Software

The ICT technician is responsible for distribution of software for each school device. If staff need software to be downloaded, they must first consult the ICT leader and/or technician. Attachments to e-mails may only be downloaded if the person receiving the e-mail is aware of the message content. Any suspicious e-mails must be reported to the ICT technician and/or Headteacher.

Personal Content and Online Identity

Images of children are displayed on the school website, or other **external hosting sites**[3]. New children receive an opt-out letter, to identify children's image privileges in school. Parents must return the letter, identifying the following:

- If the child can have their image taken and used in school;
- If the child can have their image taken and used on the World Wide Web.

It is the responsibility of the class teacher to display a class list of each child's image privileges in class. This informs them, and other adults, as to who can have their picture taken.

[3] The school may use **external hosting sites** in order to upload different content (videos, PowerPoints, sound, etc.). The ICT Leader and ICT Technician hold the password for these web sites and can assist on uploading of content.

Children are taught about the dangers of online identities, and how private information (name, address, etc) must not be shared with anyone over the internet.

Mobile and Personal Devices

Children are not allowed to bring personal devices into school unless otherwise given permission. Staff may use their own devices in the staff room, PPA room, and admin areas only. This is to protect staff against any claims children, or adults, may make against members of staff regarding taking of inappropriate images. Any exceptions to this rule must be agreed by the Head.

The school has a mobile phone which must be taken out by staff when on school trips. This is to protect staff from any accusations of photographing children with a personal device.

Westbourne also has a number of mobile devices able to record images of children. Staff must adhere to the school policy when using these in and out of school.

Social Media

Staff must not befriend pupils or ex-pupils online. Staff must ensure that their social media profiles (Facebook, Twitter) are set to private in order to protect themselves from having their data stolen (images, personal details, etc.).

E-Mail

Children and teachers may use the school e-mail in relation to school work. If any concerns are raised as a result of these conversations, then the Head of ICT leader must be consulted.

School Website and Blog

Class teachers are responsible for updating their own class page. This is done half-termly through a content management service. Staff must adhere to deadlines so that their class page is kept up to date.

The office admin staff are responsible for uploading letters and other information regarding whole school activities and events.

The website provides links to whole school blogs.

Logging E-Safety Incidents

Any breaches of the E-Safety policy or Acceptable User Agreement must be reported to the Head and/or ICT Leader and will be dealt with accordingly. The Head Teacher is the E-safety officer for Westbourne Primary School.

Linked Policies / Documents

- Acceptable User Agreement
- Twitter Policy
- Safeguarding / Child Protection
- Behaviour
- Data Protection
- Opt-out Letter

Ratified by the Governing Body May 2015

Review Date: May 2018