Highbury Primary School

'Valued as Individuals, Inspired and Nurtured as Learners'

Respect, Resilience, Confidence, Kindness, Inclusive, Aspiration

E-SAFETY POLICY

Highbury Primary and Nursery School's mission is:

- To be an inclusive, safe and caring community where each member is equally valued and nurtured to develop their potential.
- To achieve academic excellence by ensuring each pupil performs to the best of their ability.
- To work together as a team with parents and carers within the community to promote rights, respect and responsibility for the benefit of all.

At Highbury Primary School, we recognise the importance of safeguarding children from potentially harmful and inappropriate online material, and we understand that technology is a significant component in many safeguarding and wellbeing issues.
We believe that the Internet and other digital technologies are powerful resources which can enhance and potentially transform teaching and learning when used effectively and appropriately. The Internet is an essential element of 21st century life for education, business and social interaction. The school provides pupils with opportunities to use the Internet for research, remote learning and online communication, along with developing the skills necessary to access, analyse and evaluate them safely.

The Internet supports the professional work of staff and enhances the school's management information and business administration systems. Safe access to the Internet is necessary for staff and pupils. The aim of our policy is to help ensure safe responsible use of ICT and the Internet and is built on the following core principles of Digital Citizenship linked to computing.

DIGITAL CITIZENSHIP is built on three key principles:

Digital Literacy – how we protect ourselves in the online world
Those who are literate in the online world are better prepared to avoid risky situations, make better-informed decisions, and better understand how to maintain their privacy. Children will learn basic online safety habits like how to protect their accounts and reputation, the importance of strong and secret passwords, and how to update their computers and devices to defend against malware and scams.
Digital Civility – how we protect each other

Internet users should demonstrate respect for others—behaving with civility and being protective of everyone's rights (including their own). They should learn and apply the skills to behave ethically and within online social norms. Children will learn skills that include being judicious about what they say and do online as well as protecting others' privacy by not sharing personal details of friends and family without their permission.

Information Literacy – how we protect content
Information literacy is the ability to identify, locate, evaluate, and effectively use information from the Internet to complete a task, answer a question, or research a topic. Children will learn how to correctly evaluate the validity of information on the Internet, how to protect the content they publish, and how to accurately give credit to the work of others.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

1. **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
2. **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
3. **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
4. **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

We recognise that:

- The online world provides everyone with many opportunities; however, it can also present risks and challenges
- We have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online.
- We have a responsibility to help keep children and young people safe online, whether or not they are using Highbury Primary School's network and devices.
- All children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse.
- Working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

We will seek to keep children and young people safe by:

 appointing an online safety coordinator who is also our Computing lead.

 providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code of conduct for adults (see staff code of conduct).

 supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others

 supporting and encouraging parents and carers to do what they can to keep their children safe online

 developing already established procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person

 reviewing and updating the security of our information systems regularly

 ensuring that usernames, logins, email accounts and passwords are used effectively and safely
 ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate, in line with the school's Data Protection Policy which can be found on our School website
 ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given
 providing supervision, support and training for staff and volunteers about online safety
 examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

If online abuse occurs, we will respond with education. There is a clear and robust safe-guarding procedure in place for responding to abuse (including child-on-child online abuse). The school provides support and training for all staff and volunteers on dealing with all forms of abuse, including bullying/cyber-bullying, emotional abuse, sexting, sexual abuse and sexual exploitation (see School Behaviour Policy and Child Protection Policy). All responses to abuse take the needs of all parties into account – the person experiencing the abuse, any bystanders and the impact it may have on the school as a whole. The plan developed for addressing online abuse is reviewed regularly, in order to ensure that any problems have been resolved in the long term.

Data Protection and Security

Any personal data used by staff, including that gathered through digital sources will be dealt with in line with the Data Protection Policy. This can be found on our school website.

Internet Safety Awareness

To protect and educate the whole school community in its safe and responsible use of technology, including mobile technology we will:

Protect

• Put in place robust filtering and monitoring systems to limit children's exposure to the 4 key categories of risk (described above) from the school's IT systems

• Make all pupils, parents and staff aware that they are expected to follow the acceptable use of the internet and IT systems in school

Educate

• Educate pupils about online safety as part of the curriculum. Including:

* The safe use of social media, the internet and technology, including that used for remote learning
* Keeping personal information private and secure
* How to recognise unacceptable behaviour online
* How to report any incidents of cyber-bullying, ensuring pupils are encouraged to do so, including where they are a witness rather than a victim

• Train staff, as part of their induction, on safe internet use, including technology used for remote learning, and online safeguarding issues including cyber-bullying and the risks of online radicalisation. Online safety is included in the annual safeguarding training.

