Hotwells Primary School

Online Safeguarding Policy

'Learning to Bring out the Best in Everyone'

Last reviewed: October 2018

Next review date: October 2019

'The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation- technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene and escalate any incident where appropriate.' DfE Guidelines

Contents:

Please see further policies that closely relate to the information included in this document:

- Safeguarding and Child protection Policy
- Code of Conduct for School Employees
- Data Protection Policy

Core principles of Online Safety

Hotwells Primary School is committed to the safety and welfare of pupils whilst they are online. The importance of technology is recognised as a tool for learning, creativity and enjoyment to parents, pupils and staff and we aim to provide a productive, safe and stimulating environment in which to use it. Our policy is in line with Ofsted's three key risk areas for children;

- *Content: being exposed to illegal, inappropriate or harmful material.*
- *Contact: being subjected to harmful online interaction with other users.*
- *Conduct: personal online behaviour that increases the likelihood of, or causes, harm,*

Pupils are taught about online safety at an age appropriate level and are given the best possible chance of avoiding harm, providing them with the resilience to overcome challenges that they may face online. They are taught how to conduct themselves in an appropriate way towards others when online.

It is recognised that there are strong links between online activity and emotional wellbeing. Our PSHE and Computing schemes of work identify the importance of equipping pupils with the necessary tools and knowledge to assess and manage risk and there are direct links made to risks posed when using online technology.

Parents, staff and pupils work together to ensure that our community is safe and parents are included when managing incidents regarding online safety. This ensures the best possible outcomes and learning opportunities for all involved.

This policy has been written by school staff with reference to and guidance from the NCPCC and Unique Voice. It has been reviewed and agreed by the Senior Leadership Team and Governors. The policy should be reviewed annually.

Understanding Online Safety

All staff receive regular online safety as part of our overarching safeguarding procedures. This may be in the form of staff meetings, inset days or through regular updates to notify staff on developing areas or concerns to be aware of and discuss with pupils.

Alongside identifying and managing the risks associated with the online world, it is important to highlight the importance of online technology. Advice from the NCPCC is used to strike a balance between effectively recognising both the benefits and the dangers.

'Children and young people go online to connect with friends, and make new ones, to browse the internet for information, chat with others and play games. They may:

- *search for information or content on search engines*
- *share images and watch videos through websites or mobile apps*
- *use social networking websites*
- *write or reply to messages on forums and message boards*
- *play games alone or with others through websites, apps or games consoles*
- *chat with other people through online games, messaging apps, games consoles, webcams and social networks*

When online, children and young people can learn new things, get help with homework, express themselves creatively and connect with friends and family'.

The NSPCC have also listed dangers to recognise;

- *'Inappropriate content, including pornography*
- *Bullying*
- *Sharing personal information*
- *Ignoring age restrictions*
- *Grooming, sexual abuse*
- *Friending or communicating with strangers.'*

It is our aim to educate our school community on both the positives and negatives of the internet.

Our Aims

We aim to:

- Encourage an environment that allows for open conversations about online safety. Allow sufficient time to be dedicated to teaching and learning the skills for safe internet usage within school time and at home.
- Include pupils, parents and staff when dealing with online safety issues to encourage empowerment for all.
- Ensure that everyone involved in any incident is supported and incidents are acted on immediately and used as a learning tool to help avoid repeat occurrences.
- Educate parents, providing them with the same information we give to our children.
- Set clear expectations for rules for behaviour online when in school and at home. It is clear that inappropriate behaviour online will be taken as seriously as any 'face to face' action.
- Ensure that children know that using prejudicial or derogatory language is unacceptable.
- Ensure that our school internet provision is set within age appropriate restrictions regarding access to content.
- Ensure that children learn how to use security settings online and how to report incidents to the school and the website.
- Ensure parents and staff are aware of how to set appropriate privacy setting when using online social networking.
- Ensure that pupils are supported in building resilience to radicalisation by providing a safe environment to debate controversial issues and helping them to understand how they can influence and participate in decision making.
- Reward good behaviour often to heighten the awareness of positive online activity.
- Ensure our pupil's views are recognising through the annual 'Pupil Questionnaire' where they will be asked how confident they are in keeping themselves safe online and whether they know how to report any problems they might experience.

