Broadway Infant School

E-Safety Policy

Signed (chair):	Name:	Date:
Signed (Head):	Name: Juliet Lambert	Date: 11/5/2018
Date of review June 2019	Reviewed by: Resource committee	Next Review: June 2020
Date of review May 2021	Reviewed by: FGB	Next Review: May 2022
Date of review June 2022	Reviewed by: Resource committee	Next Review: June 2023
Date of review	Reviewed by:	Next Review:
Date of review	Reviewed by:	Next Review:

Footnote: Senior staff and governors will always check for any known changes in legislation or local requirements before applying this policy.

Broadway Infant School

Footnote: Senior staff and governors will always check for any known changes in legislation or local requirements before applying this policy.

E-Safety Policy

To be read in conjunction with all other policies plus:-
Equality and Community Cohesion Scheme

Introduction

Everyone at Broadway works together as a Professional Learning Community ensuring we have a learning environment which values the use of new technologies, enhances learning, encourages responsible use of ICT and follows agreed protocols and procedures to minimise potential e-safety risks.

This policy is in place to ensure:

- The e-safety of all members of the school community
- The ICT infrastructure of the school is secure and not open to misuse or malicious attack
- Users understand why they may only access the school's networks through a properly enforced password protection system, in which passwords are regularly changed when appropriate
- All children understand how to safely use Information and Communication Technology
- All other stakeholders understand their own responsibilities in relation to e-safety
- All stakeholders know, or know where to look to find, the correct procedures or responses plus actions to take, if they are confronted with an event or product that has potential e-safety concerns.
- Parents and Carers understand and support all protocols and procedures that are in place so that we do minimise potential e-safety risks.

Roles and responsibilities

The governing body is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DESIGNATED SAFEGUARDING LEAD's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The headteacher / DESIGNATED SAFEGUARDING LEAD is responsible for:

- Acting as the named point of contact within the school on all online safeguarding issues.
- Keeping up-to-date with current research, legislation and online trends.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.

Footnote: Senior staff and governors will always check for any known changes in legislation or local requirements before applying this policy.

- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting and maintaining records of online safety incidents and inappropriate internet use, both by pupils and staff.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Ensuring appropriate referrals are made to external agencies, as required.
- Reporting to the governing body about online safety on a termly basis.
- Working with the governing body to update this policy on an annual basis.

Computing Subject leader is responsible for:

- Ensuring online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Providing support for parents and families with regard to keeping their children safe online. This support / information may be in the form of information provided on the website, leaflets / materials sent home and parents meetings.

ICT technicians (INTEGRA) are responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.
- Reporting concerns about online safety on CPOMS and discussing these with the headteacher / DESIGNATED SAFEGUARDING LEAD.

Pupils are responsible for:

- Taking part in e-safety lessons and activities.
- Adhering to the Pupil Acceptable Use Agreement and school rules.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.

Footnote: Senior staff and governors will always check for any known changes in legislation or local requirements before applying this policy.

Parents/Carers are responsible for:

- Read, understand, adhere to and sign on behalf of their child the Parent/Carer Acceptable Use policy.
- Keep any passwords / log in details secure for subscriptions provided by the school.
- Ensure they model the same levels of protection within the home whenever possible.
- Attending e-safety parents events / reading information about online safety and supporting the school by re-enforcing e-safety messages at home.

The Curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in computing lessons.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using.

Pupils are taught what to do if anything appears that makes them feel uncomfortable or unsafe.

Online safety teaching is always appropriate to pupils' ages and developmental stages.

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always reviews and evaluates the resource.

Class teachers ensure that any internet-derived materials are used in line with copyright law.

Pupils are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

Remote learning

All staff and pupils using audio / video communication must:

- Wear suitable clothing – this includes others in their household.
- Be situated in a suitable 'public' living area within the home with an appropriate background – 'private' living areas within the home, such as bedrooms, are not permitted during video communication.
- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute video material without permission.

Footnote: Senior staff and governors will always check for any known changes in legislation or local requirements before applying this policy.

- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they are visible.

Pupils not using devices or software as intended will be disciplined in line with the Behaviour Policy.

The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

Staff training

All staff receive safeguarding and child protection training, which includes online safety training, during their induction.

Online safety training for staff is updated annually and staff also receive regular online safety updates as required.

The DESIGNATED SAFEGUARDING LEAD and any deputies undergo training to provide them with the knowledge and skills they need to carry out their role, this includes online safety training. This training is updated at least every two years.

In addition to this formal training, the DESIGNATED SAFEGUARDING LEAD and any deputies receive regular online safety updates to allow them to keep up with any developments relevant to their role. In relation to online safety, these updates allow the DESIGNATED SAFEGUARDING LEAD and their deputies to:

- Understand the unique risks associated with online safety and be confident that they have the relevant knowledge and capability required to keep pupils safe while they are online at school.

- Recognise the additional risks that pupils with SEND face online and offer them support to stay safe online.

