Healdswood Infant & Nursery School

Online Safety Policy

23/24

Ratified at FGB 6th December 2023

Review Autumn term 2024

Healdswood Infant & Nursery School Online Safety Policy

Context

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. This policy is written in line with 'Keeping Children Safe in Education' 2023 (KCSIE), 'Teaching Online Safety in Schools' 2019, statutory RSHE guidance 2019 and other statutory documents. It is cross-curricular and designed to sit alongside the school's statutory Safeguarding Policy. Any issues and concerns with online safety must always follow the school's safeguarding and child protection procedures.
The internet is widely used in school by all staff and pupils. KCSIE 2023 highlights that some children are at greater risk of harm than others, both **online and offline.** It is the duty and responsibility of **all staff** to ensure that pupils are using the internet safely and responsibly in school and that they understand the important of online safety to keep them safe at home and school.

What are the main online safety risks

Online-safety risks are traditionally categorised as one of the 4 Cs: Content, Contact, Conduct or Commerce (see section 135 of KCSIE 2022). These categories provide a structured approach to understand the risks and formulate appropriate potential school response, whether technological or educational.

They do not stand in isolation, and it is important to understand the interplay between all three. This is evident in Ofcom's Media and Attitudes Report 2022 which suggests 36% of children aged 8-17 had seen something 'worrying or nasty' online in the past 12 months, with 84% experiencing bullying via text or messaging, on social media, in online games, through phone or video calls, or via other aps and sites.

Healdswood Infant & Nursery School is committed to harnessing the positive impact and educational benefits of the internet while being vigilant about the potential risks. We strive to create a safe environment that no only shields our children but also imparts knowledge on how to navigate the online world safely.

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 inside and outside of school.
The Education and Inspections Act 2006 empowers Head Teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other online safety incidents covered by this policy, which may take place outside of Healdswood Infant and Nursery School.

The school will deal with such incidents within this policy (and the associated Behaviour and Anti-Bullying policies) and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Aim of the policy

Healdswood Infant and Nursery School embraces positive impact and educational benefits that can be achieved through appropriate use of the internet and associated communications technologies. We are also aware that inappropriate or misguided use can expose both adults and children to unacceptable risks and dangers. We aim to provide a safe and secure environment which not only protects all people on the premises but also educates them on how to stay safe in the wider world.
It is equally important that staff have access to regular Online Safety training and are informed of any current thinking or changes in practice. We also have a duty of care to our parents/carers and offer Online Safety updates via class dojo and information on the school website.

Legislation

This policy adheres to the Department for Education's statutory safeguarding guidance, 'Keeping Children Safe in Education,' encompassing advice on teaching online safety, preventing and tackling bullying, and relationships education. Compliance with acceptable use terms for the school's network systems and the internet is an obligation for all staff and governors. The following section outlines the online safety roles and responsibilities of individuals within the school:

The Designated Safeguarding Lead(s):

KCSIE makes clear that “the designated safeguarding lead should take **lead** responsibility for safeguarding and child protection (including online safety).”

The Governing Body:

The governing body has overall responsibility for monitoring this policy. The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).
All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school’s ICT systems and the internet.

Head Teacher:

The Head Teacher has a duty of care for ensuring the safety (including online safety) of members of the school community. The Head Teacher and other designated safeguarding members of staff are ensuring that any online safety incidents and or cyber bullying incidents are logged and dealt with appropriately in line with this policy and the behaviour policy. They are also aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

Online Safety Lead:

Takes responsibility in establishing and reviewing the school policies for computing and online safety and associated documents, including Acceptable Use Policies.
Ensure that the policy is implemented and that compliance with the policy is actively monitored

Ensures that all staff are aware of the procedures and requirements in the event of an online safety incident.

Keep up to date with online Safety issues and guidance through liaison Nottinghamshire's Local Authority Schools ICT team and through advice given by agencies such as the Child Exploitation and Online Protection Centre (CEOP)

To provide online safety training for staff, parents/carers and governors

Technical staff:

Technical staff (ATOM) support school with ICT and computing are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- That they keep up to date with online safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- That the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head Teacher/Computing Lead for investigation / action / sanction.
- The school ICT system security is reviewed regularly.
- Virus protection is updated regularly.