Staff and parents are directed to the following trusted sources for further information and advice surrounding online safety:

- NSPCC
- Thinkuknow
- Department for Education
- Mind
- Bullying Lives
- The Safer Internet centre
- kidsmart

Internet Access – Authorisation, Filtering and Monitoring

There is a duty to provide pupils with quality internet access as part of their learning experience. The purpose of internet usage in school is to raise educational standards, to enhance pupil achievement and well-being and to support the professional work of staff. It is also used for managing information and business administration systems.

- **Enhancing learning:** the school internet access is designed expressly for educational use. There is a robust filtering system to ensure that access is age appropriate for pupils. If at any time this is compromised the technicians are notified immediately (via Trading With Schools.)

  Pupils are given clear objectives when using the internet and are taught the benefits of using the internet for research; they are taught the skills required to obtain reliable and safe information.

- **Access:** all staff and pupils are granted access to the internet. Pupil access is supervised at all times.

- **Managing content:** staff and pupils are made aware that materials sourced from the internet should comply with copyright laws.

  In regard to our school website/Twitter page: no child pictured/recorded is identifiable by name. Pupil's full names are not used anywhere on our website. We comply with requests by parents and carers for their child's photograph not to be published online. This is checked

annually. SLT staff hold admin rights to the webpage and ensure that all content is appropriate and edited with the safety of our children in mind.

- **Filtering:**

  Filtering of the wider internet is controlled by our external computing team and any inappropriate or unsafe content will be identified immediately. At KS1, internet access will be limited to demonstration only or navigating pre-approved online resources.

  The school will continue to work with parents, the DfE and the TWS to ensure systems are reviewed and improved regularly to ensure our children remain protected. The technical team make regular checks to ensure that filtering methods are effective and reasonable.

  If unsuitable sites have been accessed it will be reported immediately to the Computing Co-ordinator who will work with the computing team to investigate how this occurred. The staff will be trained to remove the device on which the incident happened so that the serial number can be recorded and given to the TWS team in order for them to investigate. Parents will be informed if necessary and details will be recorded on CPOMs.

Assessing Risk

- Although 'filtering' is in place, it is impossible to guarantee that content of an inappropriate nature will never be accessed, due to the scale of the internet and the ability to 'link' information. Staff are vigilant when pupils are using school devices and educate them in how to deal with unexpected and unwanted content. These incidents are managed quickly, appropriately and supportively.

- Members of our school community are aware that it is a criminal offence to use our computer systems or devices without permission or for inappropriate purposes under the 'Computer Misuse Act 1990.

- Methods for identifying risks and how to minimise them are reviewed annually. Audits of policies and procedures are carried out regularly by the Computing lead and in conjunction with a member of SLT, the DSL, the Governor overseeing safeguarding and the TWS technical team. This audit may include a review such as the '360 Degree Safe Online Safety Self Review Tool'. As

a result of these reviews, action is taken to improve practice to ensure the highest possible standard of online safety education and implementation.

- Governors and SLT receive feedback on online safety matters, which includes details of any incidents which have occurred.
- The SLT team ensure that the Internet Policy is implemented and complied with by all.
- All incidents are recorded and patterns observed using CPOMs.

Communication

- Pupils are only able to use approved e-mail accounts on the school system. They are taught how to report inappropriate e-mail content that they receive. Pupils are regularly reminded of the importance of not sharing personal details online. All pupil school email accounts are limited to only send and receive emails from other Hotwells accounts and not from external email contacts. They are reminded never to share their email passwords.
- All correspondence sent electronically by the staff of Hotwells Primary School must be written carefully in order to uphold our reputable name in the same way that a letter would be written if sent on school headed paper.
- Pupils are taught how to safely use age-appropriate social media and how to converse online, as part of the Computing curriculum. The same advice is given to parents with the aim that safe use of social media continues out of school.
- Pupils are taught how to safely communicate when using mobile phones. Children are not allowed mobile phones with them during the day. Any mobile phones will be kept safe within the school office from the beginning of the day to the end and at no point should pupils' mobile phones be switched on during their time on school premises. Mobile devices are not permitted on school trips or residential visits..

Appropriate use of Devices

Staff:

See Appendix 2 Internet Code of Practice for Teachers and Adults

- Staff and volunteers must not use personal mobile phones or other devices for personal reasons when they are responsible for children – this includes in the classroom, in the playground or outside areas and when taking part in educational visits offsite. However, staff always have access to a mobile phone when offsite with pupils, in case of emergency.

