Safeguarding - E-Safety

SCHOOL

1

BFS

Headteacher	Chair of Governors	Review Dates
		Last Review: July 2021
Lisa Keighley	Philip Cavalier-Lumley	Next Review: July 2022

1. Policy

It is the aim of Blakehill Primary School to create a secure and safe environment that develops technology skills and provides pupils with an awareness of potential e-safeguarding issues.

This policy provides advice and clear guidance in order to ensure all internet users are aware of the risks and the benefits of using the internet and what happens if this policy is breached.

2. Purpose

New technologies have become integral to the lives of children and young people in today's society, both outside and within school.

3. Scope

All staff, children and visitors to Blakehill Primary School.

4. Principles

The internet, other digital and information technologies are powerful tools which open up opportunities for all. These technologies can stimulate discussion, improve literacy, communication skills, promote creativity and increase awareness of the context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

However, the use of these new technologies can put young people at risk both inside and outside of school. Some of these dangers may include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to loss of or sharing of personal information
- Inappropriate communication or contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video or internet games
- Potential for excessive use which may impact upon the social and emotional development and learning of the young person

- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- The sharing or distribution of personal images without an individual's consent or knowledge
- The risk of being subject to grooming by those with whom thay make contact on the internet.

The above list is not exhaustive.

It is impossible to eliminate the above risks completely. It is essential, therefore, through the provision of good education, that we build pupils' awareness to these risks. Our aim is to build pupil confidence and understanding to seek advice to be able to deal with any risks in an appropriate manner.

E-Safety incidents that may occur outside the school may be investigated by staff if they impact on pupils' wellbeing.

Internet Provision

The school internet is provided by the Bradford Learning Network, a DFE accredited educational internet service provider. All sites are filtered using the Smoothwall filtering system which generates reports on user activity. Additional forensic software filtering is conducted by Policy Control. Monthly e-mail reports are sent to the e-safety coordinator.

5. Responsibilities

Governing Body

The school governors are responsible for the approval of this policy for reviewing the effectiveness of the policy within school. This will generally be carried out by the Link Governor who sits on the E-Safety Committee.

The Link Governor is responsible for:

- Attending E-Safety Committee meetings held each term
- Monitoring e-safety logs
- Reporting and updating the full governing body and Buildings, Staffing and Finance Committee on a regular basis.

Head of School and Senior Leadership Team

The role and responsibilities of the Headteacher and Senior Leadership team includes:

- The Headteacher is responsible for ensuring the safety (including e-safety) of all members of the school community. The day to day responsibility is delegated to the e-safety coordinators.
- Ensuring the e-safety coordinators receive suitable and relevant continued professional development to enable them to carry out their duties as well as train other colleagues as and when appropriate.

- Awareness of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. This is detailed in the Child Protection Policy.
- Awareness of ‘Actions upon discovering inappropriate or illegal material’ guidance from the Bradford Curriculum ICT team.

The E-Safeguarding Committee

Blakehill Primary School has a committee who meet regularly to discuss and review policies and follow up on any e-safety incidents written on the e-safety log. They are responsible for developing e-safety action plans, taking action, reviewing progress made and communicating to relevant parties.

Notes from the E-Safety Committee meetings are recorded, filed and held in the e-safety coordinators files.

The Committee will consult with the School Network Manager on any technical issues relating to safeguarding and the security of data.

Details of the E-Safety Team are posted on the School Notice Board.

E-Safety Co-ordinators

The role and responsibilities of the e-safety coordinators includes:

- Day to day responsibility for e-safeguarding issues and has a leading role in establishing and reviewing the E-Safety Policy and Procedures
- Ensuring that all staff are aware of the procedures to follow in the event of an e-safety incident taking place. This should be carried out at the beginning of each new year and if a new member of staff joins during the academic year
- Receiving and reporting e-safety incidents and recording all incidents in the e-safety log
- Ensuring all incidents are dealt with according to the school’s Behaviour Policy and that the Headteacherl, Class Teacher, Parents and other parties are informed, where appropriate
- Coordinating the E-Safety Committee meetings and writing term reports for the Governors
- Monitoring and reviewing the e-safety teaching and learning taking place across the school
- Monitoring and reviewing the monthly Smoothwall filtering reports and Forensic Software reports (Policy Central) that are received via e-mail to school on a weekly basis.

