Horton Park Primary

We Learn to Succeed

E-Safety Policy

Author: Catherine MacGilchrist

Date: February 2019

Checked by:

Date of Governing Body Approval:

Review date:

Relevant School Aims:

1. All in our school community are valued and respected and continually learning.
2. All broaden their horizons and explore their opportunities so they can make positive life choices.

Background

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

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of 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 within and outside the school. Some of the dangers they may face include:

• Access to illegal, harmful or inappropriate images or other content
• Unauthorised access to / loss of / sharing of personal information
• The risk of being subject to grooming by those with whom they make contact on the internet.
• The sharing / distribution of personal images without an individual's consent or knowledge
• Inappropriate communication / contact with others, including strangers
• Cyber-bullying
• Access to unsuitable video / internet games
• An inability to evaluate the quality, accuracy and relevance of information on the internet
• Plagiarism and copyright infringement
• Illegal downloading of music or video files
• The potential for excessive use which may impact on the social and emotional development and learning of the young person

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The E Safeguarding Committee

Salma Rahman – Head - Designated Safeguarding Lead, CEOP Think You Know Trained
Saima Bahadur – Deputy Head – Designated Safeguarding Lead, CEOP Think You Know Trained
Catherine MacGilchrist – E-safety Leader (CEOP Think U Know Trained)
Saira Yousuf – Computer Leader
Vicki Adams - Governor
Naveed Mushtaq – Community Manager

Development and Review of this policy

This e-safety policy was approved by the Governors Staffing and curriculum committee
The implementation of this e-safety policy will be monitored by the: **The E Safeguarding committee**
Monitoring will take place at regular intervals: **Annually**
The E-Safeguarding Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.
The next anticipated review date will be: **December 2020**
Should serious e-safety incidents take place, the following external persons / agencies should be informed:
Children's services, Safeguarding Officer Bradford Local Authority
Bradford Learning Network can be contacted regarding displayed content on web sites at 385844

Monitoring the impact of the policy

The school will monitor the impact of the policy using

- Logs of reported incidents in the e safeguarding tab of CPOMS
- Internal monitoring data for network activity
- Computing Monitoring week – Computing Leader

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors Staffing and Curriculum Committee receiving regular information about e-safety incidents and monitoring reports.

The role of this governor will include:
• Regular meetings will include Safeguarding where e safety issues will be discussed
• Receiving regular reports from meetings of the e safety committee

Headteacher and Senior Leaders:
• The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to Catherine MacGilchrist
• The Headteacher is responsible for ensuring that the E-Safety team and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
• The Headteacher and E Safeguarding leader are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

Prevent
The school ensures that suitable filtering systems are in place to prevent children accessing terrorist and extremist material. The school uses Smothwall to filter appropriate information. All staff are prevent trained yearly.

E-Safeguarding Leader
• Takes day to day responsibility for e-safeguarding issues and has a leading role in establishing and reviewing the school e-safeguarding policy
• Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
• Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
• Attends the relevant Governors meetings where e safeguarding issues are discussed

Network Manager / Technical staff:
The school technician team ensures:
• That the school's IT infrastructure is secure and is not open to misuse or malicious attack
• That he keeps up to date with e-safety technical information and updates the E Safety leader or Computing Leader as relevant
• That monitoring software and anti-virus software is implemented and updated

Teaching and Support Staff are responsible for ensuring that:
• They have an up to date awareness of e-safety matters and of the current school e-safety policy
• They have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
• They report any suspected misuse or problem to the E-Safety leader for investigation
• Digital communications with students / pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems
• E-safety issues are embedded in all aspects of the curriculum and other school activities. E Safety lessons are taught through the Innovation Centres Computing Scheme of Work.

Named person for child protection
Duncan Jacques (CEO), Salma Rahman (Head of School), Saima Bahadur (Deputy Headteacher),), Shahmyla Gulshan (SENDCO), Naveed Mushtaq (Community Manager) are the named people for child protection.
They are trained in matters related to e-safety and to be aware of the potential for serious child protection issues to 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 (see cyber bullying section)

Children
• Are responsible for using the school IT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems. The AUP for children is signed annually in line with Safer Internet Day.

Parents / Carers

The school will take every opportunity to help carers / parents to understand issues related to e safety. We will assist parents to understand key issues in the following ways:
• A parent's e safety presentation
• Regular newsletters offer parents advice on the use of the internet and social media at home
• Parents are asked to discuss the pupil Acceptable use policy with their children
• Parents are asked to review the letter regarding digital and video images and opt out of having images taken and or published on the school web site or blog if they wish to do so

Community Users
Community Users/ visitors and volunteers will inform the Heateacher or Deputy Head of any web sites they wish to access. No person can log on to the internet without a user account or the Internet password. A community user account with minimal privileges will be given after discussion of the sites they wish to access.

