ambition, belief, communication

E-SAFETY POLICY

S.Smith
November
2023

Developing and Reviewing this Policy

This eSafety Policy has been written as part of a consultation process involving the following people:
Mr Simon Smith (IT Manager/Teacher/IT Co-ordinator), Mr Sharon Taylor (Head teacher)

Policy Created April 2016.
Last updated – November 2023
Policy to be reviewed annually.

E-Safety Policy 2023

Introduction

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users). Research has proven that the use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective e-Safety Policy will help children and adults develop the skills and confidence to manage potential risks and considerably reduce their impact. Our e-Safety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community is prepared to deal with the safety challenges that the use of technology brings. The policy is organised in four main sections:

· Policies and Practices
· Infrastructure and Technology
· Education and Training
· Standards and Inspection.

Bradley Primary School's vision for E-Safety

Ensure that children learn in an environment where security measures are balanced appropriately with the need to learn effectively.

· Children are equipped with the skills and knowledge to use technology appropriately and responsibly.
· Teach children how to recognise the risks associated with technology and how to deal with them, both within and outside the school environment.
· All users in the school community understand why there is a need for an E-Safety Policy.

The role of the school's E-Safety Champion

Our eSafety Champion is: Mr Simon Smith (IT Manager/Teacher/IT Co-ordinator)

The role of the E-Safety Champion in our school includes:

· Responsible for ensuring the development, maintenance and review of the school's eSafety Policy and associated documents.
· Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
· Ensuring all staff are aware of reporting procedures and requirements, should an E-Safety incident occur.
· Ensuring an E-Safety Incident log is appropriately maintained and regularly reviewed.
· Keeping personally up-to-date with eSafety issues and guidance through liaison with the Local Authority and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
· Providing or arranging E-Safety advice/training for staff, parents/carers and governors.
· Ensuring the Head teacher, SLT, staff, children and governors are updated as necessary.
· Liaising closely with the school's Designated Senior Person / Child Protection Officer to ensure a co-ordinated approach across relevant safeguarding areas.

Security and data management

ICT security is a complex subject that involves all technology users in school, dealing with issues regarding the collection and storage of data through to the physical security of equipment. In line with the requirements of the General Data Protection Regulation (GDPR), sensitive or personal data is recorded, processed, encrypted, transferred, and made available for access in school. The data is:

· Accurate.
· Secure.
· Fairly and lawfully processed.
· Processed for limited purposes.
· Processed in accordance with the data subject's rights.
· Adequate, relevant and not excessive
· Kept no longer than is necessary
· Only transferred to others with adequate protection.

All data in school is kept secure and staff are informed of what they can or cannot do with data through the E-Safety Policy.

· Mr Simon Smith is responsible for managing information.
· All staff know or are shown the location of required data.
· All staff with access to personal data understand their legal responsibilities.
· The school ensures that data is managed appropriately, both within and outside the
school environment by regular staff meetings and training.
· Staff are aware that they should only use approved means to access, store and dispose of confidential data.
· Staff who have remote access to school data ensure the data remains secure and are aware of
the dangers of unsecured wireless access at home.
· Bradley Primary School ensures that data is securely stored and satisfies the requirements of the
General Data Protection Regulations (GDPR) by backing up data both onsite and offsite.

· Mobile devices such as pen drives and external hard drives are not to be used in school unless
authorised by SLT and/or Mr Simon Smith. Sensitive data that is taken off-site must be either encrypted or password protected. Personal iPads, mobile telephones and laptop computers are not to connect to the school network or access data on the network without authorisation from SLT and/or Mr Simon Smith.

