Hart Hill Nursery School

Online Safety Policy

Updated Spring Term 2024

Ratified by SLT on 8/3/24

Signed

To be updated Spring Term 2025

Rationale

Hart Hill Nursery School is committed to safeguarding members of our school community online in accordance with statutory guidance and best practice. We are aware of the legislative framework under which this Online Safety Policy and guidance has been produced as outlined in the attached 'Legislation' Appendix.

This Online Safety Policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Hart Hill Nursery School will deal with such incidents within this policy and 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.

Aims

The aims of this policy are to:

- set expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocate responsibilities for the delivery of the policy
- regularly review in a collaborative manner, taking account of online safety incidents and changes or trends in technology and related behaviours
- establish guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- describe how the school will help prepare learners to be safe and responsible users of online technologies
- establish clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms

Roles and Responsibilities

The role of the governing body is to approve the Online Safety Policy and to ensure the review and effectiveness of the policy. The governor responsible for safeguarding and will take on the role of Online Safety Governor and will encourage regular meetings with the Online Safety Lead (DSL). During visits, they will review reports of online safety incidents, filtering control log checks and checking that the school is following the provision outline in this policy. They will report their findings to the full governing body. The governing body will also support the school in encouraging parents and carers and the wider community to become engaged in online safety activities.

The role of the Headteacher is to take day-to-day responsibility for online safety issues, including being aware of the potential for serious child protection concerns. They will have a leading role in establishing and reviewing the school online safety policies and documents. They will promote an awareness of and commitment to online safety education by awareness raising across the school and beyond into the local community. The Headteacher will be the first point of contact with the governing body, especially during the initial phases of this role for the governing body.

The Deputy Headteacher will liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated. They will organise or provide training and advice for all stakeholders as required. The Deputy Headteacher will liaise with technical staff where needed to improve practice within the school, especially linked to checks and logs that the school holds.

The Designated Safeguarding lead will ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents. They will receive reports of online safety incidents and create a log of incidents to inform future online safety developments; these will be shared with the SLT to reported back to the relevant stakeholders, as per the role detailed in this policy. They will include Online Safety in the termly safeguarding report to governors.

The Subject Leaders will work with the Senior Leadership Team to look at ways incorporate the Online Safety Curriculum into the everyday teaching that takes place in the school, so that the safeguarding message is seamless and consistent throughout the school; they will ensure that the curriculum taught is at an age and stage appropriate level for all learners.

School staff, including key workers and class teachers/room leads, are responsible for ensuring that they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices. They should understand that online safety is a core part of safeguarding and ensure they read relevant policies and documents linked to this policy. They should ensure they have read and understand how online safety issues are embedded in all aspects of the curriculum and other activities; they must supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices. Where lessons require internet use in pre-planned, children should be guided to use sites checked as suitable for use.

All school staff must immediately report any suspected misuse or problem to the DSL for investigation, in line with the school safeguarding procedures. They should also ensure that all digital communications with children and parents/carers should be on a professional level and only carried out using official school systems. All staff must have a zero-tolerance approach to incidents of online safety issues, as we do with all aspects of safeguarding. All staff should ensure they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

The ICT technician and Local Authority is responsible for ensuring that they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy. They should also ensure that the school technical infrastructure is secure and is not open to misuse or malicious attack. They will support the school to help them to meet the required online safety technical requirements as identified by the local authority. The ICT Technician should ensure there is clear, safe, and managed control of user access to networks and devices. They will keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant. With the support of the DSL and the SLT in the school, they will monitor the use of technology is regularly in order that any misuse or attempted misuse can be reported for investigation and action. The Local Authority will ensure the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.

Reporting and Responding to Concerns

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community will be made aware of the need to report online safety issues or incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Headteacher, Deputy Headteacher and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm the incident must be escalated through the agreed school safeguarding procedures.
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors
- where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure
    - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
    - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
    - once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
        - internal response or discipline procedures
        - involvement by local authority
        - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged using the form attached to this policy and handed to the DSL as soon as practicably possible
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)

- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    - staff, through regular briefings
    - learners, through lessons
    - parents/carers, through the Parentmail, school social media, website
    - governors, through regular safeguarding updates
    - local authority/external agencies, as relevant

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.

Online Safety Curriculum

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways.

The school has a planned online safety curriculum for all year groups matched against a nationally agreed framework. We use the Education for a Connected Work Framework by UKCIS/DCMS. Subject leaders, class teachers and room leads ensure:

- Lessons are matched to need; are age-related and build on prior learning.
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes, that support children to think about online safety both in school and at home
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language, at a level that is right for their stage of development.
- where children use the internet, they will use child friendly/age-appropriate search engines

Filtering and Monitoring

The school filtering policies are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents or behaviours. The school manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre appropriate filtering. Access to online content and services is managed for all users and the school receives updates and alerts from a SENSO package purchased by the school.

