****Parkview Nursery School**

**Online Safety and Acceptable Use Policy**

Initial policy September 2023 (updated September 2024)

**Section 1**

**Acceptable Use**

**Acceptable use**:

All members of the school community should use any school devices or accounts appropriately. For staff, acceptable use forms part of professional standards and is part of their contract. All new members of staff will be given resources to access accounts and informed of expectations for acceptable use.

**Browsing and searching**

With regards to the age of our children, it is probable that any misuse of browsing and searching in school would be accidental. During the year, we look at topics such as certificates on films and games, as well as who to tell if you have seen something that frightens you.

The following protocols should be adopted in school:

Teachers should not encourage the children to use search engines to seek out information on unsupervised.

All websites the children use will be accessed using the children’s computers or the class user on the school laptop. These are filtered using schools ICT and Optech filtering systems. This helps to prevent unauthorised searching resulting in inappropriate.

All websites used in school should be researched and checked each time they are used.

**File management – staff.**

All staff are provided with file storage, accessible with an internet connection, both in school and remotely.

Staff are encouraged to manage their personal filing system to ensure ease of access of their files.

Staff have access to and are encouraged to use shared drives within the school’s domain. They should collaborate with other staff to ensure they are managed and organised, informing colleagues of any major changes to the file organisation system.

The file storage system should be used exclusively for work purposes.

**Use of YouTube**

Staff can use YouTube as an aid to enhance teaching and learning.

All media used should be thoroughly checked and watched for the entire length of clips.

Children are not permitted to search YouTube for videos of their own choice and staff should both remind the children of this and check to ensure misuse in school is not taking place through supervised access in the classroom.

**Bring Your Own Device (BYOD) Policy**

Visitors to the school requesting access to the school’s internet may do so with approval from a member of the core staff team (comprising the head teacher, office staff and the teacher in charge). This will purely allow access to the school’s Wi-Fi and will in no way give access to the school’s shared drive. Requests to use external memory storage devices on a school device will normally not be accepted but may be sanctioned by the HT/DSL in exceptional circumstances.

**As with all safeguarding, it is every member of staff’s responsibility to keep themselves, their colleagues, and the children safe, when working online.**

**Section 2**

**Online Safety**

Online Safety Policy for Parkview Nursery School

Parkview Nursery School is committed to creating a safe and secure digital environment for all pupils, staff, and visitors. This policy outlines the school's approach to online safety and is written in line with the requirements of the Department for Education’s Keeping Children Safe in Education guidelines, especially its references to monitoring and filtering digital technologies to ensure responsible and appropriate use.

**Aims and Objectives of this policy:**

To protect pupils from exposure to harmful or inappropriate online content.

To ensure compliance with legal requirements and relevant standards regarding digital and technology use in schools, specifically within the Keeping Children Safe in Education guidelines (https://www.gov.uk/government/publications/keeping-children-safe-in-education--2) and the Department of Education’s Meeting Digital and Technology Standards in Schools and Colleges (https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges).

To promote responsible internet use and digital citizenship among pupils and staff.

To maintain a secure network infrastructure and protect against potential threats or unauthorized access.

To provide support and guidance for users in navigating digital technologies safely and effectively.

Monitoring and filtering systems, roles and responsibilities are detailed in appendix 1.

**Identifying and assigning roles and responsibilities to manage filtering and monitoring systems**

The Governing Board has overall strategic responsibility for filtering and monitoring and needs assurance that the standards are being met.

To fulfil this, the following is in place:

Member of the senior leadership team and governor, to be responsible for ensuring these standards are met:

Rhiannon Hughes, Head Teacher

Diane O’Brien, Safeguarding Governor

**Roles and responsibilities of staff and third parties, for example, external service providers:**

The teaching team are responsible for:

* procuring filtering and monitoring systems
* documenting decisions on what is blocked or allowed and why.
* reviewing the effectiveness of our provision
* overseeing reports

They are also responsible for making sure that all staff:

• understand their role

* are appropriately trained.

