Blacko Primary School

http://lancashire.schooljotter.com/blacko

E-Safety Policy

UPDATED: February 2019

COORDINATOR: Mr Jackson

REVIEW: February 2020
- Unless any statutory updates

POLICY

Contents

E-Safety Policy

Mission Statement

Our aim is to provide a happy, pleasant and stimulating environment where relationships between all members of the community - children and adults - are based on mutual trust, understanding and respect. The family feel of our school helps each child to develop his/her own personality in a secure and caring environment where we are mindful that toleration and respect of others are necessary attributes in a modern British civilised society.

Introduction

It is the duty of Blacko primary school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or the digital world as would be applied to the real world. Increasingly, children are accessing material through the Internet and games consoles that are not age appropriate. It is essential to address this and to encourage a lifestyle that incorporates a healthy balance of time spent using technology.

Aim

This policy is to protect the interests and safety of the whole school community and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements. It is linked and should be read in accordance with the following school policies: child protection, health and safety, behaviour and PSHE.

This policy is inclusive of both fixed and mobile internet, technologies provided by the school (such as PCs, laptops, whiteboards, tablet, digital video and camera equipment, etc) and technologies owned by pupils or staff.

The Technologies

Computing in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- E-mail
- Instant messaging
- Blogs
- Social networking sites
- Chat Rooms
- Gaming Sites
- Text messaging and picture messaging
- Video calls
- Podcasting
- Online communities via games consoles
- Mobile Internet devices such as Smart Phone and Tablets.

Whole School Approach to the Safe Use of Computing Technology

Creating a safe Computing learning environment includes three main elements at Blacko Primary School:

1. An effective range of technological tools which are filtered and monitored;
2. Policies and procedures, with clear roles and responsibilities;
3. A comprehensive E-Safety education programme for pupils, staff and parents.

Staff Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in Blacko Primary School and the Head Teacher, with the support of governors, aims to embed safe practices into the culture of the school. The Head Teacher ensures that the policy is implemented and compliance with the policy monitored. All staff are encouraged to create a talking culture in order to address any e-safety issues which may arise in classrooms on a daily basis. All visitors also receive our e-safety agreement on arrival at school.

The responsibility for e-Safety has been designated to a member of the senior leadership team. Our school e-Safety Coordinators are **Kate Richards** (Head Teacher), **Sean Jackson** (Assistant Head teacher) and **Kerrie Davis** (Computing Coordinator).

Our e-Safety Coordinators ensures they keep up to date with e-Safety issues and guidance through liaison with the PENNiNE Multi Academy Trust (MAT), Lancashire County Council and through organisations such as The Child Exploitation and Online Protection (CEOP) and 360 degrees safe. The school's e-Safety Coordinators ensures the Head, Senior Management and Governors are updated as necessary.

Staff Awareness

- All staff receive regular information and training on e-safety issues in the form of in house training and meeting time.
- New staff receive information as part of their induction.
- All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas and through a culture of talking about issues as they arise.
- E-safety records of concern are completed by staff as soon as incidents occur and are reported via the CPOMs software to the school's designated safeguarding team, Mrs Kate Richards and Mr Sean Jackson.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. These behaviours are summarised in the Acceptable Use Policies, which must be signed and returned before use of technologies in school.

Internet:

- Blacko Primary School uses BT Lightspeed "filtered" Internet Service and Impero, which will minimise the chances of pupils encountering undesirable material.
- Staff, pupils and visitors have access to the Internet through the school's fixed and mobile Internet technology.
- Staff should email school-related information using their NAME@blacko.lancs.sch.uk address and not personal accounts.
- Staff will preview any websites before recommending to pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher.
- The CEOP Report Abuse button is available on the school website. The following can be found on the school website:

Reporting Online Abuse

If you are upset or worried about something that has happened to you or your child on the internet you can report any issues to CEOP (Chick Here)

Teachers make children aware of this and when it is appropriate to use it.

