HAWKSMOOR
Learning Trust
Building Excellence

BRACKEN LEAS
PRIMARY SCHOOL

Online Safety Policy for Bracken Leas Primary School

September 2020 to 2021

Date adopted by Trustees:	Signed The Hawksmoor Learning Trust	Date November 2020
Adoption by Local Governing Body School:	Bracken Leas	January 2020

The Online Safety Leads for Bracken Leas Primary School are:

Clare Shannon (Computing Lead)
Christine Allum (Safeguarding Governor)

The Designated Safeguarding Leads are:

Paula Harwood (Head Teacher)
Daniel Alder (Deputy Head Teacher)
CarolineLewis (Lead DSL / Assistant Head Teacher)
Lauren Amery (EYFS Teacher)
Andrea Kent (SENCo)

1. What is an online safety policy?

Our online safety policy sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of all technologies to safeguard adults, children and young people within our school. The policy recognises the ever-changing nature of emerging technologies within the curriculum and media and highlights the need for regular review to incorporate development within ICT. At present the internet technologies used extensively by young people in both home and school environments include:

- School subscription websites
- Social networking
- Gaming/forums on PS4/Xbox live etc.
- Music downloading
- Mobile phones with wireless connectivity
- Email and Instant Messaging
- Class Dojo
- Office 365
- Skype / Zoom
- Video Broadcasting
- Apple/Windows apps

This policy provides support and guidance to parents and the wider community (where appropriate) for the safe and responsible use of these technologies beyond the school or educational setting. It also explains the procedures for online safety and use of technologies by children or young people.

2. Why have an online safety policy?

The use of the internet as a tool to develop learning and understanding has become an integral part of school and home life. There are always going to be risks to using any form of communication which lies within the public domain therefore it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst children access these technologies.

The risks include:

- Spam and other inappropriate e-mail.
- Online grooming.

- Illegal activities of downloading or copying any copyright materials and file-sharing via the internet or any mobile device.
- Viruses.
- Cyberbullying.
- Sexting - the sending of indecent personal images, videos or text via mobile phones for private viewing.
- Online content which is abusive or pornographic.
- Radicalisation and other religious movements.
- Social and emotional effects of an increased use of technology.
- Groups that promote self-harm and/or eating disorders.

There is also a responsibility to educate parents about the risks and how this is managed inside of school, along with what they can do at home to help safeguard their child.

As part of the 'Every Child Matters' agenda set out by the government, the Education Act 2004 and the Children's Act, it is the duty of schools to ensure that children and young people are protected from potential harm both within and beyond the school environment. Every effort will be made to safeguard against all risks, however it is likely that we will never be able to completely eliminate them. Any incidents that do arise will be dealt with quickly and according to policy to ensure children and young people continue to be protected.

3. Aims

- To emphasise the need to educate children and young people about the pros and cons of using new technologies both within and outside school or other educational settings.
- To provide safeguards and rules for online safety to guide all users in their online experiences.
- To ensure adults, including parents, are clear about procedures for misuse of any technologies both within and beyond the school or educational setting.
- To develop links with parents and the wider community ensuring input into policies and procedures.

4. Responsibilities of Pupils

Children are responsible for:

- Signing agreement to, and abiding by, the online safety rules set.
- Using the internet and technologies in a safe and responsible manner within school and at home.
- Informing staff of any inappropriate materials or contact from strangers immediately, without reprimand (age and activity dependent)
- Actively participating in the development and annual review of the online safety rules.

5. Appropriate and inappropriate use by pupils

The online safety rules for pupils provide children and young people with clear guidelines on appropriate use of the internet and technologies within school and are linked to school disciplinary procedures. Pupils sign acceptance of the rules when they join the school and they are displayed throughout the school as a reminder.
To encourage parental support of these, a copy is sent home with the related school sanctions for misuse. This is also displayed on the school website and is clearly seen around school.
Parents are asked to sign the online safety rules with their child again in Year 3 to show their support of the online safeguarding rules in place (see Appendix 3 for template).