Network Manager

The Network Manager is responsible for:

- The schools ICT infrastructures are secure and not open to misuse or malicious attack or damage
- Maintains up to date e-safety technical information and communicates to appropriate personnel including the e-safety coordinators
- Monitors software and antivirus software ensuring it is implemented and updated accordingly.

Teaching and Support Staff

Teaching and Support staff are responsible for:

- Keeping up to date of all e-safety matters and current *E-Safety Policy* and Procedures through staff meetings and training sessions
- Read, understand and sign the school's *Acceptable Use Policy*
- Understand the process for reporting e-safety incidents within school including the recording the incident in the e-safety log
- Report any suspicious misuse or problem to the E-Safety Coordinator for potential investigation
- Ensure all digital communications with pupils is professional and only carried out on official school systems
- Ensure the e-safety issues are embedded in all aspects of the curriculum
- Ensure that e-safety lessons are planned and taught every half term. Lessons should be age appropriate or reflect the needs of the age group being taught
- Ensure pupils understand and follow the pupil *Acceptable Use Policy*. Training should be provided on these policies at the beginning of each new academic year and for any new starters who join at a later stage of the academic year
- Ensure that pupils are aware of the e-safety issues relating to mobile phones, cameras and any hand held devices. The use must be monitored according to current school policy
- Ensure that any confidential files are saved on an encrypted memory stick and passwords remain confidential
- Ensure that at the end of each academic year, photographs are deleted or where applicable stored in an agreed location for school use. At the end of the current Year 6, all photographs are to be deleted.

Named Link Person for Child Protection

The named person/s responsible for child protection are trained in e-safety issues and are aware of the potential for serious child protection issues that may arise from:

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

Pupils

Pupils are responsible for using the school ICT systems and equipment in accordance with the pupil *Acceptable Use Policy*. They are briefed annually on the content of this policy and are asked to sign to verify. It is displayed in the classrooms.

Pupils are encouraged through e-safety / PSHE lessons and assemblies to share any e-safety concerns with a trusted adult.

Parents / Carers

The school will take every opportunity to help and support parents / carers to understand e-safety issues. The school will raise awareness of the key issues in the following way:

- Parent / Carer Annual meeting on E-Safety
- Acceptable Use Policy and the Mobile Devices Policy are on the School Website
- Information about e-safety and parental resources are available on the School Website
- Parents / Carers views are sought annually in an e-safety questionnaire
- Information is shared via newsletters and letters.

Community users / School Visitors

Community users and school visitors are able to log onto our BYOD (bring your own device) network. This ensures that they do not access the school network at all. The use of this is regularly monitored by the school Network Manager.

6. Procedures

Pupil Education

The education of pupils in e-safety is a crucial part of the school's e-safety provision. Children need the help and support of the school to recognise and avoid e-safety risks and to build their awareness of how to keep themselves safe. E-safety education will be provided in the following ways:

- A planned e-safety programme is delivered through ICT and PSHE in the form of the Common Sense / SWGFL Digital Literacy Scheme
- The Bradford ICT Scheme of work highlights e-safeguarding issues that arise in the context of ICT lessons
- Rules for Acceptable Use are shared at the beginning of each academic year and with any new starters as they join school
- Pupils are made aware of the process to follow if they see anything online which they find upsetting or which is unsuitable for children (Turn off and Tell)
- Pupils are made aware that any events of cyber-bullying are taken seriously by the school and are taught to understand the importance of sharing their concerns with a trusted adult
- Copyright free images and audio sources are shared with pupils and are included in the Bradford ICT Scheme of Work.

