Issue Date: November 2024

Review Date: November 2025

Lead Officer: Sarah Spargo

Filtering and Monitoring Statement for TOAST at CN4C

Introduction

At CN4C, safeguarding children and young people is at the heart of our ethos. As part of our commitment to providing a safe and secure online environment, we have implemented robust filtering and monitoring systems, in line with the statutory guidance outlined in *Keeping Children Safe in Education (KCSIE) 2024*. Our approach ensures that all children and young people, including those accessing online services through the TOAST initiative, are protected from harmful online content while fostering a productive learning environment.

Objectives

The primary objectives of our filtering and monitoring strategy are to:

- Safeguard children and young people from exposure to harmful or inappropriate content, including but not limited to, extremist materials, online abuse, and other threats to their wellbeing.

- Promote responsible and informed use of online resources.

- Provide transparency and clarity about the tools and processes in place.

- Ensure compliance with KCSIE 2024 requirements.

Filtering Systems

Our filtering system is designed to block access to content that is illegal, inappropriate, or harmful, including:

- Extremist or radicalisation materials.

- Pornographic or violent content.

- Sites promoting self-harm, suicide, or eating disorders.

- Platforms encouraging online abuse or cyberbullying.

- Malicious websites or phishing attempts.

The filtering solution used across CN4C internet access is regularly updated to adapt to emerging threats and ensure that safeguards remain effective. Age-appropriate controls are applied to allow students access to the resources they need for learning without compromising their safety.

Monitoring Systems

CN4C employs active monitoring tools to detect and flag potentially harmful activity or behaviours online. These tools include:

- Real-time alerts for flagged searches or interactions indicating risk (e.g., signs of self-harm or bullying).

- Regular reviews of usage logs for patterns that may indicate safeguarding concerns.

- Anomalous activity detection, such as attempts to bypass filtering systems or access restricted content.

Monitoring activities are conducted in a way that respects students' privacy while prioritising their safety. All monitoring practices are proportionate, transparent, and compliant with relevant data protection regulations.

Roles and Responsibilities

- **Designated Safeguarding Lead (DSL):** Oversees the implementation of filtering and monitoring policies and reviews flagged incidents.

- **IT Team:** Ensures that filtering and monitoring systems are operational, effective, and up to date.

- **Staff:** Remain vigilant and report any concerns arising from flagged activities or unusual online behaviour.

- **Parents and Carers:** Encouraged to engage with CN4C's e-safety initiatives and support safe online practices at home.

Incident Response

Any safeguarding concerns identified through filtering or monitoring systems are escalated promptly in accordance with CN4C's safeguarding policy. This includes:

- Immediate review by the DSL.

- Communication with relevant parties, including parents, if appropriate.

- Referral to external agencies where necessary.

Review and Updates

Issue Date: November 2024

Review Date: November 2025

Lead Officer: Sarah Spargo

This filtering and monitoring statement is reviewed annually or sooner if significant changes occur in technology, statutory guidance, or safeguarding priorities. Feedback from staff, students, and parents will inform any updates to ensure the policy remains effective and relevant.