In the event of inappropriate use

If a child or young person is found to have deliberately misused online technologies or equipment whilst at school, one or all of~~one or all of the~~ the following sanctions could~~will~~ apply:

- ~~Failure to abide by online safety rules and deliberate misuse of the internet/technologies will result in contact made with parents explaining the reason for S~~suspending the child or young person's use of the internet/online technologies ~~use~~ for a particular lesson or activity and contact made with the parents explaining the reason for the suspension.~~.~~
- Further misuse of the rules may result in withdrawal of a pupil's internet privileges for a period of time and a letter sent home to parents.
- A letter ~~may be~~ is sent to parents outlining the breach in Child Protection Policy where a child or young person is deemed to have misused technology against another child or adult.

In the event of accidental access to inappropriate materials, pupils are expected to notify an adult immediately and attempt to minimise or close the content until an adult can take action.

In the event of a member of staff being aware of a child having inappropriate social media accounts, contact will be made with parents informing them of this and reminding them of the legal age requirement. Appropriate online safety incident procedures are then followed.

6. The Curriculum

6.1 Internet use

It is the responsibility of schools to teach their pupils how to use the internet safely and responsibly. The following concepts, skills and competencies will be developed through both the Health and Wellbeing and ICT curricula:

- internet literacy
- making good judgements about websites and emails received
- knowledge of risks such as viruses and opening mail from a stranger
- knowledge of copyright and plagiarism issues
- file-sharing and downloading illegal content
- uploading personal information – what is and is not safe
- where to go for advice and how to report abuse.

It is also the schools' responsibility to plan in opportunities for children to make informed judgements and manage risks themselves rather than relying on filtering systems.

Online personal safety is taken extremely seriously within our school community and our pupils are encouraged to refrain from sharing personal information in any form of electronic communications. Personal informal includes:

- full name
- address
- telephone number
- email address
- images that contain identifying features (school uniform etc.)

6.2 Pupils with additional learning needs

The school strives to provide access to a broad and balanced curriculum for all learners and recognises the importance of tailoring activities to suit the educational needs of each pupil. Where a pupil has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of online safety awareness sessions and internet access.

6.3 Pupil email use

The school has set up individual class email addresses for pupils to use as a class, as part of their entitlement to understand different ways of communicating and using ICT to share and present information. Pupils will use this email account for any form of school related communications and teaching staff will monitor their class use of these systems. Teachers may want to pass this on to parents as a form of communication. Children's emails are generated using an agreed format followed by the school. If there are any cases where a child (for safeguarding purposes) cannot use this set up, alternative options should be offered, such as the email being turned off or directed to the class teacher. Children should be encouraged to update their password every three months to include a mixture of upper and lower case letters along with numbers. They should not use this email to sign up for any other sites. Pupils are only able to email internally within Bracken Leas Primary and not to any external email addresses.

6.4 Mobile technologies

Everyday technologies, including smartphones and tablets, are increasingly being used by both adults and children within the school environment. For this reason, appropriate safeguards must be in place to protect young people and staff against the following associated risks:

- Inappropriate or bullying text messages
- Images or video taken of adults or peers without permission
- Videoing violent, unpleasant or abusive acts towards a peer or adult which may be distributed
- Sexting- the sending of suggestive or sexually explicit personal images via mobile phones
- Wireless internet access which can bypass school filtering and allow access to inappropriate or potentially harmful material or communications.

Teachers are permitted to capture photos using their mobile devices as agreed by ~~*XXXX on DD/MM/YY*~~THLT Staff Use Policy Sept 2020, but must delete the images once saved/uploaded to relevant platforms.

6.5 Mobile phones

Pupils are advised not to bring mobile phones to school. If there is no alternative, they are the responsibility of that pupil and they must remain switched off whilst on school premises, and handed in to the class teacher. If there is reason to suspect that a pupil's mobile device contains inappropriate, illegal or harmful content, whilst on school grounds, it will be confiscated by staff and may be searched. The Online Safety Incident flowchart and child protection procedures will be followed if such content is discovered.

