Filtering & Monitoring Policy

Falconer's Hill Infant School

Approved by:	Rachel
Last reviewed on:	September 2024

Filtering & Monitoring Policy

Mission Statement

'We learn, we love, we laugh together'

1. Purpose and Scope

1.1. This policy outlines the guidelines and procedures for filtering and monitoring internet usage within FHIS School. This policy applies to all pupils, staff, volunteers, visitors, and any other individuals accessing the internet through FHIS's network.

2. Roles and responsibilities

2.1. The role of the Governors

2.1.1. A named member of the governing body will be responsible for overseeing the implementation and effectiveness of the school's Filtering and Monitoring Policy. This includes regularly reviewing its efficiency, ensuring compliance with legal guidelines, and collaborating with IT staff and service providers to balance safeguarding measures with educational objectives. The governing body will also play a key role in reviewing the policy annually and assessing the proportionality of costs versus safeguarding risks.

2.2. The role of the Designated & Deputy Designated Safeguarding Leads

2.2.1. The Designated and Deputy Designated Safeguarding Leads will be responsible for the day-to-day management of the school's Filtering and Monitoring Policy. This includes liaising with IT staff to ensure the appropriate filters and monitoring systems are in place, reviewing incident reports, and escalating concerns. They will also work closely with teaching staff to provide training and awareness programs related to responsible internet usage and online safety, ensuring a cohesive approach to safeguarding across the school environment.

2.3. The role of the Computing Co-ordinator

2.3.1. The Computing Coordinator is responsible for implementing and maintaining the school's Filtering and Monitoring Policy. They will liaise with ICT technicians or contractors for technical setup and troubleshooting. The Coordinator will also provide reports on policy effectiveness to Designated Safeguarding Leads and the governing body, while ensuring the systems align with educational objectives.

2.4. The role of the ICT Technicians/Contracters

2.4.1. ICT technicians or contractors are responsible for the technical setup and maintenance of the school's Filtering and Monitoring systems, in line with the policy guidelines. They collaborate with the Computing Coordinator to resolve technical issues and ensure the systems are up-to-date and effective.

2.5. The role of the class teacher

2.5.1. Class teachers are responsible for actively monitoring pupils' internet usage during lessons to ensure compliance with the Filtering and Monitoring Policy. They are also tasked with reporting any incidents of inappropriate use or content to the Designated Safeguarding Leads for further action.

3. Filtering Guidelines

3.1. Website Content Filtering:

3.1.1. FHIS will implement content filtering solutions to restrict access to websites containing illegal, inappropriate, or harmful content.
3.1.2. Content filtering will be based on predefined categories such as adult content, violence, hate speech, drugs, gambling, etc. Regular maintenance and updates of these categories will be performed to ensure effectiveness.
3.1.3. Attempts to bypass content filtering measures are strictly prohibited and may result in disciplinary actions.

3.2. Software and Application Filtering:

3.2.1. FHIS will implement software and application filtering to prevent the installation or use of unauthorised or potentially harmful software or applications.
3.2.2. Filtering will be based on a list of authorised software and applications that align with FHIS's educational objectives and security policies.
3.2.3. Attempts to install or use unauthorized software or applications are strictly prohibited and may result in disciplinary actions.

3.3. Social Media and Communication Filtering:

3.3.1. FHIS will implement filtering measures for social media platforms and communication channels to ensure appropriate use.

3.3.2. Access to social media websites and communication channels may be restricted during school hours to minimize distractions and maintain a focused learning environment.

3.3.3. Any communication that violates FHIS acceptable use policy, promotes discrimination, harassment, or involves illegal activities will be strictly prohibited.

4. Monitoring Guidelines

4.1. Network Traffic Monitoring:

4.1.1. FHIS reserves the right to monitor network traffic, including internet usage, to ensure compliance with this policy.

4.1.2. Network traffic monitoring will be performed using appropriate tools and technologies. The collected data will be used confidentially and for authorised purposes only.

4.1.3. Any suspicious or unauthorized network activity may be subject to investigation, and appropriate actions will be taken if policy violations are detected.

4.2. User Activity Monitoring:

4.2.1. FHIS may monitor user activity on school-owneddevices or devices connected to FHIS's network.

4.2.2. User activity monitoring may include but is not limited to tracking websites visited, application usage, and communication content.

4.2.3. User privacy will be respected, and monitoring will be conducted in accordance with relevant data protection laws and regulations.

5. Reporting and Consequences

5.1. Any individual who suspects a policy violation or encounters inappropriate content should report it immediately to a teacher, designated or deputy designated safeguarding lead and/or designated governor.

5.2. Violations of the filtering and monitoring policy may result in disciplinary actions, including but not limited to warnings, restricted access to network resources, or other appropriate consequences, depending on the severity and frequency of the violation.

5.3. Any issues or concerns related to the execution of the filtering and monitoring policy should be promptly brought to the attention of the Designated and Deputy Designated Safeguarding Leads and the Computing Coordinator. ICT technicians or contractors should be informed of any such issues without delay.

6. Education and Awareness

6.1. FHIS will provide regular education and awareness programs to pupils, staff, and parents/guardians to promote responsible internet usage and online safety.

6.2. Users will receive guidance on understanding and adhering to this policy, as well as resources to help them navigate the digital world safely and responsibly.

7. Policy Review

7.1. This filtering and monitoring policy will be reviewed annually to ensure its alignment with relevant laws, regulations, and best practices. Any necessary updates will be made to enhance its effectiveness and address emerging trends or challenges.

8. Data Protection Statement

8.1. The procedures and practice created by this policy have been reviewed in the light of our Data Protection Policy.

8.2. All data will be handled in accordance with the school's Data Protection Policy.

Data Audit For This Policy					
What ?	**Probable Content**	**Why ?**	**Who ?**	**Where ?**	**When ?**
Child's Name Child's data	Name data	Log-in Information Record assessments	All Staff (Where Necessary) Parents Children	Kept in children's file or shredded.	Kept in children's file or sent home.

8.3. As such, our assessment is that this policy :

Has Few / No Data Compliance Requirements	**Has A Moderate Level of Data Compliance Requirements**	**Has a High Level Of Data Compliance Requirements**
		☐