Use of mobile devices

School use of mobile devices, including laptops, tablets, mobile phones, cameras and games consoles is becoming more commonplace. Whilst these can provide a flexible solution and offer a range of exciting opportunities to extend children's learning, their use poses challenges in terms of E-Safety. Many of these devices integrate functionality to take images, access the Internet and engage users in various methods of external communication. Bradley Primary School does not allow the use of such devices in school without authorisation from SLT and/or Mr Simon Smith. The school provides iPads, laptops and digital cameras for use in class and these devices must be kept in school at all times unless agreed with by SLT and/or Mr Simon Smith. Bradley Primary School accepts that mobile phones are needed by staff in case of emergency and allow use of these in case of emergencies. Mobile phones can be used in the staff room or other locations away from children with permission from SLT but only for phone calls and are not to be used to take photographs or access the school network without authorisation from SLT and/or Mr Simon Smith. Mobile phones are to be switched off or put onto silent mode unless prior agreed with SLT. If children require mobile phones in school these are to be kept in a safe location i.e. with the class teacher unless prior agreed with SLT.
Children are not to bring mobile phones, laptops, games consoles, iPads, tablets, smart watches or any other device that allows photographs to be taken or access to the World Wide Web without prior permission from SLT. Staff and children can be contacted via the reception/office in case of emergencies. A mobile phone is provided by school for staff when going on school trips in case of emergencies. This is only to be used for contacting the school or in case of emergencies and not to be used for personal use. The office staff are responsible for ensuring the mobile phones are in credit and fully charged.

If staff/children are seen to be using mobile phones, then this must be reported to a member of the SLT or the device confiscated.

Use of digital media

The use of cameras and sound recording devices offer substantial benefits to education but equally present schools with challenges particularly regarding publishing or sharing media on the Internet, e.g. on Social Network sites. Photographs and videos of children and adults may be considered as personal data in terms of the General Data Protection Regulation (GDPR). To ensure all users are informed about the risks surrounding taking, using, sharing, publishing and distributing digital media, Bradley Primary School regularly have staff meetings/training and notify staff of what the devices can and cannot be used for. Parents are informed that their children's photographs may be used in school and on the school website when the child starts school and they have the option to opt out of this if they have any concerns with taking or using photographs of their children. This information is kept in a secure location and class teachers know who in their classes are not allowed to be photographed. All photographs are removed from the website and school within 6 years of them being taken in accordance with the General Data Protection Regulation (GDPR). Photographs are only to be taken using school property and with permission from SLT and/or class teachers. Certain areas of the school are 'off limits' for taking any photos. These include toilets, cubicles etc. Parents are notified if photographs are not allowed to be taken during school performances, plays etc.

Communication technologies

The school uses a variety of communication technologies, are aware of the benefits, and associated risks. New technologies are risk assessed against the potential benefits to learning and teaching before being employed throughout the school. This is done before the devices are purchased. As new technologies are introduced, the E-Safety Policy is updated and all users made aware of the changes. The following are examples of commonly used technologies in school: Email: Staff and children are only allowed to use e-mail in school that has been created by the IT Manager/Teacher (Mr Simon Smith).

These e-mail addresses are created using the school e-mail system and can be accessed, monitored, amended and deleted by SLT or Mr Simon Smith.
Anti –Virus: The school anti-virus software (Sophos) greatly reduces the risk of threats to equipment and the filtering system (Netsweeper) filters out any inappropriate images or content making the school e-mail system safe and manageable. Staff and children are made aware of what to do if they encounter anything that makes them feel uncomfortable. Staff are made aware of this through regular staff meetings and children through e-mail and e-safety lessons taught in school. In our school, the following statements reflect our practice in the use of email.

Social Networks: Many adults and pupils regularly use Social Network sites, e.g. Club Penguin, Moshi Monsters, Facebook or Twitter, although the minimum age for registering for some of these excludes primary school pupils. These communication tools are, by default, 'blocked' through the internet filtering system for direct use in Lancashire schools. However, comments made outside school on these sites may contravene confidentiality or bring the school or staff into disrepute. Staff are constantly made aware of the use of social media networks and are advised to only use these for personal use. Pupils and parents must not be contacted through social networks or made 'friends' and staff are aware of sanctions for inappropriate use. Children are taught dangers of using social media in Upper Key stage 2

Instant Messaging: This popular tool used by adults and pupils allows 'real time' communication and often integrates the ability to transmit images via a webcam. Although these sites are 'blocked' for use in Lancashire schools by default, they can be used offsite. Staff are not to use IM to contact parents or children without permission from a member of the SLT whether this is in school or offsite. FaceTime on iPads must not be used to contact other children or members of staff without prior permission form a member of the SLT.