6.6 Laptops/Tablets

Teaching staff are provided with school laptops/tablets to allow for school related work to be completed off site. Personal use of school issued computing facilities is permitted providing it is kept to a minimum and does not interfere with the employee's work. Sensitive data and school authorised images of pupils should not be stored on school laptops without appropriate encryption software in place. In the event that a laptop/tablet is stolen or lost there is potential for this content to be viewed by unauthorised individuals.

6.7 Video and photographs

Images or videos featuring pupils will only feature on the school website, school Twitter feed or in press coverage, if permission has been granted by parents in advance. Wherever possible group shots of children will be taken, as opposed to images of an individual, and first names only will be displayed.

Photographs should not show children in compromising positions or in inappropriate clothing (e.g. leotards/swimming costumes). Personal devices may be used to take images of pupils, but pictures should be removed from cameras and utilised appropriately within 24 hours of being taken. This is to ensure that images of pupils cannot be viewed by unauthorised individuals in the event of loss or theft.

6.8 Video-conferencing and webcams

To safeguard staff and young users, publicly accessible webcams are not to be used in school. As with video and photographs, permission will be sought from parents before a child engages in video conferencing with individuals or groups outside of the school setting (e.g. communicating with a school overseas). All video conferencing will be supervised by staff and a record of dates, times and participants held in school for audit trail purposes.

7. Web Technologies

7.1 Managing social networking and other web technologies

Social networking is now the communication form of choice for many adults and young people worldwide and, as a result, safeguards must be in place to ensure that staff and pupils are aware of the risks associated with this form of technology. To address this issue, a series of preventative measures are in place.

- Pupils are discouraged from providing personal details or identifiable information on profiles (e.g. mobile number, address, school name, clubs attended, email address or full names of friends). Children are asked to include images of avatars for their display icon instead of real pictures.
- Pupils are made aware of the risks of posting images online and how publicly accessible their content is. Background images in photographs which may reveal personal details are also addressed (e.g. house number, street name, school uniform).
- Social networking security settings are explained and recommendations made for privacy settings to be activated to 'Friends only' for all applications to restrict unsolicited access. The importance of passwords and blocking of unwanted communications is also highlighted.
- Both online and school systems for reporting abuse or unpleasant content, i.e. cyberbullying, are reinforced through the website www.thinkuknow.co.uk.

7.2 Filtering

The Exa networks filtering system provides a filtered internet service to Bracken Leas, which prevents access to illegal and inappropriate sites. The school has access to a local control list which allows websites to be added to a 'restricted list'.

Changes to the filtering will be agreed by the head teacher and online safety lead; these changes will be implemented by the school's IT support company.

In addition to the above, the following safeguards are also in place:

- Annually, the head teacher will sign a disclaimer stating agreement to the filtering levels being maintained as part of the connectivity to broadband by Exa Networks.
- Reports can be produced from the school's filtering system, SurfProtect, which show what websites and search queries have been blocked.
- Anti-virus and anti-spyware software is used on all network and stand-alone PCs or laptops and is updated on a regular basis.
- A firewall ensures information about children and young people and the school cannot be accessed by unauthorised users.
- Links to online safety websites are provided on the school website.

- Encryption codes on wireless systems prevent hacking.

7.3 Tools for bypassing filtering

Web proxies are the most popular and successful method for pupils to bypass internet filters in order to access unauthorised online content on the school network. A web proxy is capable of hiding the IP address of the user and opening unrestricted and, in cases, unidentifiable channels through which blocked material can be viewed e.g. Social networking sites, gaming websites or adult content.
To manage this safeguarding concern, pupils and staff are forbidden to use any technology designed to circumvent, avoid or bypass school security controls (including internet filters, antivirus solutions or firewalls). Violation of this rule by either staff or pupils will result in school sanctions being applied.