- If staff or pupils discover an unsuitable site, the screen must be switched off immediately and the incident reported to the e-safety coordinator(s) detailing the device and username.
- Staff and pupils are aware that school based email and Internet activity is monitored and can be explored further if required.
- Pupils using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher and then an STL member.
- Pupils are taught the rules of etiquette in email and are expected to follow them.
- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.

- Pupils consistently choosing not to comply with these expectations will be warned, and subsequently, may be sanctioned following the school's behaviour policy.
- Summaries of these ICT rules are displayed in the ICT suite and all areas with ICT resources. Pupils will be asked to sign this agreement, ensuring that they are aware of expectations (See Appendix). Copies of the agreement will also be distributed to parents to ensure that key messages are reinforced at home.

Passwords:

- Use a strong password (strong passwords are usually eight characters or more and contain upper and lower case letters, characters and numbers).
- Passwords should not be written down.
- Passwords should not be shared with other children or staff.

Mobile technology (laptops, iPads, netbooks, etc):

- Staff laptops should not be left in cars.
- Staff should only use the laptop that is allocated to them.
- Mobile Technology assigned to a member of staff as part of their role and responsibility must have a passcode or device lock so unauthorised people cannot access the content.
- When they are not using a device staff should ensure that it is locked to prevent unauthorised access.
- No personal devices belonging to staff or children are to be used during lessons at school. Staff phones may be kept in personal belongings but are not to be taken out during lessons or in the proximity to children. If pupils bring in mobile phones (for the purpose of safety if they walk to and from school alone), they should be kept out of sight all day, and will remain the responsibility of the child in case of loss or damage. Any children not following these rules will be dealt with using the school's behaviour policy.

Data storage

- Staff are expected to save all data relating to their work to the T-Drive or work OneDrive account. Under no circumstances must it be saved to a personal account or pen drive. In addition to this data must not be uploaded to pen drives or external hard drives.

- Staff laptops should be encrypted if any data or passwords are stored on them.
- Only take offsite information you are authorised to and only when it is necessary and required in order to fulfil your role. If you are unsure speak to a member of the Senior Management Team.

Social Networking Sites

- Use such sites with extreme caution, being aware of the nature of what you are publishing on-line. There should be no reference to Blacko Primary School on personal social network account. Do not publish any information online that you would not want your employer to see.
- Any information relating to school must be published via the schools individual account.
- Under no circumstances should school pupils or parents, past or present, be added as friends, unless known to you as a friend or relative prior to your appointment.
- Your role in school requires a high degree of professionalism and confidentiality.
- Any communications or content you publish that causes damage to the School, MAT, any of its employees or any third party's reputation may amount to misconduct or gross misconduct to which the School and MAT Dismissal and Disciplinary Policies apply.
- Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct.
- The Local Authority expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

Any communications made in a professional capacity through social media must not either knowingly or recklessly:

- Place a child or young person at risk of harm;
- Bring the School into disrepute;
- Breach confidentiality;
- Breach copyright;
- Breach data protection legislation (GDPR); or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:

- Making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
- Using social media to bully another individual; or
- Posting images that are discriminatory or offensive or links to such content.

Members of staff who breach the acceptable use policy (AUP) may face disciplinary action. A misuse or breach of this policy could also result in criminal or civil actions being brought against you.

Providing a comprehensive E-safety education to pupils and parents

- All staff working with children must share a collective responsibility to provide e- safety education to pupils and to promote e-safety in their own actions.
- Formally, an e-safety education is provided based on the objectives contained in the National Curriculum.
- Informally, a talking culture is encouraged in classrooms which allows e-safety issues to be addressed as and when they arise.
- The ICT Coordinator will lead an assembly twice a year, including on Safer Internet Day, highlighting relevant e-safety issues and promoting safe use of technologies.
- All classes will follow a themed days across the year, during which their class teacher will lead lessons and activities designed to educate children in keeping safe when using the internet and other new technologies.
- Staff will ensure children know to report abuse using the CEOP button widely available on many websites or to speak to any member of staff, who will escalate the concern to the ICT Coordinator with responsibility for E-safety.
- When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's ICT guidelines. (See Appendix)
- Children will have the opportunity to educate parents through assemblies and classroom activities on an annual basis.