Virtual Learning Environment (VLE) / Learning Platform: Seesaw is used throughout the school for sharing homework and setting work in event of a bubble being closed due to Covid 19. Seesaw allows children to access homework or resources uploaded by teachers. Children and staff are reminded about the importance of keeping log in details including passwords safe. Teachers are responsible for all content added to Seesaw and help/advice with this VLE is provided by the school IT Manager/Teacher (Mr Simon Smith). Once children have left school, their account should be removed within 12 months of them leaving. This is the responsibility of the class teacher.

Web sites and other online publications

The Bradley Primary School website is constantly updated with policies, newsletters, parent information and what is going on in school. This is done by Mr Simon Smith (IT Manager/Teacher), Class teachers and the office staff. Mr Smith is responsible for what appears on the website and all content added by non-administrators needs to be authorised prior to it going live.

Infrastructure and technology

The school IT Manager/Teacher (Mr Simon Smith) ensures that the infrastructure/network is as safe and secure as possible. The school subscribes to fibre broadband which is provided by Schools Broadband. Internet content filtering is provided by default (Netsweeper). It is important to note that the filtering service offers a high level of protection but occasionally unsuitable content may get past the filter service. If unsuitable content does get past the filter service, this must be reported to the IT Manager/Teacher (Mr Simon Smith) who can report and block any such content. Children must only use Infrastructure and technology in the presence of an adult and are aware of what to do if unsuitable content is encountered. This is taught to all children during computing classes delivered by the school IT Manager/Teacher (Mr Simon Smith). Sophos Anti-Virus software is included in the school's subscription and is installed on all computers in school and then configured to receive regular updates.

Pupil Access: Computing education is important for pupils to make sense of and to contribute positively to our technologically diverse world. At Bradley primary school, we provide children with technology to assist them with their learning. This includes a computing suite that children attend once a week for computing lessons with Mr Smith, iPads in each classroom and laptops that can be used as and when required. Children can only access infrastructure and technology in the presence of a trusted adult i.e. Teacher or TA. They are taught to report any unsuitable content to a trusted adult. Children have class log-ins, which are created and managed by the school IT Manager/teacher (Mr Simon Smith).

Passwords: Each class has their own log in and password that they are taught at the beginning of each year. The log in passwords do not need to be secure as the IT Manager / Teacher (Mr Simon Smith) monitor this. The administrator password is known only by the school IT Manager/teacher (Mr Simon Smith). This can be accessed by SLT by contact BT Lancashire Services if required.

Software/hardware: Software is only installed by the school IT Manager/teacher (Mr Simon Smith) A username and password known only by the T Manager/Teacher is required when installing any software. This can be accessed by SLT by contacting BT Lancashire Services if required. All required licencing including operating system, office, apps etc. is monitored and kept up to date by the school IT Manager/Teacher (Mr Simon Smith). Hardware is purchased by the IT Manager and is security marked by the office staff prior to being given to staff or put in classrooms. This is maintained and monitored by the school IT Manager/teacher (Mr Simon Smith). An audit of all software and hardware is carried out regularly (at least once a year).

Managing the network and technical support: The school employs an IT Manager (Mr Simon Smith) to manage the network and is available for technical support to other members of staff as and when required. His role includes:
· Ensuring servers, wireless systems and cabling is securely located and physical access is restricted.
· Ensuring all wireless devices have security enabled and passwords are kept secure.
· Ensuring relevant access settings been restricted on tablet devices e.g. downloading of apps or ‘in- app’ purchases.

· Managing the security of the school network.
· Regularly reviewing the safety and security of the school network.
· Ensuring computers are regularly updated with critical software updates/patches.
· Ensuring all users have clearly defined access rights to the school network.
· Installing software as and when required.
· Respond to breaches in security or suspicion of breaches of security.
· Ensuring external hard drives/pen drives and not used in school without authorisation.
· Ensuring school equipment is monitored and checked for viruses, threats or inappropriate material or software.
· Liaising with the school SLT with any issues/problems.