8. Parents

8.1 Roles

Each pupil will receive a copy of the online safety rules on an annual basis or first-time entry to the school. Pupils and their parents are asked to read and sign acceptance of the pupil online safety rules to be returned to, and stored by, the school. Parents are also encouraged to attend online safety workshops to highlight the issues surrounding young people today and technology.

8.2 Support

As part of the school's approach to developing online safety awareness with children and young people, every effort is made to offer parents the opportunity to find out more about how they can support their child to stay safe online within and beyond the school environment. Online safety parent information sessions are held to raise awareness of key internet safety issues and highlight safeguards currently in place at school (e.g. filtering and training in place to minimise online risk.) Free to order resources from Childnet (http://www.childnet-int.org/kia/parents/) and the Thinkuknow website (http://www.thinkuknow.co.uk/teachers/resources/) can be used to support this. Wherever possible, the school will endeavour to provide internet access for parents without this resource at home to ensure that appropriate advice and information on this topic can be viewed.

9. Links to other policies and procedures

9.1 Behaviour and Anti-Bullying

The Online Safety Policy is referenced throughout a number of other policies in place throughout the school, including those for behaviour, health and wellbeing, and child protection.
Cyberbullying features within the school's anti-bullying policy due to the growing number of incidents recorded. Cyberbullying will not be tolerated in or outside of school and clear procedures for dealing with cyberbullying incidents can be found within the anti-bullying policy.

9.2 Managing Allegations and concerns of abuse made against people who work with children.

The Designated Officer (formerly LADO) will be contacted in the event that an allegation of misuse or misconduct is made by a child or other adult about a member of staff. Allegations made against staff members must be reported to the head teacher immediately. In the event of an allegation being made against the head teacher, the chair of governors must be notified immediately.

9.3 Health and Wellbeing

The teaching and learning of online safety is embedded within the Health and Wellbeing curriculum to ensure that the key safety messages about engaging with people are the same whether children and young people are on or offline. Before any use of technology, online safety rules will be shared with the children. Online safety advice and information will be shared with parents via Twitter, Class Dojo and Arbor. There will be an annual online safety week in school

where all children will have lessons focused on the safe use of the internet and technologies. During the annual anti-bullying week, online safety will be discussed.