Parents:

- Parents are strongly discouraged from taking photos when on the school site. If photos are taken (for example, during performances or sports days) they are reminded that these photos should not be uploaded onto social media without permission from parents of every child within the photo.

How the policy is introduced to Pupils

- Rules for internet access and usage are introduced to pupils at the beginning of every year. These are repeated before any internet use takes place. The SMART approach to online safety is displayed in every classroom or area where devices may be used.

- Pupils are taught early in the school year about responsible use of the internet and this is revisited regularly. Open conversation and discussion takes place to encourage honesty and question and answer sessions.

- Pupils are reminded that internet activity is monitored and that the school holds access to their school email accounts and can monitor them at any point.

- All children in from Year 2 – Year 6 are presented with the 'Internet Code of Practice'. This is fully explained to them and further discussion will take place in Term 1 of each year to ensure their understanding and cooperation. These are then sent home to parents to discuss with their child and a signed copy is returned to school. If a parent/child declines to sign this agreement then that child will only be able to use the school internet on a 1:1 basis with an adult leading the application.

- Displays promote the 'SMART' approach to Online Safety.
- All pupils observe the 'SMART' approach and this will be delivered at an age appropriate level to all pupils.

How the policy is introduced to Parents

- The Online Safety Policy is signposted in school newsletters and posted on our school website.
- Regular information is provided to parents on how to keep children safe when online.
- If concerns are brought to the attention of staff during class discussion or in the wider media regarding developing issues, we may send further correspondence home to parents with specific advice and support to consider.
- Any incidents regarding the internet are reported to parents in a supportive and appropriate manner.
- A supportive partnership is encouraged between the school and parents to ensure that a uniform approach to online safety is taken. This may include inviting parents to presentations by external professionals or school staff or suggestions on safe online behaviour at home.
- Parents are involved in discussing the terms of agreement for internet use in our school with their child. A signed copy is returned by the parent before the child is allowed access to the internet in school.

Staff Awareness

- The DSL (Catherine Delor) and Senior Leadership staff should ensure that they have relevant and up to date training in the area of online safety in relation to Child Protection and Safeguarding.

- All staff, visiting staff, students and any other professional using the internet in our school are asked to sign an 'Internet Code of Practice' agreement (Appendix 2) before they are allowed to use the internet in our school. They are given a copy of this document.
- The staff are aware of the consequences for the misuse of the internet and school devices and are confident in applying these steps.
- Staff development regarding the safe and responsible use of the internet as well as understanding of this policy is given as required.
- Visiting staff such as teaching students may be given temporary access to the school Google Drive. This access is terminated as soon as their time in school ends. Their access is limited to ensure sensitive documentation is not available to them. Their access will allow them to use the 'All Staff' folder which contains school policies. It is made clear to them that their access is monitored as is any online activity that they carry out.
- All staff are given a gmail account in order to use the Google Drive. Staff are made aware that their activity when using this is monitored and the content of their email account can be accessed, monitored and terminated at any time.
- Staff should not transfer sensitive information on portable devices such as memory sticks. This information should instead be communicated using encrypted email. Careful consideration should be taken before transmitting sensitive information.
- Use of staff laptops are covered under Appendix 2 Internet Code of Practice for Teachers and Adults

Dealing with Incidents and Complaints

- All incidents and complaints in relation to online behaviour should be reported to the Computing Lead and/or a senior member of staff to deal with.
- Any incident or complaint involving a member of staff must be reported straight to the Head teacher.
- Pupils and parents will be informed of the complaints procedure.
- All incidents that have involved risk/potential of risk must be recorded on to CPOMs immediately.

- All incidents must be communicated in the appropriate manner to the wider staff team in order to use it as a learning opportunity (for both pupils and staff) and to reduce the chance that reoccurrences might take place.
- Following any incident, parents and staff will work together in order to deal with the situation in a positive and thorough manner.
- If a serious incident has been reported where staff or pupils have been put at significant risk or have posed such a risk to others then senior staff should decide whether police contact is an appropriate measure.

