E-Safety Policy

Prepared by: Hemant Mistry
Date referred to the School Improvement Committee: 14/09/2017
Date of next review: Autumn term 2019

E-Safety Policy
(This policy works in collaboration with the Acceptable Use Policy which all adults in school sign)

The Policy covers the following areas:

Physical Safety
Network Safety
Internet Safety
E-mail Safety
Use of Digital Media
E- Bullying
Mobile Phones
Other Technologies
Copyright
Data Protection Act
E-Safety Pupil Rules (AUP)

Explanation of Text

New technologies have revolutionised the movement, access and storage of information with important implications for all schools. Use of ever more powerful computers, broadcast media, the Internet, digital recorders of sound and images together with increased opportunities to collaborate and communicate are changing established ideas of when and where learning takes place. At Evington Valley Primary School, we recognise that learning is a lifelong process and that e-learning is an integral part of it. Ensuring that we provide pupils with the skills to make the most of information and communication technologies is an essential part of our curriculum. The school is committed to the continuing development of our ICT infrastructure and embracing new technologies so as to maximise the opportunities for all pupils, staff, parents and the wider community to engage in productive, cooperative and efficient communication and information sharing.

However, as in any other area of life, children are vulnerable and may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies. Additionally, some young people may find themselves involved in activities which are inappropriate, or possibly illegal. E-safety seeks to address the issues around using these technologies safely and promote an awareness of the benefits and the risks.

Definition of e-Safety

The term e-safety is used to encompass the safe use of all online technologies in order to protect children and young people from known and potential risks.

The term e-safety is defined for the purposes of this policy as the process of limiting the risks to children and young people when using Internet, Digital and Mobile Technologies through a combined approach to policies and procedures, infrastructures and education, including training, underpinned by standards and inspection.
(source BECTA. BECTA was closed by the coalition government 31st March 2011).

This policy sets out clearly our expectations on pupils, parents and members of the wider community to ensure best practice.

Risks

For many pupils, the online 'virtual' world is as real to them as the 'real' world. And it spans across all contexts of their social interaction, home, school, peer groups, neighbourhoods but also unknown audiences on the internet; and it does so 24/7. Children and young people do not always recognise the inherent dangers of the internet and often do not understand that online behaviour may have offline consequences.

Physical Safety:

- All electrical equipment in the school is PAT tested annually to ensure that it is safe to use. Pupils are taught about the dangers of electricity as part of the science and PSHE curriculum – these are taught through topic lessons. We expect pupils to behave appropriately near electrical sockets and appliances.
- All the projectors and interactive screens (currently in the Main Hall, Drama Hall and all classrooms) in our school have maximum light levels below the government's health and safety guidance. Pupils are taught that they should not look directly at strong light sources such as the sun, lasers or projectors. We expect all users to not look directly into the light beam when working on the interactive whiteboards.
- Workstations, laptops, tablets and mobile devices are cleaned and sanitised regularly.
- We expect all users to refrain from eating and drinking when using any IT equipment.
- Pupils are taught correct posture for sitting at a computer and that sitting for too long at a computer can be unhealthy. We expect all users to take responsibility for their own physical well-being by adopting good practices.
- Computers and other ICT equipment can be easily damaged. Pupils are taught the correct way to use ICT equipment. We expect pupils to respect ICT equipment and take care when transporting, handling and using.

Network Safety:

- We expect all pupils to only logon using their own or class username and password. Each user is given an allocation of disk space for the storage of their work. Pupils are taught how to save their work into their "My documents" area and the Public shared drive. We expect pupils to save and keep their work to build up a portfolio of evidence.
- Access to other users "My documents" areas are restricted by the network. Pupils are taught not to access another user's work without permission. We expect pupils to respect the privacy of all other users and to make no attempt to access or interfere with another user's work.
- On the network there are "Public Drive" areas where many different groups of users can save work so that it is available to others. Pupils are taught how to access and save to these shared resource areas. We expect pupils to respect the contributions of others, not to delete or alter others' work and to ensure that they only save work to shared areas with permission.
- Pupils are taught to only print when necessary to save resources for financial and environmental reasons. We expect pupils to only print out work when directed by staff to do so.
- Network policies prevent changes being made to computer settings. Pupils are taught that making changes may prevent the computer from working properly. We expect all users to make no attempt to alter the way the computer is set up.

- Only network administrators are permitted to install software and applications on to workstations, laptops and tablets. Pupils are taught that the network or an application may not function properly if programmes are installed. We expect all users to make no attempt to download and install any programme onto the network, any requests for software to be installed must be made to the ICT Technician.
- We strongly encourage users to be using an encrypted memory stick. Supply staff, volunteers and visitors must give their memory stick to the ICT Technician to be scanned before being used.
- All users of the network can be monitored remotely by the network administrators. Pupils are taught that their use of the network can be monitored. We expect all users to understand that their use is subject to monitoring.