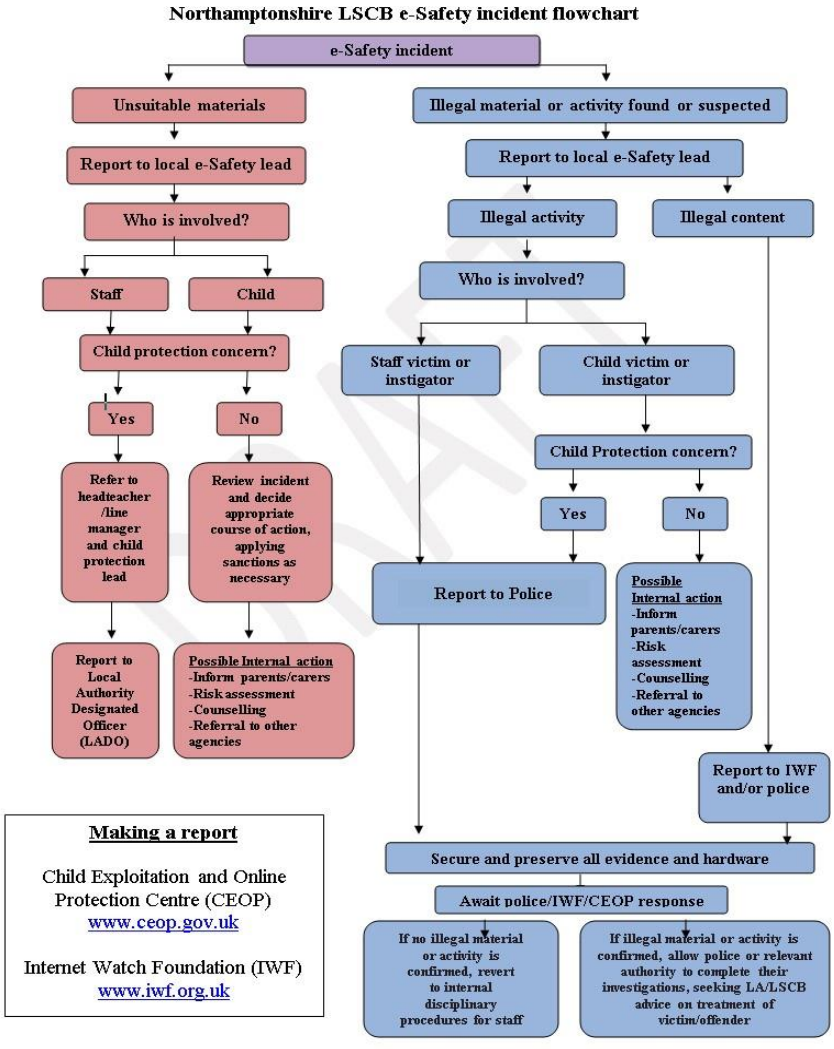
10.4 School website and Twitter

Parental consent is required for the uploading of any images onto the school website or Twitter. Consideration is given to which information is relevant to share with the general public and secure areas will be used for information pertaining to specific audiences. The online safety policy will also be published on this platform alongside recommended websites and support guidance.

9.5 Staff ICT Online safety Policy

The Trust has a staff policy which sets out the online safety of online resources, along with devices to ensure the safety of pupils and adults, both in and out of school.

Appendix 1 – Online Safety Incident Flowchart



There are three instances when you must report directly to the police.

- Indecent images of children found (i.e. under 18 years of a sexual nature).
- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child.

CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if an indecent image is found. The police will advise on how to deal with the machine

if they are unable to send out a forensics team immediately. If in doubt, do not turn off the machine. The Internet Watch Foundation www.iwf.org.uk offers further support and advice in dealing with offensive images online. It is important to remember that any offensive images received should never be forwarded, even if it is to report them as illegal, as this constitutes illegal activity and you will be liable to prosecution and investigation by the police.

Appendix 2 - Parent and Child Online safety Agreement

Dear Parents,

As part of an enriched curriculum, your child will be accessing the internet, school email and virtual learning environment via a filtered service provided by the EXA Network. In order to support the school in educating pupils about safe use of the internet, we are asking parents and children to read and sign acceptance of the attached online safety rules. Completed forms should be returned to the school as soon as possible.

The rules provide an opportunity for further discussions with your child about safe and appropriate use of the internet and other online tools (e.g. smartphones), both within and beyond school (e.g. at a friend's house or at home). Sanctions in place for misuse of technologies and subsequent breach of the rules are detailed in the full Online Safety Policy which parents are welcome to view on the school website.

Should you wish to discuss the matter further please contact the school.

With best wishes

Paula Harwood
Head Teacher

Online safety Rules Return Slip

Child Agreement:

Name: _____Class:_____

- I understand the rules for using the internet and email safely and responsibly.
- I know that the adults working with me at school will help me to stay safe and check that I am using the computers to help me with my work.

Child Signature: _____ Date: _____

Parental Agreement:

- I have read and discussed the rules with my child and confirm that he/she has understood what the rules mean.
- I understand that the school will use appropriate filtering and ensure appropriate supervision when using the internet, email and other online tools.
- I understand that filtering can never be completely fool proof and occasionally inappropriate materials may be accessed. I accept that the school will endeavour to deal with any incident that may arise swiftly and according to policy.
- I understand that my child's safe use of the internet and online technologies outside of school is my responsibility.

Parent/Carer Signature: _____ Date: _____

Key Stage 1 Online Rules

These are our rules for using the internet safely and responsibly.