• follow policies, processes, and procedures

• act on reports and concerns

The Head Teacher works closely with governors and is the designated safeguarding lead (DSL) and our external IT service providers in all aspects of filtering and monitoring.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective.

The HT/DSL works closely together with IT service providers to meet the needs of our setting.

The HT/DSL takes lead responsibility for safeguarding and online safety, in the following areas:

• filtering and monitoring reports

• safeguarding concerns

• checks to filtering and monitoring systems

The HT/IT service provider has technical responsibility for:

• maintaining filtering and monitoring systems

• providing filtering and monitoring reports

• completing actions following concerns or checks to systems

The HT and IT service provider work to:

• procure systems

• identify risk

• conduct reviews

• conduct checks

**Review of filtering and monitoring provision**

For filtering and monitoring to be effective it should meet the needs of pupils and staff and reflect specific use of technology while minimising potential harms.

To understand and evaluate the changing needs and potential risks of our school, the filtering and monitoring provision is reviewed at least annually.

Additional checks to filtering and monitoring are informed by the review process so that the governing body has assurance that systems are working effectively and meeting safeguarding obligations.

**Meeting the standard**

Governing bodies and proprietors have overall strategic responsibility for meeting this standard. They should make sure that filtering and monitoring provision is reviewed, which can be part of a wider online safety review, at least annually.

The head teacher/DSL and the IT service provider conduct the review where necessary, and the responsible governor is informed/involved, as necessary. The results of the online safety review are recorded for reference and made available to those entitled to inspect that information.

**Technical requirements:**

A review of filtering and monitoring is conducted to identify current provision, any gaps, and the specific needs of our pupils and staff.

This includes:

• the risk profile of your pupils, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)

• what our filtering system currently blocks or allows and why

• any outside safeguarding influences, such as county lines

• any relevant safeguarding reports

• the digital resilience of our pupils

• the related safeguarding or technology policies we have in place

• the checks that are currently taking place and how resulting actions are managed

To make our filtering and monitoring provision effective, our review informs:

• related safeguarding or technology policies and procedures

• roles and responsibilities

• training of staff

• curriculum and learning opportunities

• procurement decisions

• how often and what is checked

• monitoring strategies

The review is done annually, or when:

• a safeguarding risk is identified

• there is a change in working practice, like remote access

• recent technology is introduced

When checking filtering and monitoring systems we will make sure that the system setup has not changed or been deactivated. The checks will include a range of:

• school owned devices and services, including those used off site

• user groups, for example, teachers, pupils, and guests

A log of checks will be kept so they can be reviewed. We will record:

• when the checks took place

• who did the check

• what they tested or checked

• resulting actions

The HT/DSL will make sure that:

• all staff know how to report and record concerns

• filtering and monitoring systems work on new devices and services before releasing them to staff and pupils

**Blocking harmful and inappropriate content, without unreasonably impacting teaching and learning.**

An active and managed filtering system is an important part of providing a safe environment for pupils to learn.

No filtering system can be 100% effective. We understand the coverage of our filtering system, any limitations it has, and mitigate accordingly to minimise harm and meet our statutory requirements in Keeping children safe in education (KCSIE) and the Prevent duty.

Our filtering system blocks internet access to harmful sites and inappropriate content. It does not:

• unreasonably impact teaching and learning or school administration

**Technical requirements to meet the standard:**

Our filtering system is operational, up to date and applied to all:

• users, including guest accounts

• school owned devices

• devices using the school broadband connection

Our filtering system:

• filters all internet feeds, including any backup connections

• is age and ability appropriate for the users, and is suitable for our setting

• manages multilingual web content, images, common misspellings, and abbreviations

• identifies technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them

• provides alerts when any web content has been blocked

Mobile and app content is often presented in a different way to web browser content. If your users access content in this way, you should get confirmation from your provider as to whether they can provide filtering on mobile or app technologies. A technical monitoring system should be applied to devices using mobile or app content to reduce the risk of harm. On guidance from Hudson Hill Consulting when the children are using the iPad in the classroom it is important that staff ensure the use of guided access so that no filtering settings can be tampered with accidentally.