The school has established and effective routes for users to report inappropriate content, with a clear process in place to deal with requests for filtering changes. Filtering logs are regularly reviewed and alert the school to breaches of the filtering policy, which are then acted upon.

Where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice. Access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

The school monitors all network use across all its devices and services. An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored. There is a staff lead responsible for managing the monitoring strategy and processes.

There are effective protocols in place to report abuse or misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with safeguarding policy and practice. Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

The school follows the UK Safer Internet Centre appropriate monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies strategy informed by the school's risk assessment. These may include:

- physical monitoring (adult supervision in the classroom)
- internet use is regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- where possible, school technical staff regularly monitor and record the activity of users on the school technical systems

Technical Security

The school technical systems are managed in ways that ensure that the school meets recommended technical requirements. There are regular reviews and audits of the safety and security of school technical systems completed by the ICT Technician. The school ensures servers, wireless systems and cabling are securely located and physical access restricted. There are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies in the cloud.

The school ensures all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the ICT Technician, who will report these to SLT termly. All Staff have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security. All school networks and system are protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password by the ICT Technician, who will keep an up-to-date record of users and their usernames.

The Headteacher is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied, with the support of the ICT Technician. Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint (anti-virus) software.

Mobile Technologies

Mobile technology devices may be school owned or personally owned and might include smartphone, tablet, wearable devices, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school learning platform and other cloud-based services such as e-mail and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. The school's mobile technologies policy includes procedures and expectations linked to, but not limited to, safeguarding, behaviour, anti-bullying, acceptable use, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's online safety education programme.

The school acceptable use agreements for staff, learners, parents, and carers outline the expectations around the use of mobile technologies.

Staff should read and understand the mobile technology policy to confirm expected use in school.

Social Media

With widespread use of social media for professional and personal purposes requires clear guidance for staff to manage risk and behaviour online. Core messages should include the protection of learners, the school and the individual when publishing any material online.

Expectations for teachers' professional conduct are set out in the DfE Teachers Standards but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

All schools and local authorities have a duty of care to provide a safe learning environment for learners and staff.

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

- ensuring that personal information is not published
- 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, procedures and sanctions
- risk assessment, including legal risk
- guidance for children that is age and stage appropriate
- guidance for parents or carers

School staff should ensure that:

- no reference should be made in social media to children(past or present), 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 minimise risk of loss of personal information
- they act as positive role models in their use of social media

When official school social media accounts are established, there should be:

- a process for approval by senior leaders
- clear processes for the administration, moderation, and monitoring
- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with

Personal use
Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy; personal communications which do not refer to or impact upon the school are outside the scope of this policy.

The school permits reasonable and appropriate access to personal social media sites during school hours, where the member of staff is on their break and using their own device. Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

Monitoring
As part of active social media engagement, the school may, at times, pro-actively monitor the Internet for public postings about the school. The school will effectively respond to social media comments made by others according to an agreed communication by a member of the Senior Leadership Team. When parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers will 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 learners 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. Although this may not appear an issue with the children in our school being so young, 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 all users about these risks and will implement procedures to reduce the likelihood of the potential for harm.

The school may use live-streaming or video-conferencing services, to support online learning, similar to the live lessons taught in COVID-19. We will make sure that our procedures for this are in line with national and local safeguarding policies and that clear procedures are shared with all stakeholders prior to events being arranged.

When using digital images, staff will educate learners about the risks associated with the taking, use, sharing, publication and distribution of images. We will teach the children about consent and will not share digital images without consent. Where a digital image has more than child in it, this will not be shared with either party.

Staff and volunteers are aware of those learners whose images must not be taken or published. All digital images should only be taken on school devices, unless authorised by the most senior member of staff; where personal devices are authorised for a particular reasons, images are deleted immediately after use and the device is checked by a member of SLT.

Where digital images are used on the school website, permission is requested from parents prior to upload. Learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Parents and carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy and the privacy notice.

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-facing website
- Social media
- Online newsletters
- Parentmail Email and Texting System

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 young people, publication of school calendars and personal information – ensuring that there is less risk to members of the school community, through such publications.

Where children's work, images or videos are published, their identities are protected, and full names are not published.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.
The school:

- has a Data Protection Policy
- implements the data protection principles and can demonstrate that it does so
- has paid the appropriate fee to the Information Commissioner's Office (ICO)
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest.
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule" supports this
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- has clear and understood policies and routines for the deletion and disposal of data
- has a Freedom of Information Policy which sets out how it will deal with FOI requests
- provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff

When personal data is stored on any mobile device or removable media the device will be password protected. Where possible, devices will have up to date antivirus software. Data will be securely deleted from the devices, in line with this policy once its use is complete.

Monitoring and Reviewing of the Policy

The impact of the Online Safety Policy and practice is regularly evaluated through the review of online safety incident logs; behaviour reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.