Education

Pupils
The education of pupils in e-safety is an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.
E-Safety education will be provided in the following ways:
• E-safety is taught every term in every year group following the Innovation Centre SOW. All objectives link directly with the National Curriculum End of Key Stage Expectations.
• E-safety is delivered as part of PHSE within the Spiral Curriculum.
• Key e-safety messages are reinforced as part of a planned programme of assemblies. They take place twice a year
• Pupils are taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information. Validation of information is covered in the Information Literacy strand of the Innovation Centre Computing scheme of work
• The SMART rules are displayed on the desktops of laptops and workstations. They are also displayed within all classrooms.
• Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information. Evaluation and cross referencing of sources is covered in the Information Literacy strand of the Innovation Computing scheme of work which the school follows
• Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. Copyright free audio and image sources are detailed in the Media strands of the Innovation Computing scheme of work which the school follows.

Staff Training
It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:
• A Staff meeting covering e safety will take place annually. This will be delivered by a member from the Curriculum Innovation Team, E-safety Police Officer or a member of the E Safeguarding Committee
• An audit of the e-safety training needs of all staff will be carried out regularly
• All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
Three members of staff Salma Rahman, Saima Bahadur and Catherine MacGilchrist have been trained as Think U Know Trainers. They are qualified to deliver CEOP Think U Know sessions to children and will receive regular updates on practice through the CEOP web site.
Governor Training
Governors take part in e-safety training / awareness sessions. E Safety training is planned annually and delivered by staff from the E-safety Committee.

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 also generates reports on user activity. If staff require access to a site which is blocked, they must first email SLT for approval. Following this, SLT or the Computing Leaders will ring eICT on 01274439300. eICT keep a log of all the changes requested and all user activity when using PCs and laptops.

Use of digital and video images - Photographic, Video

• When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images online

• Staff are allowed to take digital / video images to support educational aims. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes

- Teaching staff are responsible for storing photographs and images safely and securely. Staff will also ensure that images are deleted annually.

• Photographs of children published on the website, social media (Twitter) or blog must not contain full names

• Pupils' full names will not be used anywhere on a website, social media (twitter) or blog

• Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website

Personal Data Protection

Staff must ensure that they:

• At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse

• For information about data stored in the cloud see the data policy.

• 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 such as memory sticks and encrypted machines

The school Privacy notice to parents is available to view through the school website (see the Data Protection Policy.)

Parents can request all information through the freedom of information requests (see the data policy)

Passwords

All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security to SLT.

Passwords for new users, and replacement passwords for existing users can be allocated by Technical support service. All old usernames and accounts are deleted annually.

Network passwords are stored in a secure location only accessible by SLT. The 'master/administrator' passwords for the school systems, used by technical staff are also available to the Head teacher and kept in a secure place.

Members of staff will be made aware of the school's password policy:

• At induction

• Through the school's e-safety policy and password security policy

• Through the Acceptable Use Agreement

Pupils / students will be made aware of the school's password policy:

• In Computing and / or e-safety lessons within the Innovation Centre SOW

• Through the Acceptable Use Agreement

All users (at KS2 and above) will be provided with a username and password by the IT Technician who will keep an up to date record of users and their usernames. Pupil passwords are set as follows:

Reception – generic password and pupils are supported whilst using devices

Year 1-2 simple passwords

KS2 – mixture of words and numbers

All children have individual logins for Iamlearning, Purple Mash, Education City and Mathletics and other curriculum websites as needed.

There will be a forced password change every 90 day for staff.

Cyberbullying

Please see our school Anti Bullying Policy.

Cyberbullying is the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature. Examples of electronic communication are social networking web sites and apps, texting, use of other mobile or tablet apps, email or online software.

Pupils and adults who feel as if they are being bullied in any way need to talk to someone who they trust. Pupils need to talk to a trusted adult.
Make sure you keep any evidence of cyberbullying by taking screen captures. Make a note about the time and date of any of these messages and any details about the sender.
Do not forward messages to other people, this means you are joining in the bullying. Stop it by reporting it to a trusted adult.
Do not reply to any bullying messages, this could make things worse and shows the bully that they are getting a response from you.
The school may report serious cyber bullying incidents to the Police.

Social Media

As part of our web site pupils will have a blog they can contribute to. All comments and posts are moderated by teachers before they are published. Pupils know that they must not share personal information on the blog or use it to communicate with people they do not know in real life.
All members of 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 will be checked regularly by the e-safety committee to ensure compliance with the Social Media, Data Protection, Digital Image and Video Policies.
A school Twitter account is managed by teaching staff. The purpose of this is to act as a one-way communication channel to keep parents/carers updated on school events. Parents should still use telephone, email or face to face contacts to communicate with school. This twitter account is protected and only approved members can view the content.
Class teachers and SLT have access to the Twitter account and they must only use the school mobile phone to post. School will only post images of children who have parental permission to do so.

Mobile device policy

Staff

Staff must not use personal mobile phones in lessons. Personal mobile phones should be placed in a locked cupboard during directed hours. Except in urgent or exceptional situations, mobile phone use is not permitted during teaching time, while on playground duty and during meetings. In accordance with the Acceptable Use Policy staff should not use personal devices for photography in school.

