

Policy/Procedure Title	Web Filtering Policy	
Review Cycle (*Please specify)	Yearly	
Responsible Department	IT Services	
Procedure *Owner (*Overall responsibility)	Head of IT Services	
Responsible *Person (if different to above) *responsibility for communicating changes and staff training where appropriate		
Types of provision this procedure applies to: (delete as appropriate)	All staff All learners All contractors All third parties	
Revision Record		
Rev. No.	Date of Issue	Details and purpose of Revision:
1	15/09/2023	Ratified
2	14/08/2024	Reviewed
3	12/02/2026	Reviewed

Equality Impact Assessment

Whenever a policy is reviewed or changed, its impact assessment also must be updated. The Equality Act 2010 seeks to simplify discrimination law and introduced statutory duties to promote equality whereby The College of West Anglia must, in the exercise of its functions, pay due regard to the need to promote equality in relation to the protected characteristics.

Could any staff or students be adversely impacted by this policy/process? If yes give details and how this will be mitigated:

Date:	Action and Monitoring:

E, D & I Statement

This procedure has been reviewed in line with the Equality Act 2010 which recognises the following categories of individual as Protected Characteristics: Age, Gender Reassignment., Marriage and Civil Partnership, Pregnancy and Maternity, Race, Religion and Belief, Sex (gender), Sexual Orientation and Disability. We will continue to monitor this procedure to ensure that it allows equal access and does not discriminate against any individual or group of people.

Contents

Introduction	2
Objective	2
Compliance	2
Monitoring	3
Filtering	3
Restricted sites include:	3
Reporting	4

Introduction

The college offer an extensive range of IT systems across campuses and online for course related activities and drop-in purposes. This policy applies to all College students and describes what the College considers acceptable use of College IT systems and data by students. By reading, **Introduction**

The College of West Anglia recognises the benefits and opportunities which technologies offer to teaching and learning. However, we also recognise that there are a multitude of harmful resources and content which we are obliged to keep learners safe from under the Keeping Children Safe in Education (KCSIE) requirements, we will do all that we can to make our learners and staff stay e-safe and to satisfy our wider duty of care. This web filtering policy is more for informational purposes and should be read in conjunction with the e-safety policy.

The policy applies to all users who have access to the college IT systems or their own devices using the college Wi-Fi whilst on-site.

Objective

The objective is to ensure that all learners and staff are kept safe from all illegal, harmful and inappropriate web content and that the college adheres to national policy and regulations. This is accomplished by using access control lists, web filtering, and conditional access. We also actively monitor the logs on the firewall and produce reports for senior leadership.

Compliance

Meeting digital and technology standards in schools and colleges is a set of standards set out by the Department of Education. The college currently follows these standards and has already implemented the recommendations within this.

Monitoring

The college has the following software in place to monitor user activity:

- a. Smoothwall monitor (formerly e-Safe).
- b. R;pple.

Smoothwall monitor automatically alerts the safeguarding team when certain criteria are met. However, the above in themselves are not enough, so they are augmented with web filtering.

Filtering

The college uses FortiGate Fortinet firewalls in order to prevent intrusion however these devices also provide filtering to stop users accessing inappropriate sites. This is achieved via blacklists on the appliance which are updated automatically on a daily basis via the vendor. IT Services also actively block individual sites as and when requested or if they come to light via other means such as a request.

FortiGate, the vendor, is part of the:

- a. Counter-Terrorism Internet Referral Unit List
- b. Internet Watch Foundation.

The firewall appliances themselves can also handle:

- a. Multi-lingual web content.
- b. Filter images based on their URL.
- c. Common misspellings.

As standard the college has enabled the blocking of:

- a. All gambling sites.
- b. All pornographic sites.
- c. All radicalisation sites.

Restricted sites include:

1. Illegal content – such as:
 - a. Illegal images.
 - b. Terrorist content.
 - c. Child abuse.

2. Harmful content – Sites which promote:
 - a. Self-harm.
 - b. Suicide.
 - c. Drug abuse.
 - d. Violence.

3. Inappropriate content – such as:
 - a. Discrimination of any form.
 - b. Gambling sites.
 - c. Piracy and copyright theft.
 - d. Pornography.

These sites can only be blocked once they are known about hence this list is updated on a daily basis. A test was performed to check the level of blocking, the results are attached at Appendix A.

Reporting

Reports are created on a weekly and monthly basis. They report on:

1. Attempts made to restricted sites.
2. Searches made using offensive language.