Filtering and monitoring Policy

The Crescent Primary School

Approved by:	Governing Body- Resources	**Date:** 21/01/26	
Last reviewed on:	13/01/2026	**Responsibility:** Governors-resources	
Next review due by:	21/01/ 2028		

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for e-safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Key Personnel

Who will be responsible for creating and reviewing the policy – Head Teacher Who can provide technical expertise on Internet filtering – DRIFT IT

Responsibilities

The responsibility for the implementation of the school's filtering policy will be held by the DRIFT IT. They will manage the school filtering, in line with this policy and will keep records / logs of changes and breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:

- be logged in change control logs
- be reported to a second responsible person:
- report to a second responsible person every half term in the form of an audit of the change control logs
- report to the Safeguarding Governor every half term in the form of an audit of the change control logs

All users have a responsibility to report immediately to the Headteacher any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programs or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by Schools Broadband via Drift IT. The filtering & firewall system is FortiGate NGFW. Fortigate and Schools Broadband are members of the Internet Watch Foundation (IWF)

The following test was performed using South West Grid For Learning (SWGFL) online filtering test
Check Your Internet Connection Blocks Child Abuse & Terrorist Content (swgfl.org.uk)

Test Filtering

Filter Test Results

Tests were performed at 13/01/2026 09:31

Your Connection

Type
School

Organisation
The Crescent Primary School

Postcode
SO50 9DH

Location
Hampshire, England

Device
Windows, Edge 143.0.0.0

IP Address
149.71.109.140

Filtering Provider
NetSweeper / FortiGate (Schools Broadband)

Network
TALKSTRAIGHT

Results Overview

CSAM	Terrorism	Adult	Decryption
✓	✓	✓	⏻

Child Sexual Abuse Material

Blocked

Description
Tests whether you are blocking websites on the IWF Child Abuse Content URL list.

Results & Recommendations
It appears that your filtering solution includes the IWF URL Filter list, blocking access to Child Sexual Abuse content online

Terrorism Content

Blocked

Description
Tests whether you are blocking websites on the Counter-Terrorism Internet Referral Unit list (CTIRU).

Results & Recommendations
It appears that your filtering solution includes the Counter-Terrorism Internet Referral Unit (CTIRU) URL filter list, blocking access to unlawful terrorist content online

Adult Content

Blocked

Description
Test whether your Internet filter blocks access to pornography websites

Results & Recommendations
It appears that your filtering solution includes blocking for online pornography

Only designated technicians at Drift have access to the firewall and filtering system to ensure we can monitor change requests.

Illegal content is managed by Drift IT and filtered using the Fortigate firewall and filtering. There is a clear route for reporting and managing changes to the filtering system.

Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- Any breach of the filtering policy will result in action in line with the school Disciplinary Policy

- Any filtering issues should be reported immediately to Drift IT.
- Requests from staff for sites to be removed from the filtered list will be considered by the Head Teacher. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Head Teacher.

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through the e-safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, INSET.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School E-Safety Policy and the Acceptable Use Agreement.

Audits/Reporting Logs of filtering change controls and of filtering incidents will be made available to:

- Head Teacher
- E-Safety Governor
- Safeguarding committee
- External Filtering provider / Local Authority / Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

Table of Changes	
Year	Change
2026	Filtering test re-run