The HT/DSL enforces Safe Search, or a child friendly search engine or tools, to provide an additional level of protection for our users on top of the filtering service.

All staff are aware of reporting mechanisms for safeguarding and technical concerns. They should report if:

• they witness or suspect unsuitable material has been accessed

• they can access unsuitable material

• they are teaching topics which could create unusual activity on the filtering logs

• there is failure in the software or abuse of the system

• there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks

• they notice abbreviations or misspellings that allow access to restricted material

**The school has effective monitoring strategies that meet the safeguarding needs of the school.**

The importance of meeting the standard

Monitoring user activity on school devices is an important part of providing a safe environment for children and staff. Unlike filtering, it does not stop users from accessing material through internet searches or software.

Monitoring allows the school to review user activity on our devices. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing us to take prompt action and record the outcome.

Our monitoring strategy is informed by the filtering and monitoring review. A variety of monitoring strategies are required to minimise safeguarding risks on internet connected devices and include:

• physically monitoring by staff watching screens of users

• network monitoring using log files of internet traffic and web access

• individual device monitoring through software or third-party services

See Appendix 1 below for further detail on this.

Meeting the standard:

The governing board supports the teaching team to make sure effective device monitoring is in place which meets this standard and the risk profile of the school.

The HT/DSL takes lead responsibility for any safeguarding and child protection matters that are picked up through monitoring. The management of technical monitoring systems require the specialist knowledge of both safeguarding and IT staff to be effective.

Technical requirements and how the school meets the standard:

The governing board support the teaching team to review the effectiveness of our monitoring strategies and reporting process. We will always make sure that incidents are urgently picked up, acted on and outcomes are recorded. Incidents could be of a malicious, technical, or safeguarding nature. It is clear to all staff how to deal with these incidents and who should lead on any actions.

The HT/DSL and external third-party providers manage device monitoring, they:

• make sure monitoring systems are working as expected

• receive safeguarding training including online safety

• record and report safeguarding concerns to the DSL

They also make sure that:

• monitoring data is received in a format that staff can understand

• users are identifiable to the school, so concerns can be traced back to an individual, including guest accounts

In the online safety section of Keeping children safe in education there is guidance on the four areas of risk that users may experience when online.

Our monitoring provision identifies and alerts the HT/DSL to behaviours associated with them:

**content**: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

**contact**: being subjected to harmful online interaction with other users; for example: 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.

**conduct**: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending, and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.

**commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial frauds. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

The school acknowledges that technical monitoring systems do not stop unsafe activities on a device or online. Staff should:

• provide effective supervision

• take steps to maintain awareness of how devices are being used by pupils

• report any safeguarding concerns to the DSL

School monitoring procedures are reflected in our Acceptable Use Policy and integrated into relevant online safety, safeguarding and

organisational policies, such as privacy notices.

**Appendix 1**

**Core school responsibilities for Monitoring and Filtering:**

Head Teacher: Rhiannon Hughes

Designated Safeguarding Lead: Rhiannon Hughes

Named person responsible for Monitoring and Filtering: Rhiannon Hughes

School IT Support: Managed internally, in conjunction with Hudson Hill Consulting Ltd

Monitoring systems:

• physically monitoring by staff watching screens of users:

• comprehensive training is given to all staff to ensure that they can do this and are aware their responsibilities

• live supervision by staff on a console with device management software

• Our Google Classroom learning platform allows us to monitor use of all Google apps, whilst also physically monitoring activity

• network monitoring using log files of internet traffic and web access

• We subscribe to Securely.com whose filtering, blocking and keyword search alert system conforms to these requirements

• individual device monitoring through software or third-party services

• The Securely.com system allows for individual device and user monitoring for all school accounts and devices both on and off site

Systems and Checks for Filtering and Monitoring:

Three, termly compliance days in place to monitor IT usage:

Rhiannon Hughes

APPROVED By:

Name:

**Date: 16th September 2024**  **Review Date: September 2025**