Terminology

Sexting:

Sexting is when someone sends or receives a sexually explicit text, image or video. This includes sending 'nude pics', 'rude pics' or 'nude selfies'. Pressuring someone into sending a nude picture can happen in any relationship and to anyone, whatever their age, gender or sexual preference.

However, once the image is taken and sent, the sender has lost control of the image and these images could end up anywhere. By having in their possession, or distributing, indecent images of a person under 18 on to someone else, young people are not even aware that they could be breaking the law as stated as these are offences under the Sexual Offences Act 2003. For more information regarding sexting please see our Safeguarding and Child Protection policy.

Peer on Peer Abuse:

At Blacko Primary School we continue to ensure that any form of abuse or harmful behaviour is dealt with immediately and consistently to reduce the extent of harm to the young person, with full consideration to impact on that individual child's emotional and mental health and well-being. For more information regarding Peer on Peer Abuse please see our Safeguarding and Child Protection policy.

Maintaining the Security of the School IT Network

Outside agenises, Head Teacher and the Computing coordinator maintains the security of the school network and is responsible for ensuring that virus protection is up to date at all times. However it is also the responsibility of the IT users to uphold the security and integrity of the network.

Complaints procedure

As with other areas of school, if a member of staff, a child or a parent / carer has a complaint or concern relating to e-safety then they will be considered and prompt action will be taken. Complaints should be addressed to the e-safety Coordinator in the first instance, who will undertake an immediate investigation and liaise with the leadership team and those members directly involved. Incidents of e-safety concern will be recorded using a Record of Concern proforma and reported to the school's designated safeguarding officer, Mr Mark Harrison, in accordance with school's child protection policy. Complaints of Cyberbullying are dealt with in accordance with our Anti-Bullying Policy.

Monitoring

The Head Teacher or other authorised members of staff may inspect or monitor any ICT equipment owned or leased by the school at any time without prior notice.

Monitoring includes: intercept, access, inspect, record and disclose telephone calls, e- mails, instant messaging, internet/intranet use and any other electronic communications (data, e-mail, texts or image) involving employees without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures, to ensure the effective operation of School ICT, for quality control or training purposes, to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

All concerns regarding children and any disclosures made will be recorded on school's agreed proforma. This will be done as soon as possible and within 24 hours of the disclosure and then given to the DSL or if not available will be given to the backup DSL's. . It is recognised that in some cases the initial reporting to the DSL will be verbal to enable a timely response to the concerns raised. For more information regarding the Safeguarding and Child Protection recording and monitoring processes please see our Safeguarding and Child Protection policy.

Breaches of Policy

Any policy breaches are grounds for disciplinary action in accordance with the School Disciplinary Policy. Policy breaches may also lead to criminal or civil proceedings.

Incident Report

All security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's Designated Safeguarding Person either **Mrs Kate Richards** or one of the e-Safety coordinators **Mr Sean Jackson** or **Mrs Kerrie Davis.**

Pupil Mobile Phone Expectations

Blacko Primary School
Mobile Phone use policy for pupils

We recognise that mobile phones are part of everyday life for many children and that they can play an important role in helping pupils to feel safe and secure. However, we also recognise that they can prove a distraction in school and can provide a means of bullying or intimidating others. Therefore: -

- Pupils are not permitted to have mobile phones at school without requesting permission from the head teacher or their class teacher (e-mail, telephone call or letter).

- If agreed, the phone must be switched off before coming into the school grounds and handed to their class teacher at registration. The phone will then be sent kept in a secure place in the classroom or admin office.

- Pupils are responsible for collecting their phone at home time (the phone is left at the owner's own risk).

Pupil:

- I will switch my mobile phone off before entering the school grounds.

- I will hand my mobile phone to my class teacher at registration.

- I will be responsible for collecting my mobile phone at the end of the school day.

- I will not switch my mobile phone on until I have left the school grounds.

- If I do not follow these rules, I understand that the head teacher will confiscate my phone.

- If my phone is confiscated, I understand that a parent must come into school the following day to collect it from the school office.