Filtering and virus protection: Filtering is managed by the school IT Manager/Teacher (Mr Simon Smith) who has control of what websites can be blocked/unblocked. All staff are aware that they must report any threats to equipment by viruses to the IT Manager/Teacher (Mr Simon Smith) as soon as possible.

Dealing with incidents

All incidents must be report to the school IT Manager/Teacher (Mr Simon Smith). This can be done by completing an incident form, e-mailing him or leaving a message in his room. Incidents that are illegal, concern the IT manager or the person reporting the incident feels the need to report it to a member of the school SLT, must contact the head teacher. The head teacher must refer illegal offences to the relevant external authorities e.g. Police, CEOP, Internet Watch Foundation (IWF). Children are taught to turn monitors off if inappropriate material on websites is displayed and report this to the IT Manager/teacher or to tell a trusted adult.

If someone whether it is a child or member of staff is accessing inappropriate websites purposely, using other peoples log ins, deliberately searching for inappropriate content, using external hard drives/pen drives in school, or using chat rooms forums etc. in inappropriate ways, then this needs to be reported to the IT manager/Teacher or a member of the SLT.

Education and Training

Both adults and children need to be digitally literate and aware of the benefits that the use of technology can provide. However, it is essential that children are taught to use technology responsibly, securely and safely, being able to recognise potential risks and know how to respond. They should, for example, be able to communicate safely and respectfully online, be aware of the necessity to keep personal information private, be taught how to search effectively and be discerning in their evaluation of digital content and be aware of the need to respect copyright and Intellectual Property rights. The three main areas of E-Safety risk (as mentioned by OFSTED, 2013) that your school needs to be aware of and consider are:

· Children need to be taught that not all content is appropriate or from a reliable source, e.g. inappropriate content, pro anorexia, self-harm sites, hate sites etc.
· Children need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies e.g. grooming, cyberbullying, identity theft etc.
· Children need to be made aware that their personal online behaviour can increase the likelihood of, or cause harm to themselves and others e.g. disclosure of personal information, health and wellbeing, sexting, copyright etc.

When teaching computing it is important to identify and order the underlying knowledge. Mr Smith teaches computing throughout the school from reception class all the way through to the end of year 6 when the children leave for secondary school. Long-term plans for the topics taught for each year group are agreed during staff meetings with Mr Smith, class teachers and SLT. Assessment is done yearly so Mr Smith and the class teachers know where the children are at with their learning and children are ready for what comes next. The number of subject specialists for computing is low.

This is having a negative impact on the quality of education the children receive in computing. Mr Smith is educated to degree level in a computing subject and is a trained primary school teacher. Therefore, at Bradley primary school, the children have access to a teacher who has excellent subject knowledge and we feel that the children leave primary school with great knowledge in key topics for computing.

E-Safety across the curriculum

Children are taught about the threats and risks involved and how to stay safe online throughout their time at Bradley Primary School. This is covered in computing classes and during other lessons when children are going online. This is progressive though all years and children are constantly asked and taught about risks and threats when using the internet. E-Safety and Staying Safe displays are present in the computing suite and each classroom has posters and reminders of how to stay safe online that have been created by the children. Children are taught about the threats and risks involved and how to stay safe online throughout their time at Bradly Primary School. This is covered in computing classes, within the classroom and during assemblies. This is progressive though all years and children are constantly asked and taught about risks and threats when using the internet. E-Safety and Staying Safe displays are present in the computing suite and each classroom has posters and reminders of how to stay safe online that have been created by the children.

Every year the school holds an online safety week, which raises more awareness about staying safe online. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. ” (Byron Report, 2008). Bradley Primary School offer opportunities for parents to be informed about E-Safety through Newsletters, school website and the E-Safety policy, which is available to be viewed via the school website. Parents are also invited into school for an online safety talk that is carried out by a teaching member of staff who has had relevant training.