Network Security and Management

'Trading with Schools' are employed by the school to ensure:

- that the technical infrastructure is secure and not open to misuse or malicious attack
- that the school meets required online safety technical requirements
- that users can only access the networks and devices through properly enforced password entry. They will also enforce regular password changes
- that the filtering system is applied and updated on a regular basis and that this is the responsibility of a team of people and not of a single individual
- that they remain up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update the school staff with relevant information
- that the network, internet, learning platforms, remote access and email is regularly monitored in order that any misuse/attempted misuse can be reported to the Head teacher
- that monitoring systems and software are implemented and updated in agreement with the school
    - Servers, wireless systems and cabling will be securely located and physical access will be restricted. This is for safety purposes and also to avoid tampering of any kind with our technical equipment that may harm the school computing system.
    - Administrator passwords for the school email/Google Drive systems as well as passwords for the school webpage will be held by Senior Management as well as the Head teacher.

Appendix 1

Hotwells Primary School

Internet Code of Practice for Pupils

- I will only use the internet when supervised by a teacher or adult.
- I will never tell anyone I meet on the internet my home address, my telephone number or my school's name without permission, or send a picture of myself. I will never arrange to meet anyone in person.
- I will never give any passwords to anyone, even my best friend, and I will log off when I have finished using the computer.
- I will never hang around in a chat room if someone says or writes something which makes me feel uncomfortable or worried and I will always report it to a teacher or parent.
- I will never answer unpleasant, suggestive or bullying emails or messages and I will always report it to a teacher or parent.
- I will not look for bad language, inappropriate images or websites and I will report bad language, inappropriate images or websites to a teacher or parent if I come across them accidentally. I know that my teacher can check the websites I have visited!
- I will always be myself and will not pretend to be anyone or anything I am not. I know that the posting of anonymous messages and the forwarding of chain messages is not allowed.
- I understand that I can only use websites for my work in school and that I will not be allowed to use the Internet if I look at unsuitable material on purpose.
- I may not download any software from the Internet. I know that information on the Internet may not always be reliable and may need checking. I know that some websites may be sponsored by advertisers.
- I will not use the internet or email to send or encourage material which is illegal, extremist, offensive or annoying or invades another person's privacy.

✂ ----------

Pupil's Name: _____

I have read the Code of Practice for Pupils and I have discussed it with my son/daughter. We agree to support the school's policy.

Signed (Parent/Guardian/Carer) _____

Date: _____

Appendix 2

Hotwells Primary School

Internet Code of Practice for Teachers and Adults

Teachers/adults should be familiar with the school's online safety policy and the Hotwells Primary School Internet Code of Practice for Pupils.

I will use all IT equipment issued to me in an appropriate way.

I will not:

- Access any offensive website or download any material that is deemed inappropriate
- Use the internet excessively for personal use – this includes email
- Access social networking sites during work time and will not converse in any way with pupils on personal social networking accounts. If I am contacted in this way I must bring it to the attention of the Head teacher.
- Place inappropriate content onto the internet
- Send any offensive or inappropriate emails
- Download any materials or files that may corrupt or interfere with school security systems
- Upload any photos or information that could identify specific children unless permitted by parents through their annual 'Photo consent'
- Upload any information or behave in a way that could put pupils or staff in danger or bring the school into disrepute

I understand that:

- A Staff laptop remains the property of the school at all times. On leaving school employment the laptop is returned immediately.
- Only members of staff are allowed access to school laptops and passwords should NOT be shared.
- The school laptop must not be left unsecured (logged in) when unsupervised – including when it is in a classroom.
- The school laptop must be kept securely at the end of the school day, for example, locked in the school office cupboard. If it is taken off school premises it is the staff member's sole responsibility to ensure that it is stored securely.

- If on extended leave I must hand my laptop back to the school unless with prior agreement with the headteacher.
- No new software should be loaded onto a school laptop without the permission of the school. TWS carry this out to ensure viruses are not downloaded.
- Deliberately accessing internet sites or content that contains illegal material is a criminal offence
- When using a laptop within the classroom, appropriate action should be taken to ensure videos, audios or any other content is checked rigorously before being shown to children to ensure that it is appropriate. Measures should be taken to maintain the highest possible standard for safety when using the internet for learning in the classroom. For example, when showing a 'YouTube' clip, apps such as 'Nicer Tube' can be used to remove all pop-ups or window display around the video.
- The school reserves the right to view all emails and computer files and may monitor internet sites visited
- Disciplinary actions may be taken if the internet is used inappropriately.

✂ ----------

I agree to abide by the Hotwells Primary School Code of Practice for Teacher and Adults

I have read the Online- safety Policy and Code of Practice for Pupils. I agree to support the school's policy.

Signed _____ Date _____