INTERNET FILTERING POLICY

DATE CREATED	September 2023	**DATE OF NEXT REVIEW**	September 2025
POLICY OWNER(S)	Head of IT		
DESIGNATION	All Staff		

Purpose of policy	The purpose of the Internet Filtering Policy is to ensure the appropriate, responsible and safe use of the internet within St Elizabeth's Centre and to protect the organisation's network, users and clients from potential, security threats, legal liabilities, and offensive or inappropriate content. This policy outlines the guidelines for filtering internet content accessible through the organisation's network.
Intended audience	This policy applies to all employees, contractors, consultants, clients and any other personnel who have access to St Elizabeth's internet services. The same policy applies to the use of internet access on personal devices, which are added to our Client network using the same authentication process.
Links to other policies	Keeping children safe in education 2023 (publishing.service.gov.uk)

Internet Content Filtering Mechanism

St Elizabeth's Centre will implement and maintain an internet content filtering mechanism to restrict access to certain websites and content categories based on predefined filtering rules. The filtering mechanism may use a combination of hardware, software, and third-party services to ensure the effectiveness of filtering.

This policy takes full account of Keeping Children Safe in Education September 2023 (KCSIE), Keeping children safe in education 2023 (publishing.service.gov.uk)

1. Blocked Content Categories

The following categories of internet content will be blocked or restricted from access by default:

a) Adult Content: Any sexually explicit or pornographic material.
b) Illegal Activities: Websites promoting or facilitating illegal activities, including but not limited to hacking, piracy, and illegal drug use.
c) Terrorism (PREVENT Duty), Discrimination and Hate Speech: Content promoting terrorism, hatred, discrimination, or violence against individuals or groups based on race, ethnicity, religion, gender, sexual orientation, or disability.
d) Malicious Content: Websites known to host malware, viruses, or other harmful software.
e) Phishing and Fraud: Websites attempting to deceive users or engage in fraudulent activities.
f) Social Engineering: Content designed to manipulate users into revealing sensitive information.
g) Gambling: Websites related to online gambling or betting.
h) Excessive Bandwidth Consumption: Websites that consume significant bandwidth and may impact network performance.
i) Other Inappropriate Content: Any content deemed inappropriate or harmful to the organisation's reputation and values.

2. User Responsibility

a) Acceptable Use: Users are expected to use the internet responsibly – please see Communications, Email and Internet Security Policy.
b) Reporting: Users must report any websites that they believe are wrongly categorised or believe should be blocked to the IT department.
c) Bypass Attempts: Users are strictly prohibited from attempting to bypass or disable the internet content filtering mechanism. Any such attempts may result in disciplinary action.

3. Review and Updates

The internet filtering policy will be reviewed periodically by the Head of IT to ensure its effectiveness and relevance. Updates to the policy will be made as necessary to adapt to changing internet usage trends and emerging threats and in accordance with statutory guidance.

4. Non-Compliance

Failure to comply with this Internet Filtering Policy may result in disciplinary action, up to and including termination of employment or other appropriate consequences, as determined by St Elizabeth's management team.

5. Legal Considerations

St Elizabeth’s Centre will ensure that its internet filtering practices comply with all applicable laws and regulations regarding internet usage and data privacy. The organisation will also respect the rights of users while maintaining a safe and secure online environment.