Teaching and Support Staff

The Teaching and Support Staff, is responsible for:

- Remaining informed about online safety matters and implementing school policies.
- Adhering to the Staff Acceptable Use Agreement.
- Reporting any suspected misuse to the Head Teacher/DSL.
- All digital communications with parents/carers should be professional using the agreed school procedure (Code of Conduct).
- Ensuring online safety awareness permeates the curriculum and implementing the
- Monitor the use of digital technologies*, e.g. laptops, iPads* etc in lessons and the wider school where permitted and implement the policy with regards to these devices.
- Monitoring digital technology use in lessons, following current policies.

Parents/Carers

Parents/carers are important partners in promoting online safety. Our school engages parents/carers through Class Dojo, school website updates, and parents' evenings, promoting the importance of online safety practices and encouraging the guidelines on the appropriate use of:

• Digital and video images taken at school events.

• Access to parents' sections of the website.

Managing filtering

In accordance with KCSIE 2023, the governing board oversees the designated safeguarding lead's understanding of filtering and monitoring systems. Regular reviews, effective monitoring and filtering system is inappropriate content, and safeguarding-aligned monitoring strategies are integral to our approach.

Managing filtering KCSIE 2023 includes:

- The governing body should ensure the designated safeguarding lead (DSL) takes responsibility for understanding the filtering and monitoring systems and processes in place as part of the role (*paragraph 103*).
- Governors should ensure all staff understand the expectations, roles and responsibilities of filtering and monitoring as part of their safeguarding training (paragraph 124).
- The Child Protection policy includes the school approaches for filtering and monitoring on school devices and school networks (paragraph 138).
- Governors should review the DfE's filtering and monitoring standards and liaison with the Head Teacher to ensure the school is upholding the standards (paragraph 142).

Furthermore, the updated KCSIE (paragraph 142) relating to the filtering and monitoring standards 'which set out that schools' should:

• *Identify and assign roles and responsibilities to manage filtering and monitoring systems*

• *Review filtering and monitoring provision at least annually*

• *Block harmful and* inappropriate content without unreasonably impacting teaching and learning

• Ensure effective monitoring strategies are in place that meet their safeguarding needs.

Education and Curriculum

Healdswood Infant & Nursery recognises the diverse digital landscape, our approach aims to equip pupils with the essential knowledge and behaviours that empower them to navigate the online world safely and confidently, irrespective of the device, platform, or application they encounter.

Online safety should be a focus of the curriculum and teachers should reinforce online safety through the curriculum. The online safety curriculum should be broad, relevant and provide progression:

- The curriculum is coherently and cumulatively sequenced to ensure all children acquire the knowledge and understanding essential to being safe online.
- Learning is context-relevant with agreed progression (National Curriculum) leading to evidenced outcomes.
- Children's needs are addressed through effective teaching and assessment (QFT).
- Digital competency and online safety are taught through other curriculum subjects *e.g. PHSE.*
- It incorporates relevant national initiatives and *opportunities e.g. Safer Internet Day and Anti-Bullying .*
- Ensure that teaching will be accessible to children at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- Ensure children are guided to websites which are safe.
- Where children are allowed to access the internet, staff should be vigilant in supervising the children and monitoring the content of the websites.

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Pupils are made aware of the impact of cyber bullying during assemblies, safer internet day, RSHE and anti-bullying week.

Parent Education

Parents / Carers have an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and carers through regular communication on Class Dojo and the school website.

Cyber Bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.
To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.
The school also sends information/leaflets and regularly updates the Online Safety section of the school website on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.
In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy.

Uses of Technology

Access to Our School Website:

Our school website is freely accessible without the need for a username or password. The Computing Lead is responsible for monitoring the site, while individual staff members are responsible for the content on class pages. All users are obligated to ensure that only appropriate material is uploaded. In the event of encountering any inappropriate content, users are encouraged to report it directly to the Head Teacher, who will take the necessary action.

Protection of Personal Data:

Personal data handling at Healdswood Infant and Nursery School adheres to the Data Protection Act 2018 and GDPR guidelines, which can be found on our website. Users are expected to follow these guidelines, ensuring that data is:

- Accurate
- Secure
- Processed fairly and lawfully
- Used for a limited purpose
- Retained for no longer than necessary
- Transferred only with adequate protection

Data Security Measures:

At Healdswood, we take the security of data seriously. The following measures are in place:

- Relevant staff are aware of the location of data.
- Staff with access to personal data understand their legal responsibilities.
- The school ensures that data is appropriately managed within and outside the school environment.
- All staff are aware that they should only use approved means to access, store, and dispose of confidential data.
- Staff with remote access to school data are required to maintain its security, being conscious of the risks associated with unsecured wireless access outside the school premises.