• Educate parents about online safety via the school's website and through communications sent directly to them. We will also share clear procedures with parents, so they know how to raise concerns about online safety

At Highbury Primary School we believe that alongside having a written safety policy, it is essential to educate all users in the safe and effective use of the Internet and other forms of digital communication. We see education in appropriate, effective and safe use as an essential element of the school curriculum. This education is as important for staff and parents as it is for pupils.

Practical Steps for Remote Learning

1. All remote learning and any other online communication will take place in line with current confidentiality expectations.

- Staff are responsible for all e-mails they send and are expected to use the same professional levels of language and content as would be expected in any correspondence leaving the school.
- All e-mails will copy in their year group colleague or member of SLT if appropriate, and use BCC if communicating with multiple users.
- Use of TEAMs chat is monitored for inappropriate use, and any misuse is investigated and recorded using CPOMs.
- All participants are made aware that TEAMs record all activity.

2. Staff will never record lessons or meetings using personal equipment.

3. Only members of the Highbury Primary School community will be given access to classes in TEAMs.

4. Access to TEAMs will be managed in line with current IT security expectations; for example; use of strong passwords, logging off or locking devices when not in use.

Behaviour Expectations

When recording or sharing videos, participants are required to:

- wear appropriate dress.
- ensure backgrounds of videos are neutral (or may be blurred).
- ensure that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds.
- professional levels of language and content used in videos should be the same as would be expected in the classroom.
- All videos should be viewed in a shared area, and all participants should be aware of other people in the background and of their conduct.
- Any online meetings, which have been agreed with SLT, should always be conducted alongside another school professional.

Online Performances (such as Nativity)

- Performance will be recorded, not live.
- Parents will be asked to consent to their child being included.
- A time-scale will be provided for when and how long the performance will be available for, and the platform being used to share the performance.
- Acceptable use agreements have been signed by staff, pupils and parents/carers.
- The school has considered the minimum age requirement for the platform being used to share the performance, how the performance is being shared with the audience and what strategies are in place to prevent onward sharing.

- Expectations for performance behaviour are discussed with staff and pupils prior to their performance.

Policy Breaches and Reporting Concerns

Participants are encouraged to report any concerns during remote learning. These are all dealt with in line with the Data Protection Policy. All data breaches are reported to Mrs Rhodes as the Data Champion and any other concerns are shared with Mrs Watson as Head Teacher. Any safe-guarding concerns will be reported to Mrs Watson, as the Designated Safe-guarding Lead, or Mrs Frost and Mrs Hartt in her absence, in line with our Child Protection Policy. Inappropriate online behaviour will be responded to in line with existing policies such as acceptable use of technology, allegations against staff, anti-bullying and behaviour. Consequences for deliberate misuse may include restricting/removing use, contacting parents or police if a criminal offence has been committed.

Online Safety

https://www.thinkuknow.co.uk/Teachers/

http://www.saferinternet.org.uk/

With the current speed of on-line change, some parents and carers have only a limited understanding of online risks and issues. Parents may underestimate how often their children come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. Some of the risks could be:

• unwanted contact

• grooming

• online bullying including sexting

• digital footprint (the information about a particular person that exists on the internet as a result of their online activity).

The school will therefore seek to provide information and awareness to both pupils and their parents through:

• Acceptable use agreements for children, teachers, parents/carers and governors

• Curriculum activities involving raising awareness around staying safe online

• Information included in letters, newsletters, web site

• Parents evenings / sessions

• High profile events / campaigns e.g. e-safety week

• Building awareness around information that is held on relevant web sites and or publications

• School social media policy

Social media

https://www.thinkuknow.co.uk/Teachers/Resources/

http://www.saferinternet.org.uk/search-results?keywords=social%20networking

http://www.childnet.com/search-results/?keywords=social%20networking

http://www.kidsmart.org.uk/socialnetworking/

Cyberbullying

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/37485 0/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

http://www.hampshire.police.uk/internet/asset/f0db2eea-0e3c-4fb4- b98ce3fa681b860P/primary-social-networking-cyber-bullying

Central to the School's anti-bullying policy should be the principle that 'bullying is always unacceptable' and that the school ethos of 'Pro-Kindness' is promoted so that 'all pupils have a right not to be bullied'. The school should also recognise that it must take note of bullying perpetrated outside school which spills over into the school and so we will respond to any cyberbullying we become aware of carried out by pupils when they are away from the site. Cyberbullying is defined as "an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend himself/herself."