All staff receive a copy of this policy upon their induction and are informed of any changes to the policy.

Staff are required to adhere to the Staff Code of Conduct and the Acceptable Use Policy at all times.

All staff are informed about how to report online safety concerns.

The headteacher / DESIGNATED SAFEGUARDING LEAD acts as the first point of contact for staff requiring advice about online safety.

Digital Communication

Staff are given approved school email accounts and are only able to use these accounts at school and when doing school-related work outside of school hours.

Personal email accounts are not permitted to be used on the school site or for school related communication.

Any email that contains sensitive or personal information is only sent using secure and encrypted email or via a secure information transfer site (e.g. Sofie).

The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff are made aware of this.

Users must immediately report, to the Headteacher the receipt of any email, text etc. or the appearance of any images when using the Internet that makes them uncomfortable, is offensive, threatening or bullying in nature. Users must not respond to any such contact.

Social Media

Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school.

Staff receive training on how to use social media safely and responsibly.

Staff are not permitted to communicate with pupils or parents over their personal social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media.

Where staff have an existing personal relationship with a parent or pupil, and thus are connected with them on social media, e.g. they are close family friends with a parent at the school, they will disclose this to the headteacher and will ensure that their social media conduct relating to that parent is appropriate for their position in the school.

Footnote: Senior staff and governors will always check for any known changes in legislation or local requirements before applying this policy.

Social Media use on behalf of school

The school's official social media channels are only used for official educational or engagement purposes.

Staff members must be authorised by the headteacher to access to the school's social media accounts.

All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.

The school website

The headteacher is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law.

Personal information relating to staff and pupils is not published on the website.

Images and videos are only posted on the website if relevant permission have been gained.

Digital and video images – Photographic, Video

When using digital images, staff will teach children about the risks associated with taking, using, sharing, publishing and distributing images appropriate to their young age. In particular staff will discuss with children the risks attached to publishing their own images on the internet in relation to open and public sites e.g. social networking sites.

Staff are allowed to take digital /video images to support educational aims but they must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such a purpose.

Care should be taken when taking digital/ video images that children are appropriately dressed and are not participating in activities that might bring the individual or the school into disrepute.

Children must not take, use, share, publish or distribute images of others without their permission

Where children are using mobile devices, cameras and video:

- Teach children that they have a responsibility to consider and respect the feelings of others when capturing images
- Ensure images are stored safely, securely and only shared with appropriate people in accordance with this policy

Footnote: Senior staff and governors will always check for any known changes in legislation or local requirements before applying this policy.

Publishing Images/ children's work

Consent will be gained from Parents/Carers before publishing recognisable photos of children on our school website and/or our closed school Facebook page.

Consent will be gained from Parents / Carers before photos of children are sent to the local press.

Children's work can only be published with the permission of the child and their Parent/Carer.

Technical – infrastructure/equipment, filtering and monitoring

The school broadband Internet access is provided via BT via INTEGRA traded services and this includes a filtering service to limit access to unacceptable material for all users.

The school uses INTEGRA schools IT and is therefore covered by the relevant Local Authority E-Safety Policy and guidance.

Servers, wireless systems and cabling are securely located within the building and physical access is restricted.

The school's network and school-owned devices are appropriately monitored.

Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are reviewed and monitored by INTEGRA Schools IT to ensure they are running correctly.

Technical security features, such as anti-virus software, are kept up-to-date and managed by INTEGRA schools IT.

Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments.

Staff members and pupils report all malware and virus attacks to INTEGRA schools IT.

All users have clearly defined access rights to school ICT systems and are provided with individual user names and passwords.

Users are responsible for the security of their user name and password. They must not allow other users to access the system using their log on details and must immediately report any suspicion or evidence that there has been a breach in security to the Headteacher.

Users are required to lock access to /log off devices and systems when they are not in use.

Teachers can only take data off site using their designated teacher laptop, which is password protected.

Footnote: Senior staff and governors will always check for any known changes in legislation or local requirements before applying this policy.

Teachers who use an alternate Internet provider whilst working at home using their school laptop, are responsible for ensuring all information and data linked to the school remains secure.

General Data Protection Regulation

The school complies with the General Data Protection Regulation.

Staff must ensure they:

- Take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly 'logged off' at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

Managing reports of online safety incidents

Concerns regarding a staff member's online behaviour are reported to the headteacher who decides on the best course of action in line with the relevant school policies.

Concerns regarding a pupil's online behaviour are reported to the headteacher/DESIGNATED SAFEGUARDING LEAD who investigates concerns with relevant staff members and are dealt with in accordance with relevant school policies.

All online safety incidents and the school's response are recorded on CPOMS.

Monitoring

The monitoring of the schools' responsibilities in relation to E-Safety work is the combined responsibility of the Governing Body and will be reviewed annually.

Footnote: Senior staff and governors will always check for any known changes in legislation or local requirements before applying this policy.