Pupils are taught:

- in all lessons to be aware on the content that they access online and learn how to validate the accuracy of the information they find
- how to search for information safely and safe search engines are used by teaching staff
- to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Staff Education

It is essential that all staff receive regular e-safeguarding training and they understand their responsibilities as outlined in this policy. Training will be offered as follows:

- Annual e-safety training to be delivered by the e-safety coordinator
- An annual audit of staff e-safety training will be completed and any training needs identified will be used to plan future training
- The results of the annual questionnaire from parents / carers and pupils will highlight any relevant issues to the school or particular year groups. These will be used to direct training.
- All staff will receive a briefing and a copy of the *Acceptable Use Policy* and the *E-Safeguarding Policy* on an annual basis.
- New starters will receive copies of the policies as above in their Induction pack.

The E-Safety Coordinator has completed NSPCC ceop approved e-safety training.

Planning and e-safety work will be monitored regularly and will be used to direct training.

Managing ICT systems and access

Access to ICT systems is managed by the Network Manager and ICT/e-safety Coordinators. All pupils receive logins and accounts for:

- School systems
- Purple Mash
- RM Maths
- Google Classrooms

A team of pupils (Blakehill Bloggers) also have access to the school blog. These accounts are managed through administrator privileges which are only known to the Network Manager and e-safety coordinators. Accounts are created for new starters at the beginning of the academic year and any new starters that join during the school year. Accounts are deleted annually for any leavers including those pupils in Year 6.

Adult accounts and passwords are also created in the same way. Adults are given accounts for the same school systems plus the school blog. Accounts are created and deleted for new starters and leavers as required.

Passwords

All users (both staff and pupils) have the responsibility for the security of their user name and password and must not allow other users to access the systems using their login details. Any concerns about sharing passwords or logon details must be reported to the e-safety coordinator.

- Passwords for new users and replacement passwords for existing users can be allocated by the e-safety coordinator or Computing Lead
- Staff are made aware of the school's password rules via Induction, the Acceptable Use Policy and this policy.

- Pupils are made aware of the school's password rules via Computing/E-Safety lessons and through the Pupil Acceptable Use Policy.
- Old user names and accounts are deleted at least annually.
- All pupils have their own individual passwords and login for accessing the school's ICT systems. These passwords are changed periodically.

Personal Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

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

All staff must ensure that:

- Safe keeping of personal data at all times to minimise the risk of loss or use
- Use personal data only on secure password protected computers and other devices such as encrypted memory stick, ensuring that they properly 'logged off' at the end of any session in which they are using personal data
- Ensure that memory sticks used are password protected
- Ensure that information is saved on secure drives that can only be accessed by password.

Use of digital and video images (photographic and video)

- Staff should inform and educate pupils about the risk associated with the taking, use, sharing, publication and distribution of images
- Staff are allowed to take digital/video images to support educational aims. These images should only be taken on school equipment. Personal equipment should not be used for these purposes. All classes have an iPad for this purpose
- The school *Media & Photo Policy* states that parents must inform the school in writing if they wish to opt out of this policy. The policy states that school will take pictures/videos/audio of pupils to be used within school and on the school blog and website. A list of pupils who have opted out will be kept in the class register and in the office.

- Photographs will be published with first names only on the blog, website and in the press. In incidences where names are required (some media/newspapers) parental permission will be sought.
- Teaching staff are responsible for storing photographs and images safely and securely. Staff will also ensure images are deleted annually and once the pupil/s have left the school.

Responding to incidents of misuse

All members of the school community are held responsible as users of ICT. There may be incidents when infringements of this policy could take place either through careless or irresponsible behaviour or through deliberate misuse.

If apparent or actual misuse appears to involve illegal activity such as:

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

The above list is not exhaustive.

If any of the above occurs it is important that the device is not shut down as evidence could be erased but that it is moved to a secure site. All matters must be reported to the Head of School / Designated Safeguarding Lead or an E-Safety Coordinator.