- We learn how to use the internet safely.
- We can send and open messages with an adult.
- We can write polite and friendly emails or messages to people that we know.
- We only tell people our first name.
- We learn to keep our password a secret.
- We know who to ask for help.
- If we see something we do not like we know what to do.
- We know that it is important to follow the rules.
- We are able to look after each other by using the internet safely.
- We can go to www.thinkuknow.co.uk for help.

Key Stage 2 Online Rules

These are our rules for using the internet safely and responsibly.

- We use the internet to help us learn and we know how to use it safely and responsibly.
- We send emails and messages that are polite and friendly.
- We will only email, chat or go on webcam with people that we know in real life, with permission from our teachers or parents.
- We make sure that an adult always knows when we are online.
- We never give out passwords or personal information (like our full name, school or address)
- We never post photographs without permission and never include names with photographs.
- We know who to ask if we need help.
- If we see anything on the internet or on email that is scary or makes us feel uncomfortable, we know what to do.
- We never open emails or links from people we don't know.
- We know that the rules are there to keep us safe and must not be broken.
- We are able to keep ourselves and each other safe by using the internet in a responsible way.
- We can go to www.thinuknow.co.uk for help

Further Information and Guidance

- www.parentscentre.gov.uk (for parents)
- www.ceop.co.uk (for parents and adults)
- www.iwf.org.uk (for reporting of illegal images or content)
- www.thinkuknow.co.uk resources for children, teenagers, parents and professionals
- www.netsmartzkids.org (5 – 17)
- www.kidsmart.org.uk (all under 11)
- www.phonebrain.org.uk (for Yr 5 – 8)
- www.bbc.co.uk/cbbc/help/web/staysafe (for Yr 3/4)
- www.hectorsworld.com (for FS, Yr 1 and 2 and is part of the thinkuknow website above)
- www.education.gov.uk (for adults and professionals
- www.digizen.org.uk (for materials from DCSF around the issue of cyberbullying)

Staff Procedures Following Misuse by Pupils

The head teacher will ensure that these procedures are followed, in the event of any misuse of the internet, by a child or young person:

A. An inappropriate website is accessed inadvertently:

- Reassure the child that they are not to blame and praise for being safe and responsible by telling an adult.
- Report website to the online safety lead if this is deemed necessary who will add site to the banned list immediately.

B. An inappropriate website is accessed deliberately:

- Refer the child to the Online safety Rules that were agreed.
- Reinforce the knowledge that it is illegal to access certain images and police can be informed.
- Decide on appropriate sanction and notify parent.
- Report on school behaviour log and if necessary, My Concern.

C. An adult or child has communicated with a child or used ICT equipment inappropriately:

- Ensure the child is reassured and remove them from the situation immediately.
- Report to the head teacher and designated safeguarding lead immediately.
- Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
- If illegal or inappropriate misuse then the head teacher must follow the Allegation Procedures.
- Contact CEOP (police) as necessary.

D. Threatening or malicious comments are posted to the school website or learning platform about a child in school:

- Preserve any evidence and inform the head teacher immediately.
- Report on school behaviour log and if necessary, My Concern.
- Inform the online safety lead so that new risks can be identified.
- Contact the police or CEOP as necessary.

E. Threatening or malicious comments are posted on external websites about an adult in the school or setting:

- Preserve any evidence and inform the head teacher immediately.
- Report on school behaviour log and if necessary, My Concern.

N.B. There are three incidences when you must report directly to the police.

- Indecent images of children found.
- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child.

CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if an indecent image is found. They will advise on how to deal with the machine, if they are unable to send out a forensics team immediately. If in doubt, do not power down the machine. Grabbing a screenshot is not a technical offence of distribution, but of 'making' an image. www.iwf.org.uk will provide further support and advice in dealing with offensive images on-line. It is important to remember that any offensive images that may be received should never be forwarded to anyone else, even if it is to report them as illegal as this constitutes illegal activity and you will be liable to prosecution and investigation by the police.