Internet Safety:

- When using any internet enabled device at Evington Valley all access to the Internet is protected by a number of different filters. These filters are designed to prevent accidental or deliberate access to unsuitable materials. In addition, the network administrators can request to add site addresses which are considered to be unacceptable via the web filter provider Capital Bytes. However, no system is 100% safe and we expect users to behave responsibly. Pupils are taught that the Internet contains many websites that are useful but that there are also websites that are unpleasant, offensive, not child-friendly or can damage your computer. Evington Valley invests in safeguarding monitoring software (Future Digital) to generate screen captures where inappropriate material is accessed or where inappropriate searches are made. The screen captures are captured based on a large database of banned words and phrases which is updated regularly. We expect pupils to make no attempt to access a website that they know to be unsuitable for children and/or containing offensive language, images, games or other media.
- All social media websites such as Facebook and YouTube have a minimum age of 13 years old required to be able to register and use the website. We expect no pupils at Evington Valley Primary to be registering to any social media websites including the use of online gaming websites such as Xbox live and the PlayStation network.
- Pupils accessing the Internet at home are subject to the controls placed upon them by their parents or carers. However, any home use of the Internet made in connection with the school or school activities; any of its staff, pupils and governors or any partnership organisation will be subject to this policy and any breach dealt with as if the event took place at school. We expect all members of our school community to behave as positive ambassadors of the school in all school related activities made through the Internet.
- The school website contains school policies, newsletters and other information. We expect all persons accessing the school website to treat the content with respect and make no attempt to reproduce, use or alter any part

in any way with malicious intent. No part can be reproduced for commercial reasons without written permission from the school.

Use of YouTube and other media sharing websites:

YouTube contains a wealth of extremely useful educational videos that will be used in the classroom led by an adult. YouTube (and similar websites) is a video sharing website and it also contains features that deem it to be a social media network. ONLY adults will have access to YouTube using their own school network login credentials. Children will not be able to access YouTube using their own network login.

Email Safety:

Currently children at Evington Valley Primary have no personal email addresses supplied by the school and must not use any other personal email address providers in school such as Gmail or Hotmail.

Occasionally some classes may have a class email address that will enable them send and receive emails as part of their Computing unit of work. This could be emailing link schools for examples. The class teacher monitors usage and pupils never have knowledge of the email login credentials. Pupils are taught that emails being sent must have a clear learning purpose and be written in polite and coherent manner.
We expect all users to communicate appropriately through email and use their evingtonvalley.leicester.sch.uk email address for work purposes only. Future Digital is active on all devices and will create screen captures of any banned words or phrases. Some pupils will have their own webmail accounts at home, and we strongly discourage this. As webmail is independent of the school they do not necessarily come with the safeguards and filtering that we set for email usage. Therefore, we do not permit the use of personalised email accounts by pupils at school or at home for school purposes. Pupils are taught that using a personalised webmail account in school or for school use is not permitted. We expect pupils to use school issued email accounts with adult supervision and only when needed to cover a unit of work.

Digital Images:

- Digital still and video cameras are used for recording special events as well as being an essential tool for everyday learning experiences across the curriculum and to capture evidence. Parents are asked to sign a consent form for images of their children to be used for school purposes. Some images celebrating the work of pupils involved in everyday and special event activities may be selected to be shown on the school website, separate permission is sort for this. On the website we never associate names with images. Evington Valley will happily remove any image of a child on the school website at the parent or carer request.
- There are occasions when digital images, video and live conferencing of pupils will be shared with authorised partner schools and organisations for

collaborative learning projects and publications. Separate permission for this will be sort from parents and carers. All such use of recording equipment is monitored and supervised by staff.

- Digital images and videos of pupils are stored on school cameras and any other recording equipment. At the end of each term the media must be deleted from the camera memory

Cyber/ E-Bullying:

- Evington Valley Primary takes bullying very seriously and has robust procedures for identifying and dealing with it. E-bullying is the use of any online communication medium to offend, threaten, exclude or deride another person or their friends, family, gender, race, culture, ability, disability, age or religion. Pupils are taught about bullying as part of the PSHE curriculum. We expect all members of our community to communicate with each other with respect and courtesy. Bullying of any type will not be tolerated by Evington Valley and will be dealt with under the procedures within the Whole School Policy on Behaviour, including bullying.