By cyber-bullying, we mean bullying by electronic media:

• Bullying by texts or messages or calls on mobile phones

• The use of mobile phone cameras to cause distress, fear or humiliation

• Posting threatening, abusive, defamatory or humiliating material on websites, to include blogs, personal websites, social networking sites

• Using e-mail to message others

• Hijacking/cloning e-mail accounts

• Making threatening, abusive, defamatory or humiliating remarks in on-line forums

Cyber-bullying may be at a level where it is criminal in character. It is unlawful to disseminate defamatory information in any media including internet sites. Section 127 of the Communications Act 2003 makes it an offence to send, by public means of a public electronic communications network, a message or other matter that is grossly offensive or one of an indecent, obscene or menacing character. The Protection from Harassment Act 1997 makes it an offence to knowingly pursue any course of conduct amounting to harassment. If we become aware of any incidents of cyberbullying, we will need to consider each case individually as to any criminal act that may have been committed. The school will pass on information to the police if it feels that it is appropriate or are required to do so.

Sexting

https://www.thinkuknow.co.uk/Teachers/Resources/

http://www.hampshire.police.uk/internet/adviceandinformation/safe4me/Safe4me+%27Sexting%27

https://www.ceop.police.uk/Media-Centre/Press-releases/2009/What-does-sextingmean/

'Sexting' often refers to the sharing of naked or 'nude' pictures or video through mobile phones and the internet. It also includes underwear shots, sexual poses and explicit text messaging. While sexting often takes place in a consensual relationship between two young people, the use of Sexted images in revenge following a relationship breakdown is becoming more commonplace. Sexting can also be used as a form of sexual exploitation and take place between strangers. As the average age of first smartphone or camera enabled tablet is 6 years old, sexting is an issue that requires awareness raising across all ages. The school will use age appropriate educational material to raise awareness, to promote safety and deal with pressure.

Parents should be aware that they can come to the school for advice.

Gaming

http://www.saferinternet.org.uk/search-results?keywords=gaming

http://www.childnet.com/search-results/?keywords=gaming

http://www.kidsmart.org.uk/games/

http://www.lgfl.net/esafety/Pages/Primary-resource-matrix.aspx

Online gaming is an activity that the majority of children and many adults get involved in. The school will raise awareness:

• By talking to parents and carers about the games their children play and help them identify whether they are appropriate.

• By supporting parents in identifying the most effective way of safeguarding their children by using parental controls and child safety mode.

• By talking to parents about setting boundaries and time limits when games are played.

• By highlighting relevant resources.

Online reputation

http://www.childnet.com/resources/online-reputation-checklist

http://www.saferinternet.org.uk/search-results?keywords=online%20reputation

http://www.kidsmart.org.uk/digitalfootprints/

Online reputation is the opinion others get of a person when they encounter them online. It is formed by posts, photos that have been uploaded and comments made by others on people's profiles. It is important that children and staff are aware that anything that is posted could influence their future professional reputation. The majority of organisations and work establishments now check digital footprint before considering applications for positions or places on courses.

Grooming

http://www.saferinternet.org.uk/search-results?keywords=grooming

http://www.childnet.com/search-results/?keywords=grooming

http://www.internetmatters.org/issues/online-grooming/

Online grooming is the process by which one person with an inappropriate sexual interest in children will approach a child online, with the intention of developing a relationship with that child, to be able to meet them in person and intentionally cause harm.

The school will build awareness amongst children and parents about ensuring that **the child**:

• Only has friends online that they know in real life

• Is aware that if they communicate with somebody that they have met online, that relationship should stay online.

That **parents should**:

• Recognise the signs of grooming

• Have regular conversations with their children about online activity and how to stay safe online

The **school will** raise awareness by:

• Including awareness around grooming as part of their curriculum

• Identifying with both parents and children how they can be safeguarded against grooming

Health and Safety

Highbury Primary School maintains a safe working environment for pupils and teachers using ICT resources, both in classrooms and in the Library, which was designed in accordance with health and safety guidelines. Pupils are supervised at all times when Interactive Whiteboards and digital projectors are being used.