Mobile Device and Removable Media:

- All data stored on mobile devices and removable media is safeguarded through password protection and encryption.
- Devices containing sensitive data may be taken off the school premises with approval of the Head Teacher.
- Personal devices accessing school systems, such as downloading emails or files to smartphone is prohibited.
- Healdswood Infant and Nursery School proactively manages and mitigates the risk of administrative data loss.
- Staff, parents/carers, volunteers and contractors are prohibited from using any mobile devices where children are present.

Social Media

With widespread use of social media for professional and personal purposes it is imperative to establish a comprehensive policy that offers clear guidance to staff on managing online risks and behaviour. The fundamental principles of this policy revolve around safeguarding children, the school, and individuals when engaging with social media.

Teachers' professional conduct is outlined in the DfE Teachers Standards, emphasizing the trust inherent in their roles but all staff in school must understand that their responsibilities place them in a position of trust and that their conduct should reflect this.

The school provides the following measures to ensure reasonable steps are in place to minimize risk of harm to children through:

- ensuring that personal information is not published
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues
- clear reporting guidance, including responsibilities and procedures.
- risk assessment
- guidance for children, parents/carers

School staff should ensure that:

- no reference should be made in social media to children, parents/carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions should not be attributed to the school

- security settings on personal social media profiles are regularly checked to minimize risk of loss of personal information

Monitoring of public social media:

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school
- When parents/carers express concerns about the school on social media we will urge them to make direct contact with the school to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and children need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

The school will inform and educate children about these risks and will implement policies to reduce the likelihood of the potential for harm.

- staff/volunteers must be aware of those children whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes.
- in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other children in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational purposes, but must follow school policies concerning the sharing, storage, distribution and publication of those images.
- care should be taken when sharing digital/video ensuring that images are appropriate.
- Photographs published on the website, or elsewhere that include children will be selected carefully and will comply with Online Safety Policy
- Children's full names will not be used anywhere on a website, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of children are taken for use in school or published on the school website/social media.
- images will be securely stored in line with the school retention policy.

Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through:

- Public website
- Class Dojo

The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of children, and personal information – ensuring that there is least risk to those of our school community, through such publications. Where images or videos are published, their identities are protected, and full names are not published.

The school provides information about online safety *e.g., publishing the schools Online Safety Policy and acceptable use agreements*.

Communication of the Policy

Pupils:

- The Online safety policy will be conveyed to children age appropriately.
- All children will be taught about the importance of being safe online.
- Children will be notified of the monitoring of network and internet in school.
- Age-appropriate curriculum opportunities will be taught to educate children about e-safety, adapting content to address evolving risks, *e.g. apps.*

Employees:

- All staff will receive a copy of the online safety policy and are required to sign to confirm their understanding and agreement to abide by the guidelines.
- Staff are aware of system monitoring, and professional standards are expected.

Parents/Carers:

- The policy will be communicated to parents/carers through the school website.
- Parents/carers are requested to sign the photograph consent form during their children's registration.

Appendix 1: Acceptable Use Agreement: Staff and Governors

This policy is designed to ensure that all staff are aware of their professional responsibilities. All staff are expected to sign this policy and adhere at all times to its contents.

➢ I have read and understood Healdswood Infant and Nursery School's full Online Safety policy and agree to uphold the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils. I will report any breaches or suspicions (by adults or children) in line with the policy.

➢ I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Head teacher (if by an adult).

➢ I will only use the school's email / Internet / and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.

➢ I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

➢ I will ensure that all electronic communications with pupils and staff are compatible with my professional role.

➢ I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils or parents/carers.

➢ I will only use the approved, secure e-mail system(s) for any school business.

➢ I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal or sensitive data taken off site must be encrypted.

➢ I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

➢ Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head teacher.

➢ I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.

➢ I will support the school approach to online safety and not deliberately upload or add any images, video, or text that could upset or offend any member of the school community.

➢ I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

➢ I will support and promote the school's online safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

➢ I understand this forms part of the terms and conditions set out in my contract of employment.

I agree to follow this code of conduct and to support the safe and secure use of ICT

throughout the school

Signature…………………………………………….Date …………………………………….

Name………………………………….Job title…………………………….