Mobile Phones & Smart Watches:

- Pupils are not permitted to have mobile phones and/or smart watches upon their person in school. We recognise that our oldest pupils may walk on their own to and from school and parents may wish them to have a mobile phone for emergencies. However, we discourage this on security grounds as they are easily lost, damaged or stolen. Pupils are taught that they shouldn't have a mobile phone and/or on their person in school and that any phone brought in must be handed to the office for the duration of the day.
- Staff members should ONLY use their mobile phones in the staff and PPA room

Other technologies:

- Podcasting– Some pupils will be given opportunities to create oral recordings. Some of these recording may be made available as podcasts through the Internet so that they can be shared with interested members of the school community.

Copyright:

- There are many free to use resources on the Internet, the majority of image, sound and music files are covered by copyright laws. Some can be used for educational reasons without permission provided that the source is stated and that they are not made available outside the school. Some cannot be used under any circumstances; this is particularly so for music but can apply to other types of file e.g. photographic images. Care therefore needs to be taken with multi-media work which incorporates anything downloaded from the Internet or any other published source that it is not uploaded onto the school's website or broadcast through any other technology. Pupils are taught that the people who put their work on the Internet may not always want people to copy

or use their work and that they should check whether they have permission. We expect all users to respect copyright laws.

- It is important to know what work is original and when chunks of text have been copied from other sources such as the Internet. Pupils are taught that they should not present the work of others as their own work. Older pupils are taught about copyright and how to extract or paraphrase information. We expect all pupils to make it clear what is their own work and what is quoted from other sources.

Data Protection Act:

- The Data Protection Act 1998 gives you the right to access information held about you or your child by the school. The school has the right to charge for supplying this information. Further information on the Data Protection Act can be obtained from: https://www.gov.uk/data-protection
- Evington Valley Primary is committed to ensuring personal information is properly managed and that it ensures compliance with the Data Protection Act 1998 (DPA). The School will make every effort to meet its obligations under the legislation and will regularly review procedures to ensure that it is doing so.

Rules for Responsible Internet Use for Children at Evington Valley Primary School (AUP)

Evington Valley Primary has a variety of internet enabled devices that help us with our learning. These rules will help us keep safe online and help us be fair to others. Adults at Evington Valley encourage all pupils to follow the SMART Internet rules (http://www.kidsmart.org.uk/beingsmart/) in addition to this we also actively encourage pupils to follow the following rules.
I want to stay safe while I am using a computer and I know that anything I do on the computer may be seen by someone else.

I will:

- I will only access the computer system with the login and password I have been given and keep my password a secret
- I will not access other people's files
- tell an adult if anything makes me feel scared or uncomfortable
- I will not bring in memory sticks or CDs/ DVDs from outside school and try to use them on the school computers without permission from a teacher.
- make sure all the messages I send are polite and tell an adult if I get a nasty message
- I will report any unpleasant material to my teacher immediately because this will help protect other pupils and myself;
- not give my mobile number, home number or address to anyone who is not a real friend
- not tell people about myself on-line (I will not tell them my name, anything about where I live or where I go to school) and agree never agree to meet a stranger.
- not load photographs of myself onto the computer
- I understand that the school may check my computer files and may monitor the internet sites I visit;
- I will not create any social media accounts and accounts for online gaming as I must be over 13 years of age and I will not complete and send forms without permission from an adult.

I have read through this agreement with my child and agree to these safety restrictions.

Signed: _____ Parent/ Carer

Name of child: _____

Class: _____

Date_____

Useful websites for up-to-date information about e-safety issues:

Childnet www.childnet-int.org
Resources to help you use the internet safely and positively as a professional, and information to help safeguard your workplace and the young people you work with.

CEOP www.ceop.gov.uk
Child Exploitation Online Protection Centre for reporting internet abuse

Think you know www.thinkuknow.co.uk
Practical online advice and training resource for children, parents and professionals by CEOP

SAFE https://safe.met.police.uk/internet_safety/consequences_and_the_law.html
Facts and the law on internet issues provided by the Met Police

NSPCC www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/
NSPCC online safety advice

Share Aware www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware/
Useful NSPCC site which can support parents in how to talk to their children about the dangers of sharing information online.

UK Safer Internet Centre www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals
Useful information, advice and resources to help professionals support young people to stay safe online.

Internet Watch Foundation www.iwf.org.uk
UK hotline for reporting illegal content.

Barnardos
www.barnardos.org.uk/what_we_do/barnardos_today/resources_internet_safety

National Education Network www.nen.gov.uk/online-safety
Online safety advice and training resource for children, parents and teachers

OFCOM www.ofcom.org.uk
Provides information on how to keep up with new technology

Digizen www.digizen.org/cyberbullying
Cyberbullying specific information and guidance