

Date Approved	Approved by	Next review Date	Version
September 2023	Mohamed Yusuf Executive Director	September 2024	01

Online Safety Filtering and Monitoring Policy

Addendum to the Child Protection and Safeguarding Policy

Senior Leadership:	Alfred Grezaj	E: a.grezaj@oasiscareandtraining.org.uk	N: 020 7639 6192 (EXT 309)
Designated Safeguarding Lead:	Janet Edwards	E: JEdwards@oasiscareandtraining.org.uk	N: 0203 0072114
Somtech Support Services:	Abdirahman Ali	E: support@somtechs.com	N: 07961 474616

This policy is written in line with the following legislation and guidance:

Keeping children safe in education 2023 (publishing.service.gov.uk)

- [Keeping children safe in education 2023](#)
- [Meeting DIGITAL AND TECHNOLOGY STANDARDS IN SCHOOLS AND COLLEGES UPDATED March 2023.](#)
- [Appropriate Filtering and Monitoring - UK Safer Internet Centre](#)

Contents

1. Introduction
2. Aims
3. Roles and responsibilities
4. Technologies in use
5. Links with other policies
6. Review

1. Introduction

In compliance with the Department for Education's statutory guidance on 'Keeping Children Safe in Education 2023, schools and colleges in England are required to implement appropriate filters and monitoring systems to prevent access to harmful or inappropriate material through their IT systems. However, it is crucial for schools and colleges to ensure that these measures do not excessively restrict the educational content available to students online, particularly in the context of online teaching and safeguarding. While internet filtering has traditionally been a standard practice in schools and college, the emphasis has now shifted towards implementing strengthened measures

as a key aspect of Ofsted's assessment of online safety during inspections. It is essential to acknowledge that no filtering system can guarantee complete effectiveness and should be complemented by sound teaching practices and vigilant supervision.

2. Aims

The aims of Oasis Care and Training Agency (OCTA) are as follows:

- Promote the safe and responsible use of technology.
- Prevent unauthorised access to illegal content.
- Maintain the security and integrity of networks and devices.
- Enable appropriate access for IT management and support purposes.

3. Roles and responsibilities

DfE Filtering Standards requires OCTA to identify and assign roles and responsibilities to manage their filtering and monitoring systems, and include

Role	Responsibility	Name / Position
Responsible Governor	Strategic responsibility for filtering and monitoring and need assurance that the standards are being met.	Executive Director: Mohammed Yusuf
Senior Leadership	Team Member Responsible for ensuring these standards are met and: • procuring filtering and monitoring systems • documenting decisions on what is blocked or allowed and why • reviewing the effectiveness of your provision overseeing reports Ensure that all staff: • understand their role • are appropriately trained • follow policies, processes and procedures act on reports and concerns	Commercial Training Director Alfred Grezaj
Designated Safeguarding Lead	Lead responsibility for safeguarding and online safety, which could include overseeing and acting on:	Janet Edwards Programme Manager for Apprenticeships/DSL

	- filtering and monitoring reports - safeguarding concerns checks to filtering and monitoring systems	
IT Service Provider	Technical responsibility for: - maintaining filtering and monitoring systems - providing filtering and monitoring reports completing actions following concerns or checks to systems	Abdirahman IT Manager – Somtech Support Services
All staff need to be 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	

3. Technologies in use

Filtering:

Gateway Filtering:

- All network traffic from OASIS's devices undergoes gateway filtering. Rules for filtering are based on users, user groups, devices, and device groups, providing tailored access levels to ensure a safe browsing experience.
- Websites are restricted based on categorised content, adhering to relevant standards and recommendations.
- Uncategorised websites are blocked for apprentices, learners, guests, and staff.

DNS Filtering:

- OCTA's network traffic is subject to gateway filtering while operating on OASIS's networks. Standard rules are applied, covering inappropriate (e.g., adult content),

illegal, or malicious traffic for all users and devices, facilitated by Barracuda Networks

Device Filtering:

- Devices used by apprentices and learners have additional software installed for real-time filtering, possibly managed by Somtech Support Services.
- All devices are equipped with endpoint security software to filter and restrict access to potentially malicious or risky traffic or applications.
- Network filtering controls and rules are managed by Somtech Support Services in coordination with the Executive Team.
- Staff may request filtering exemptions with appropriate educational or business justifications by contacting Somtech Support Services.

Monitoring:

- Devices for learners and apprentices may have additional software installed for remote monitoring of exams and tests, keyboard input monitoring, immediate remote device control, or device lockout capabilities.
- Usage of monitoring software is restricted to designated staff as per Somtech Support Services' directives.
- All devices have management software enabling remote inventory, management, and support access and control by Somtech Support Services.
- Endpoint security software audits and tracks actions across devices, users, applications, and system services, automatically identifying security risks and threats.

Reporting:

- If a violation of filtering or monitoring rules concerning learners or apprentices is detected, the detecting system automatically alerts Somtech Support Service or their designated staff members.

4. Links with other policies

- This policy links to the following policies and procedures:
 - Staff Code of Conduct
 - Safeguarding and Child Protection Policy
 - Online Safety Policy

5. Review

This policy will be reviewed by the IT Manager (Somtech Support Services) annually.

There will be a review of filtering and monitoring conducted by the DSL which will cover:

- Related safeguarding or technology policies and procedures

- Roles and responsibilities
- Training of staff
- Curriculum and learning opportunities
- How often and what is checked
- Monitoring strategies
- This review should be conducted minimally annually, or when
- A safeguarding risk is identified
- There is a change in working practices, like remote access or the way in which personal devices access our network
- New technology is introduced

The annual review will inform updates to the Safeguarding policy which are reported and approved in Autumn 2024