Digital and Video Images of Pupils

Parental permission is sought to cover the use of photographs of pupils on the school website, in the local press and for displays etc. within school.

School Website

Our school website promotes and provides up to date information about the school, as well as giving pupils an opportunity to showcase their work and other aspects of school life. In order to minimise risks of any pupils' images on the school website being used inappropriately, the following steps are taken:

• Group photos are used where possible, with general labels or captions.

• Full names are not used.

• The website does not include home addresses, telephone numbers, personal emails or any other personal information about pupils or staff.

Social Media Chatrooms, blogs and other social networking sites are blocked on school computers by the Local Authority filters, so pupils do not have access to them in the school environment. However, we regard the education of pupils on the safe and responsible use of social software as vitally important and this is addressed through our Internet Safety Education for pupils. Instances of cyber-bullying of pupils or staff are regarded as very serious offences and dealt with according to the school's discipline policy and child protection procedures. Pupils are aware that any misuse of digital technology should be reported to a member of staff or trusted adult immediately.

Use of social networking sites for staff

School staff are required to maintain a separation between their professional and their private lives. This can be difficult especially given the strong relationships with pupils and parents and for those living within the community served by the school. It is expected that many colleagues would also become friends and there are many circumstances in which a member of staff could come into contact with a member of the school community which are unrelated to the fact they work in the school, such relationships are not viewed as professional. However, where any aspect of the school or school activities are mentioned or where information obtained through working at the school is discussed then professional expectations apply. Staff will ensure that they understand how any site they use operates and therefore the risks associated with using the site.

Staff will;

- Consider carefully who they accept as friends on a social networking site. They will not accept friendship requests from pupils or parents – as they may be giving them access to personal information and allowing them to contact staff inappropriately.
- Report to the Headteacher any incidents where a pupil has sought to become their friend through a social networking site.
- Take care when publishing information about themselves and images online- assume that anything they publish will end up in the public domain.
- Ask themselves whether they would feel comfortable about a current or prospective employer, colleague, pupil or parent viewing the content of their page.
- Not post anything that names or involves the school, or may be interpreted as slanderous towards colleagues, pupils or parents.
- Ensure they follow school procedures for contacting parents and/or pupils and only contact pupils and/or parents via school-based computer systems.
- Not use social networking sites to contact parents and/or pupils.
- Through their teaching, alert pupils to the risk of potential misuse of social networking sites.

The use of mobile phones

- Staff are aware of the restrictions placed on them with regards to the use of their mobile phone and cameras, including that:

  *Staff are allowed to bring their personal phones to school for their own use, but will limit such use to non-contact time when pupils are not present

  *Staff will not take pictures or recordings of pupils on their personal phones or cameras

- Staff, pupils and parents are made aware that staff have the power to search pupils' phones, as set out in the DfE's guidance on searching, screening and confiscation

Filtering and Monitoring

Appropriate Use:

Children are permitted to use the Internet for educational purposes under the guidance and supervision of school staff. Access is restricted to approved platforms and websites deemed suitable for the primary school age group.

Content Filtering:

The school employs content filtering measures to restrict access to inappropriate or harmful content, ensuring students can only access educational and age-appropriate materials.

Monitoring:

Internet usage within the school will be monitored to ensure compliance with this policy. Monitoring aims to maintain a safe and positive online environment for all students.The DSL has responsibility for ensuring effective Filtering andMonitoring procedures are in place.

Reporting Inappropriate Content:

Children are encouraged to report any inappropriate content encountered during Internet usage to a member of staff immediately.

Consequences of Violation:

Violations of this policy may result in disciplinary actions as outlined in the school's behaviour policy. Repeat violations may lead to restricted or revoked Internet privileges.

Education and Awareness:

Primarily through the computing and PSHE curriculum, children are taught to assess and evaluate content on the internet to help ensure their own safety.

Responsibilities:

The Senior Leadership Team are responsible for implementing, enforcing, and regularly reviewing this policy to ensure its effectiveness and relevance.

Parental Involvement:

Parents are encouraged to actively monitor and guide their children's Internet usage outside of school hours, reinforcing safe online practices.

This policy is reviewed annually by the governing body in line with the policy review schedule.

Approved by the Governing Body:
……

Date implemented: December 2023 Review Date: December 2024