Pupils

School does not allow children to bring mobile phones into class. All mobile phones must be handed in to the office at the start of the day and are returned at the end of school.
As part of the digital literacy scheme of work we use 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's Mobile Devices

School has the Chromebooks, iPods and iPads and cameras. The use of these devices is covered in the pupil and staff acceptable use policies. Pupils know that they must not take pictures of other people without their permission. They are not allowed to download or install apps on any device. These devices are monitored whilst in use by children to ensure appropriate use.

E-safguarding Incident Log (CPOMS)

All E-safety incidents to be recorded on CPOMS. This will be monitored termly by the Esafety committee.

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

Technical Security

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the *school infrastructure / network* is as safe and secure as is reasonably possible and that:

- Users can only access data to which they have right of access.
- No user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- Access to personal data is securely controlled in line with the school's data protection policy.
- logs are maintained of access by users and internet access is logged
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice, as a result of the above reports

The management of technical security is the responsibility of the E Safety Leader/technical team.

The school is responsible for ensuring that the infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It also ensures that the relevant people receive guidance and training and will be effective in carrying out their responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems by the E Safety Leader working with Technical support. These will be based upon documents recommended by SWGfL
- Servers, wireless systems and cabling are securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- All users have clearly defined access rights to school technical systems as detailed in network and Smoothwall profiles. Network profiles are managed by school technical support. Smoothwall profiles are managed by eICT.
- The E-Safety Leader is responsible for ensuring that software licence logs are accurate and up to date
- Mobile device management software is used to deploy licences and restrictions to pupil ipads in school. School also uses Chromebooks which are managed through the G suite admin console.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Policy
- AUPs asks all users to report any suspicious activity or behaviour using the school network to the E-Safeguarding Leader
- An agreed policy is in place for the provision of temporary and restricted access of visiting users such as supply teachers onto the school system. This also extends to restricted internet access.
- The staff and pupil AUPs prohibit the downloading of executable files and the installation of programmes on school devices by users
- Removable media may only be used for school purposes. Encrypted USBs will be used for any personal data.
- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, Trojans etc.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- Any email containing personal data is sent using GalaxKey, an encrypted email system.

Filtering

The responsibility for the management of the school's filtering policy will be held by the E Safety Leader. They will manage the school filtering, in line with this policy and will be able to access records of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:

- Include logs from eICT, which can be checked termly by the E-Safeguarding Leader
- be regularly reported to the Online Safety Group in the form of emails from eICT

All users have a responsibility to report immediately to the E- Safeguarding Leader any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon.

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement. *Monitoring will take place as follows:*

Monitoring

The school uses eSafe, a forensic monitoring software solution. This is used on laptops and Chromebooks. This records incidents of inappropriate and illegal behaviour which may be carried out by users. This includes searches, other internet activity and also records keystrokes in programmes. Reports are sent to the Headteacher. These are logged and appropriate action is taken. These are discussed at online safety committee meetings.

IPads use an unauthenticated internet connection. This means it is harder to track individual activity. Therefore, staff will physically monitor and supervise use.

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images – The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978.**					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008.					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986.					X
	Pornography.				X	
	Promotion of any kind of discrimination.				X	
	Threatening behaviour, including promotion of physical violence or mental harm.				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.				X	
Using school systems to run a private business.					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school.					X	
Infringing copyright.					X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords).					X	
Creating or propagating computer viruses or other harmful files.					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet).					X	
On-line gaming (educational).			X			
On-line gaming (non-educational).					X	
On-line gambling.					X	
On-line shopping / commerce.				X		
File sharing.					X	

Use of social media.			X		
Use of messaging apps.				X	
Use of video broadcasting e.g. YouTube.			X		

Pupils

Incidents:	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Unauthorised use of non-educational sites during lessons	X							
Unauthorised use of mobile phone / digital camera / other mobile device	X	X			X			
Unauthorised use of social media / messaging apps / personal email	X				X			
Unauthorised downloading or uploading of files	X	X		X	X			
Allowing others to access school network by sharing username and passwords	X			X				
Attempting to access or accessing the school network, using another student's / pupil's account	X			X				
Attempting to access or accessing the school network, using the account of a member of staff		X		X	X			

Corrupting or destroying the data of other users		X			X			
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X			X	X		X
Continued infringements of the above, following previous warnings or sanctions		X	X		X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X			X	X		X
Using proxy sites or other means to subvert the school's / academy's filtering system		X		X	X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident	X			X	X		X	
Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X						

Actions / Sanctions

Incidents:	Refer to Headteacher	Refer to HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	x		
Inappropriate personal use of the internet / social				x		

media / personal email						
Unauthorised downloading or uploading of files				x		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account				x	x	
Careless use of personal data e.g. holding or transferring data in an insecure manner	x					
Deliberate actions to breach data protection or network security rules	x	x		x		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	x			x	x	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x	x			x	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	x	x			x	
Actions which could compromise the staff member's professional standing	x	x			x	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	x	x			x	
Using proxy sites or other means to subvert the school's / academy's filtering system	x			x		
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x		x	x	
Deliberately accessing or trying to access offensive or pornographic material	x	x	x	x	x	x
Breaching copyright or licensing regulations	x			x		
Continued infringements of the above, following	x			x	x	

previous warnings or sanctions						