- If my parent is unable to collect my phone from the office, I can collect the phone myself on Friday, after school.

- Under no circumstances must I communicate with others via a smart watch. My phone will be switched of so this isn't possible.

Pupil signature: ……

Parent:

- If I wish my child to bring a mobile phone into school, I will ask permission from the head teacher by signing this agreement.

- I understand that the school does not accept responsibility for mobile phones lost on the school premises.

- I understand that if my child uses their phone inappropriately in school, I will be asked to collect it for them from the school office the following day. If I am unable to do so, the phone will be kept in the school office until after school on Friday, when my child may collect it.

Parent signature: ……

If you give your children permission to have a mobile phone while at school, please tick the box below. If this form it returned without a tick in the below box, we will assume that your child does not have permission to have a mobile phone within their possession.

[ ] I **do** give my children (Name):…….. permission to take their mobile phone to school.

Thank you,

Mr. Sean Jackson.

Blacko Primary School

ICT Acceptable use policy for pupils for use at home (H) and at school (S).

The school has installed computers and Internet access to help our learning. These rules will keep us safe and help us to be fair to others.

- I will only use ICT in school for school purposes. (S)
- I will ask permission from a member of staff before using the Internet and will only be online when an adult is in the room. (S)
- I will only use my login and password and never share these with others. (S) (H)
- I will only open and delete my own files. (S)
- The messages I send will be polite and sensible and contain no indecent or harmful images. (S) (H)
- I will not use external hard drives / pen drives to transfer documents in school.
- I will never give out my own or other people's name, address or phone number online. (S) (H)
- I will not share images of other pupils/parents/staff on social media/the internet. (S) (H)
- I will never upload any images of school activities to any social networking site. (S) (H)
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. (S) (H)
- If I see anything I am unhappy with on the computers, I will turn the screen off and tell my teacher or an appropriate adult straight away. (S) (H)
- I understand that the school can check my computer use and that my parents/carers can be contacted if school staff are concerned about my e- safety. (S)
- I will not friend members of staff on Facebook on any other social media sites (H)
- I will not friend parents and / or pupils who attend Blacko primary School, I understand that that this will be monitored through the use of the Impero software (S)

Pupil Signed: _____ Date:_____

Parent Signed: _____ Date:_____

Blacko Primary School

ICT Acceptable use policy for staff, governors and visitors

These rules are designed to protect staff and visitors from e-safety incidents and promote a safe e-learning environment for pupils.

- I will only use the school's Internet, email, computers, laptops and mobile technologies for professional purposes as required by my role in school.
- I will not disclose my password to anybody else.
- When accessing school emails or any other sensitive information relating to Blacko Primary School, employees will ensure that it is conducted on a device that had the appropriate security measures (anti- virus, firewall, encryption) and that locked out when away from the device and logged off each of the sites after use.
- I will ensure that any online communications with staff, parents and pupils are compatible with my professional role.
- I will not use external hard drives / pen drives to transfer documents in school.
- I will not give out my own personal details to pupils or parents.
- I will send school business emails using my school email address, if I have been provided with one, not my personal email address.
- I will ensure any data that I store is stored on my OneDrive account.
- I will not browse, download, upload or distribute any material which could be considered offensive, illegal or discriminatory.
- Images of pupils will only be taken and used for professional purposes in line with school policy with consent of the parent or carer. Images will not be distributed outside of school without the permission of the parent/carer and Head Teacher.
- If it is necessary to bring my own personal devices into school, these will only be used during non-contact time without pupils.
- I will report any e-safety concerns to the designated safeguarding officer and deputy designated safeguarding officer immediately using CPOMs.
- I will report any known sexting incidents to the DSL and / or Deputy DSL on the Performa's provided.

- I will monitor and report any known peer on peer abuse incidents to the DSL and / or Deputy DSL on the Performa's provided.
- Mobile phones will be out of sight and switched to silent. Staff phones may be kept in personal belongings but are not to be taken out during lessons or in the proximity to children.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support the school's e-safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

I understand the procedures and agree to follow them with immediate effect.

Print Name: _____

Signed: _____ Date: _____