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	Reviewed by:	Next Review:
Date of review	Reviewed by:	Next Review:
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.

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

E-Safety Policy 2019-20

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.

Aims

We aim to ensure:

- We enable children to safely benefit from and use all new technologies appropriate to their age and skills.
- Parents and Carers understand and support all protocols and procedures that are in place so that we do minimise potential e-safety risks.
- We keep up-to-date and regularly inform all stakeholders in relation to e-safety issues so that everyone is confident that they can play their part in ensuring children remain safe and operate within a safe on-line environment both in school, at home, and in the wider community.

This in turn also contributes to the support of our whole school aims- children will:

Be safe, happy, enthusiastic and ready to learn together
Experience learning through a creative fun and fulfilling curriculum
Have enquiring minds that explore, investigate and question
Gain a sense of achievement and satisfaction
Feel part of the local community and the wider world.

Objectives:

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
The school meets the e-safety technical requirements outlined in the SWGFL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
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 all 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.
SWGFL is informed of any issues relating to the filtering applied by the Grid

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

Staff

All staff will be made aware of their responsibilities with regard to e-safety and will be made aware of the potential serious child protection issues which could arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying

The Designated person for Child Protection in our school is the Headteacher. He/she will be trained in relation to e-safety and will ensure that staff E-Safety training takes place in conjunction with Child Protection training.

All staff, including Supply Teachers, will be expected to maintain an up to date awareness of e-safety matters and the current school e-safety policy and practices. They will have read, understood and signed the school's Staff Acceptable Use Agreement. (Appendix 1 and 3) They will report any suspected misuse or problem to the Headteacher for investigation/ action/sanction. Any digital communication between members of our Professional Learning Community e.g. staff, Parent/Carers, children, Governors etc. via Email/Learning Platforms/voicemail etc. must be professional in tone and content and only carried out using official school systems. All new staff will be give e-safety guidance and training.

Staff will integrate reinforcing the need for e-safety awareness within any appropriate learning tasks they offer to children in their care. They will take responsibility for supervising and monitoring children whilst engaged in learning using ICT and ensure:

Where Internet use is pre-planned teachers should:

- Guide children to sites checked as suitable for their use
- Ensure processes are in place for dealing with any unsuitable material that is found in Internet searches
- Teach children what to do if anything appears that makes them feel uncomfortable or unsafe

Where email/blogs etc. are used, because the official school email service/learning platform may be regarded as safe and secure and is monitored:

- Only use school based email/blogs etc.
- Teach children what is/is not considered acceptable to use or include within email/blog etc. correspondence
- Ensure children are only accessing known contacts vetted by the teacher/school

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.

Where children are using mobile devises, 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

Parents/Carers

Parent/Carers play a crucial role in ensuring that their children understand the need to use the Internet/mobile devises in an appropriate way. Our school therefore takes every opportunity to help Parents/Carers understand the issues that surround e-safety through Parent/Carer Information Events (P.I.E), newsletters, website, the learning platform plus information about local e-safety campaigns.

Parents and Carers will be expected to:
Read, understand, adhere to and sign on behalf of their child the school's Family Acceptable Use Agreement. (FAUA) (Appendix 5)
Access the school website/learning platform in accordance with the FAUA
Support the school in ensuring they model the same levels of protection within the home whenever possible.
Parent/Carers need to be aware that the school's E-Safety Policy covers their child's actions out of school, if related to their membership of the school (For example whilst using the learning platform or website) so it is in all stakeholder's interests to continually promote e-safety good practice.

To help Parents and Carers to achieve this, the school will also offer if requested, individual advice and guidance in relation to the safe use of ICT within the home, in addition to information covered by whole school e-safety events.

Children

Whilst recognising that the children within our school are very young, they will be expected to learn about the correct way to behave when using ICT and once they have gained this knowledge, in the same way that they are expected to know how to behave appropriately in school, they will be expected to take responsibility for their actions when using ICT. As their e-safety awareness develops they will be expected to apply this learning to all future learning tasks. As part of the teaching of e-safety they will be asked to read, understand, adhere to and sign a Children's Acceptable Use Agreement (CAUA) (Appendix 4) when they enter Year 1 and 2. A copy of this CAUA will be sent home to share with Parents/Carers. Reception children will also have a form but this will be signed on their behalf by the parent/carer after it has been shared with the child.

Children will also be taught about the importance of adopting good e-safety practice when using digital technologies out of school because the school's E-Safety Policy covers their actions out of school, if related to their membership of the school. (For example whilst using the school's learning platform or website)

Community Users

In the event of Community Users requiring access to the school's ICT systems as part of the school's extended schools provision they will be expected to sign a Community User AUA before being provided with access to school systems. (Appendix 3)

Governors

Governors will receive and e-safety update annually as part of the Headteacher's Report. They will take part in e-safety training/ awareness sessions whenever possible.

Technical – infrastructure/equipment, filtering and monitoring

The school broadband Internet access is provided via Virgin Media and is therefore covered by their Security Policy and Acceptable Usage Policy.

The school managed service is provided by South Gloucestershire Local Authority 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.

All users have clearly defined access rights to school ICT systems

All users are provided with individual user names and passwords however the user name and password for our very youngest children may be shared with Parents/Carers and teachers who are responsible for keeping the integrity of these passwords secure.

User IDs and passwords have been created which are differentiated to the ability levels of the children because we recognise a balance has to be drawn between the character requirements of a secure password and a young child's ability to recognise letters and use a computer keyboard.

The 'master/administrator' passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher and is kept in a sealed envelope in the school safe. All other passwords associated with the management of the school are known by the Headteacher and the Deputy Head and are also kept in a sealed envelope in the school safe.

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.

The school maintains and supports the managed filtering system provided by SWGfl. Any filtering issues should be reported immediately to the Headteacher and SWGfl.

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.

The school infrastructure and individual work stations are protected by up to date virus software.

Teachers can only take data off site using their designated teacher laptop, which is password protected or their designated teacher memory stick, which is password protected and encrypted, therefore all staff are encouraged to use remote access whenever possible.(Appendix 6)

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.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the Foundation Stage and key Stage 1 curriculum

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

Publishing Images/ children's work

Photographs published on our learning platform will be carefully selected and will comply with good practice guidance on the use of such images.

Photographs of children will not be published on the school website.

Photographs which celebrate children's achievements in school will be sent to the local press from time to time if Parents/ Carers have given their permission for this to take place.

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

General Data Protection Regulation

The school complies with the General Data Protection Regulation.

Staff must ensure they:
At all times 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 devises, 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 devises

Responding to incidents of misuse

If any apparent or actual misuse appears to involve illegal activity i.e.

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminal racist material
- Other criminal conduct, activity or material

The SWGfL flow chart should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

Monitoring

The monitoring of the schools' responsibilities in relation to E-Safety work is the combined responsibility of the Headteacher and the assigned Governor.

The responsibility for this policy has been delegated to the Headteacher. This policy will be reviewed at least every three years.

Signed: Juliet Lambert

Headteacher

Date: 11/05/2018

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