Filtering and Monitoring Policy

Inspire ● Enrich ● Enjoy ● Succeed

'Let your light shine before others, that they may see your good deeds and glorify your Father in Heaven.'
Matthew, 5:16

We **inspire** a love of learning, confidence and resilience; to strive to shine before God and others.
Our unique curriculum **enriches** well-being, learning attitudes, and the ability to fulfil potential; **enjoying** a life according to God's teaching.
We are a Christian family, celebrating faith, individuality and diversity, giving the opportunity to **succeed**.

Approved by:	Governing Body	**Date:**	January 2024
Next review due by:	January 2025		

Our Federation's Christian Vision and Values, 'Valuing All God's Children' document (Church of England) and KCSiE 2023 informed the consultation for and adoption of this policy.

Compassion ● Forgiveness ● Hope ● Justice ● Respect ● Honesty ● Love

1 Policy Statement

The Federation of Snape Community & Thornton Watlass CE Primary School (STW) is committed to ensuring that our children are effectively safeguarded at all times. Safeguarding and child protection must always be the highest priority and at the forefront of everything we do.

The potential risks from online use are extensive and ever evolving, but can be categorised into four areas:

- being exposed to illegal, inappropriate or harmful material;
- being subjected to harmful online interaction with other users;
- personal online behaviour that increases the likelihood of, or causes, harm;
- risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

It is essential that all of the children we educate and care for are safeguarded from potentially harmful and inappropriate online material. An effective approach to online safety empowers our federation of schools to protect and educate the federation community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate. All staff are expected to take this responsibility seriously and we have adopted a 'whole-federation' approach to online safety (refer to Online Safety Policy).

This policy focuses specifically on the web filtering and monitoring in place within our federation to protect children and young people. It must be read in addition to the federation's:

- Online Safety Policy;
- Acceptable Use Policy;
- Camera and Mobile Phone Policy;
- Child Protection Policy;
- Child Protection Manual;
- Prevent Policy.

This policy is written in line with the relevant legislation, regulations and government guidance, including:

Keeping Children Safe in Education (KCSiE) 2023, DfE

Meeting digital and technology standards in schools and colleges (DfE)

UK Safer Internet Centre Online Safety Policy

Prevent Duty Guidance (HM Government)

It will be reviewed annually or whenever significant changes are made to national policy and legislation.

2 Roles and Responsibilities

2.1 Governors

- The governing body will monitor the effectiveness of this policy and hold the EHT/ Designated Safeguarding Lead to account for its implementation. They should be doing all that they reasonably can to limit children's exposure to risks online risks through the federation's IT system.

- The DfE's filtering and monitoring standards requires schools to:
    - 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.
    - have effective monitoring strategies in place that meet their safeguarding needs
    - review the standards and discuss with IT service providers what more needs to be done to support school in meeting this standard.
- Consider meeting the Cyber security standards for schools and colleges. Broader guidance on cyber security Cyber security training for school staff - NCSC.GOV.UK.

2.2 Designated Safeguarding Lead (DSL)

- The DSL should take lead responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place. This should be explicit in the role-holder's job description;
- The DSL should ensure, with the support of NYES Digital (North Yorkshire IT), that the schools within the federation have appropriate filters and monitoring systems in place, that are informed in part by the risk assessment required by the Prevent Duty, and regularly review their effectiveness;
- The DSL will work closely together with NYES Digital to meet the needs of the schools and request system specific training and support as and when required. They will take lead responsibility for any safeguarding and child protection matters that are picked up through web filtering and monitoring systems in place;
- The DSL should ensure that all staff undertake safeguarding and child protection training, (including online safety which includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring) at induction; this training should be updated on an annual basis;
- The DSL should consider the age, development range of the children and their needs, how often they access the IT system and the proportionality of costs versus safeguarding risks;
- The DSL receives daily reports of sites that have been blocked following attempted access. It is the DSL's responsibility to ensure they are receiving them. NYES Digital must be informed if daily updates are not received. It is also the responsibility of the DSL to inform NYES Digital of any changes or updates to these contacts;
- The DSL will investigate attempted access of inappropriate sites (breaches) as soon as possible and take appropriate action. Attempted access of websites related to extremism will be referred appropriately in line with the Prevent Duty and local arrangements for reporting.
- The DSL is responsible for recording any breaches including the nature and the outcome. Data relating to breaches is reported within the 1st of the Month Checks and monitored by governors.

2.3 All Staff

- All staff are required to adhere to the Federation of STW's internal procedures relating to safeguarding and child protection and managing allegations as well as the Local Safeguarding Partnership's procedures;
- Staff are required to support the DSL in investigating breaches as appropriate.

Staff, volunteers, contractors and visitors must not, under any circumstances, allow a child or young person to use their device, online account or hotspot or share any of their login details or passwords. This is for the safety and protection of the child and the staff member/ adult.

3 Filtering and Monitoring System

NYES Digital operates a highly secure web filtering system on the internet link to both schools within the federation (Snape & Thornton Watlass) via Smoothwall's Universal Threat Management (UTM) system. This means that it safeguards the computers and internet use within the federation, and it also offers safeguards on every mobile phone and tablet used in the setting over the setting's Wi-Fi network. Web filtering and monitoring helps to keep young people safe from illegal content and help protect them from extremism online when using the setting's Wi-Fi, it is informed in part, by the risk assessment required by the Prevent Duty.

All users should understand that the primary purpose of the use of the internet in a school context is educational. The web site categories that are blocked are to ensure the safety and well-being of children.

The web filtering system does not safeguard the use of a mobile phone or tablet that is accessing the internet over mobile phone signals. Children are only permitted to use school devices linked to the school's Wi-fi; use over mobile phone signals is not permitted under any circumstances.

Children, parents/ carers and staff are required to sign an IT user agreement on an annual basis.

The daily Smoothwall reports, and any instant notifications, of blocked sites received by the DSL are investigated immediately.

The breach is recorded and records include the date, nature/ category of breach, the website address and device IP address accessed from. In addition, the findings including any necessary actions/ reporting are recorded.

Notifications will be stored by the setting for a period of six months unless there are safeguarding concerns. If there are safeguarding concerns the information will be stored in line with statutory requirements for record retention.

Breaches of this Filtering and Monitoring Policy by staff will be considered a possible disciplinary offence (in line with the Staff Conduct Policy and Staff Acceptable Use Agreement).

4 Meeting the Filtering and Monitoring Standards for Schools

The following documents have been made available to support schools to meet the DfE Filtering and monitoring standards for schools and colleges:

- A questionnaire/spreadsheet to help work through the standards to assess compliance;
- Annual School Online Safety Audit & Risk Assessment template;
- A web filtering overview is provided in the KCSiE 2023; the DSL is expected to complete appropriate training, i.e. Filtering and Monitoring: Developing Systems to Keep Children Safe Online, Primary (National College).