Internet Safety Report

June 2022

Created by: Mr Simon Smith

Contents Page

1 Introduction

This is the first Internet and e-safety report at Bradley Primary School and aims to give staff, parents and children an understanding of using the internet safely and effectively both in and out of school. It identifies risks, opportunities and challenges and measures the school has in place to allow and educate children and staff on using the internet safely.

2 Opportunities, Risks & Challenges

2.1 Opportunities

Bradley Primary School aim to give children and staff constant internet and network access to use as an educational resource and platform for communication and creativity. The school network allows users to save resources in a secure area on the server that can be accessed from any device that is connected to the school network. Users only have access to certain drives on the network that aims to reduce the risk of accidental or intentional deletion of resources. The school server is backed up daily offsite in case of damage, fire, theft etc.

Children have access to various devices including computers, iPads and laptops and have weekly computing lessons with the school computing teacher, Mr Smith. During computing lessons, children have access to the internet for research purposes. Mr Smith delivers online safety lessons every year to each year group that educates the children on how to use the internet safely and effectively and what to do if they feel threatened or upset when using this resource.

2.2. Risks

Although the internet is a great source of information, there are distinct risks involved with using it including content, contact and conduct. Children are educated during weekly computing lessons on what to do if they feel threatened or upset when using technology or the internet.

The school firewall and internet filter reduces the risk of children accessing websites that may contain upsetting or threatening content. The school web filter has various levels of filtering dependent on who logs on to the device. Mr Smith manages filtering and can block or allow websites as required.

2.3 Challenges

There are many challenges both to staff and parents when using the internet and these challenges change frequently as technology advances. New websites are created frequently and it is a challenge to block these from being accessed if they contain upsetting or threatening content. Mr Smith manages the school web filter but the company, who provide this resource, Schools Broadband, are responsible for filtering at a higher level. Violence, drugs, racism, discrimination, sexual content etc. are blocked by the filtering company and cannot be accessed or unblocked whilst using the internet in school.

Outside school, children will not have the web filtering software when using the internet and the challenges and risks increase because of this. Children are made aware of this during computing lessons and are taught to only use computers in school and at home when there is an adult present and what to do if they do see anything that is inappropriate or upsets them.

3 Filtering

The school uses web-filtering software called Netsweeper. Schools broadband who also provide the school with their internet access and firewall provide this. Netsweeper enables organizations to protect internet users from harmful online content and provides web filtering, digital monitoring, and online activity reporting solutions to ensure digital safety for both staff and children.

Netsweeper's client filtering technology ensures filtering is enforced on all devices (Windows, Mac, Chrome, Android, and iOS) and will monitor internet traffic on those devices, even when they are not connected to a Netsweeper filtered network. This enables schools to provide students with devices for remote learning and remain confident that they will be protected from online harm.

The school IT Manager, Mr Smith can monitor which device has accessed the internet, what websites have been visited, what search terms have been used and when each device has accessed the internet. This allows the school to monitor internet use and access and identify any risks or users trying to use this resource for anything other than what was intended.

4 Staff

Bradley Primary School provides computers and iPads for use by staff as an important tool for teaching, learning and administration of the school. All members of staff have a responsibility to use the school's computer systems in a professional, lawful and ethical manner.

The internet and level of filtering is provided to allow staff to use this resource for teaching and learning only. Staff are aware that certain websites can be accessed by staff that may not be appropriate for children i.e. YouTube and social networking sites. Staff need to be aware of the risks involved when accessing these sites; especially in the presence of children and to ensure the sites are safe and appropriate when doing so.

Staff are aware that the use of personal mobile phones, laptops, iPads or other computing technology is not allowed in school without authorisation from SLT. Personal devices are not to be added to the school network without permission and personal devices are not to be used for taking photographs of children in or out of school without permission from SLT.

Each member of staff is provided with a personal email account for communicating in and out of school, with their own username and password. As such, users must not disclose password information to anyone, including the IT manager unless they need a password reset. In the event of a password becoming compromised, users will be required to change their password immediately or notify the IT manager.

5 Parents

Parents are made aware of risks involved when using the internet in and out or school by accessing the school website and school newsletters. Using the internet at home comes with many risks. These devices do not have the same level of security as schools and parents need to be aware of the risks involved and kept up to date with and changes or threats.

Online bullying, grooming, inappropriate websites and children playing computer games that are not appropriate for their age range is a huge problem. Parents need to be made aware of threats, and prevention measures to allow their children to use the internet and technology safely and responsibly. E-safety training for parents has been offered in the past on numerous occasions but interest was low.

6 Children

Children who attend Bradley Primary School have daily access to technology that has internet access. Each year group has a bank of iPads that can be used for using educational apps, internet access, taking photos and videos. Laptops are also accessible for the same educational purposes.

Children have weekly computing lessons, learning about e-safety and staying safe online, digital research, digital literacy, computer science, programming amongst other subjects. Children are educated on what to do if they do come across anything that upsets them.

Children are taught not to use devices unless they are in the company or an adult and what risks and threats they are when using these devices. They are also taught the differences when using devices in and out of school and that they can speak to an adult they trust if something does upset them when using devices in and out of school.

7 Plans for the Future

As technology and threats frequently change, teachers and parents need to be updated and made aware of these threats. Mr Smith has attended numerous e-safety courses and is constantly in contact with the web filter provider regarding new threats and monitoring of internet usage in school. Children have e-safety lessons every year and these lessons need to be constantly updated to include any new threats.

Parents also need to be kept up to date with changing technology and threats and a yearly internet safety newsletter and/or training needs to be given/offered to them.