If misuse has taken place which is not illegal it is important that any incidents are dealt with in an appropriate manner and members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through the normal behaviour / disciplinary procedures.

Whilst it is impossible to record possible sanctions for every eventuality, a list of types of misuse and sanctions are included in Appendix c. and d.

Cyber-Bullying

Cyber bullying is the use of electronic communication to bully a person. This may take the form of sending messages of an intimidating or threatening nature. Examples of forms of electronic communication are social networking websites and apps, texting, use of mobile or tablet apps, email or online software.

Pupils are taught about cyber bullying through E-Safety and PHSE lessons. Pupils are encouraged to share concerns of cyber bullying with a trusted adult. The adults in school will support the pupil by:

- Collecting evidence of the bullying taking place by recording the date, time and where possible screen captures
- Advising the child not to forward on messages to other people as this may continue the bullying
- Advising the pupil not to reply to the messages.

Full details of how the school manages incidences of bullying can be found in the Anti-bullying Policy. The school may decide to report serious cyber bullying incidents to the Police.

Social Media

Blakehill Primary School uses social media in the following ways:

- A text to parents system which is managed by the school office. This is used as a reminder or information service for parents / carers.
- Our PTFA use a Facebook page to provide information service for parents / carers. The PTFA also use this page to inform / update / remind parents / carers about school events and PTFA meetings. This account is managed by the Chair, Secretary and Treasurer of the PTFA.
- A Twitter account is used to inform/update/remind parents about school events. This account is managed by the ICT coordinator.
- As part of the school website, we have a blog which our team of Blakehill Bloggers contribute. All comments and posts are moderated by the ICT coordinator before they are published. Pupils know they must not share personal information on the blog or use it to communicate with people they do not know in real life.
- All staff must keep their personal and professional lives separate on social media. Personal opinions should never be attributed to the school. The school's use of social media for professional purposes is checked regularly by the E-Safety Committee to ensure the school is complaint with this policy.

Mobile devices

Staff

Staff must not use mobile phones in lessons. Mobiles must be switched off or on silent or discreet mode during the following times:

- Teaching time (with the exception of urgent or exceptional situations)
- Playground duty
- During meetings

In accordance with the Acceptable Use Policy staff should not use personal devices for photography in school. Only school cameras or devices are allowed.

Pupils

School does not allow pupils to bring mobile phones into class. All mobile phones must be stored in the school office. They must be handed in at the office before the start of the day and returned at the end of the school day. As part of the literacy scheme of work pupils are taught about the dangers of using mobile phones. The fact that location services can say exactly where you are and how quickly children can post content online before thinking about the consequences.

School Mobile devices

Blakehill Primary School has a variety of mobile devices including iPads, iPods Touches, Acer Tablets and Chromebooks. All of the statements included in the Acceptable Use Policy apply to these mobile devices. Pupils are informed that they must not take photographs of other people without their permission. They are not allowed to download or install apps on any device. These devices are subject to the same levels of internet filtering as all the school computers accessed by pupils.

Please Note:

The school may exercise its right to monitor the use of the school's information systems and internet access to intercept email or to delete inappropriate materials where it believes unauthorised use of the schools information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound. (Regulation of Investigatory Powers Act 2000).

7. Monitoring and Review

The implementation, monitoring and review of this policy is the responsibility of the E-Safeguarding Committee.

Review of this policy will take place on an annual basis or more regularly if there are any significant new developments in the use of technologies or/and new threats of incidents that have taken place.

8. Distribution

This policy will be available on the Blakehill Primary School website or via the Headteacher.

9. Cross Referencing

This policy refers to the following policies:

Acceptable Use Policy (pupils and staff- see below)

Child Protection Policy

Mobile Devices policy

Media & Photo Policy

Anti-Bullying Policy

Safeguarding Policy

Data Protection Policy