William College

Web Filtering and Monitoring Policy

© William College. All rights reserved

Document Version Control	
Document Title	Web Filtering and Monitoring Policy
Version	1
Reviewing Committee	Senior Leadership and Management Team
Approving Committee	Senior Leadership and Management Team
Policy Lead	IT Coordinator
Date of Last Review	May 2026
Date of Approval	May 2026
Date Effective from	June 2026
Date of Next Review	November 2027

© William College. All rights reserved

William College

Table of Contents

1. Introduction 3
2. Purpose 3
3. Scope 3
4. Roles and Responsibilities 4
5. Storage, Retention, and Use of Logged Information 4
6. Implementation of Web Filtering and Monitoring 4
7. Determination and Review of Restricted Content 5
8. Restricted Content 5
9. Incident Reporting Procedures 6
10. Data Protection and Privacy 6
11. Policy Review 6
12. Related Policies and Legislation 7

© William College. All rights reserved

1. Introduction

Web filtering and monitoring are essential security practices at William College to maintain a safe and efficient online environment for students, staff, and visitors. These measures aim to prevent access to harmful, malicious, or unsuitable material while supporting academic freedom and safeguarding the integrity of William College's IT systems.

2. Purpose

This policy provides a framework for the effective management of web filtering and monitoring at William College in line with Prevent and Safeguarding obligations, as well as ensuring the security and reliability of network and digital resources.

Under the Prevent duty, William College is legally required to take steps to stop individuals from being drawn into terrorism. Careful consideration has been given to the Office for Students' (OfS) sector-specific guidance on implementing Prevent.

The primary aims of this policy are:

- Protecting users from harmful or inappropriate online content.
- Preserving the security and integrity of William College's IT infrastructure.
- Ensuring adherence to legal and regulatory requirements, including Prevent and Safeguarding duties.
- Encouraging responsible and ethical internet use within the William College community.

3. Scope

This policy applies to all students, staff, and visitors using William College's IT systems, all devices connected to the network including desktops, laptops, mobile devices, and guest BYOD equipment, all campuses where Wiliam College offers network access, and cloud-based platforms and remote users connecting via VPN. The restrictions enforced by this policy should be read alongside the Acceptable Use of IT Services Policy, which outlines expected behaviours for network and equipment users, and the Safeguarding and Prevent Policy, which set out the college's broader approach to safeguarding and preventing terrorism.

As a result of these security measures, certain websites may be inaccessible unless prior permission has been granted. William College retains logs of user activity for purposes such as network monitoring, cybersecurity, operational management, and investigations linked to the Prevent duty. Definitions and purposes of data collection are provided when connecting to the organisation's Wi-Fi.

The recorded information includes firewall traffic and website access logs, user identity details (where available), source and destination IP addresses, traffic type, intrusion prevention data, and website categorisation.

© William College. All rights reserved

4. Roles and Responsibilities

The IT Coordinator is responsible for deploying and managing web filtering technology, reviewing logs for investigations, and ensuring compliance with this policy; they authorise requests for access to websites restricted for cybersecurity reasons.

The Designated Safeguarding Lead authorises requests for access to websites restricted for safeguarding reasons and serves as the point of contact if any safeguarding concerns are raised by the IT team while carrying out duties under this policy.

The Designated Prevent Lead authorises requests for access to websites restricted for Prevent-related reasons and acts as the point of contact if any Prevent concerns are identified by the IT team during their work under this policy.

The Provost jointly authorises requests for access to restricted websites where the purpose relates to academic or research needs.

Members of the Senior Leadership and Management Team are responsible for ensuring that all staff and students under their supervision are aware on the significance of web filtering and monitoring as part of William College's cybersecurity awareness programme.

5. Storage, Retention, and Use of Logged Information

All web activity logs are securely stored on William College's encrypted servers, accessible only to authorised IT staff. Retention periods comply with GDPR requirements to ensure data is retained only for as long as necessary for safeguarding, security, and operational purposes.

Web activity logs are kept for 30 days, after which they are permanently deleted unless required for ongoing investigations or other compliance needs. Access to this data is strictly limited to security incidents, policy breaches, or formal requests from safeguarding or compliance teams. Logs are periodically reviewed for security audits, network optimisation, and compliance verification.

6. Implementation of Web Filtering and Monitoring

William College uses dedicated devices to manage web filtering and monitoring across its campuses. The system is designed to:

- Filter content according to the categories outlined in section 8.
- Monitor and record web activity.
- Ensure compliance with safeguarding and security policies.
- Detect and log attempts to access restricted websites.
- Capture device name, IP address, and attempted URLs.
- Maintain online safety and compliance with Prevent obligations.

© William College. All rights reserved

7. Determination and Review of Restricted Content

The IT team applies web filtering based on restricted content categories listed in section 8, which are reviewed during each policy update cycle. The detailed list of restricted websites is only accessible to the authorised roles highlighted in section 4 to ensure system effectiveness.

Staff and students who need access to sensitive material for legitimate academic purposes must submit a request to the IT team, including justification and any supporting documentation such as research requirements. Requests are assessed within five working days by the IT team and the relevant authorising staff member identified in section 4, according to the restricted content category concerned. All requests and decisions are recorded, and access is granted under controlled conditions.

If a request is refused, users will receive a formal explanation by email, which can be escalated for final review to Senior Leadership.

Academic freedom will be considered when evaluating requests for access to restricted content, in line with the Academic Freedom and Freedom of Speech Code of Practice.

8. Restricted Content

Restricted content categories under the Prevent Duty:

Content	Definition
Extremism	Encourages or glorifies terrorism, radicalisation, or hate-based ideologies.
Violence and Gore	Contains excessive violence, graphic imagery, or disturbing material.
Hate Speech	Promotes discrimination, bigotry, or incites violence against individuals or groups.
Weapons and Firearms	Encourages the use, sale, or manufacture of illegal weapons and firearms.
Misinformation and Fake News	Spreads false or misleading information that may cause harm or deception.

Restricted content categories under Safeguarding duties:

Content	Definition
Self-Harm	Encourages acts of self-injury, suicide, or participation in hazardous challenges that could result in harm.
Drugs and Substance Abuse	Advocates or facilitates the consumption, distribution, or production of illegal drugs and related substances.
Gambling	Promotes online wagering, casino-style games, and other gambling activities.
Pornography and Adult Content	Includes sexually explicit material or services intended for adult audiences.
Online Harassment and Cyberbullying	Enables abusive behaviour online, including threats, doxxing, intimidation, or other forms of harassment.

© William College. All rights reserved

These categories aim to safeguard system integrity and ensure compliance with regulatory standards:

Content	Definition
Malware / Hacking	Encourages system compromise through tools such as anonymous browsing, filter circumvention, or sites hosting harmful software.
Piracy and Copyright Infringement	Supports unlawful downloading, streaming, or sharing of copyrighted works.
Phishing and Fraud	Engages in deceptive tactics to obtain sensitive personal or financial information.
Illegal Activities	Promotes or facilitates criminal behaviour including fraud, theft, or exploitation.
Proxy and VPN Services	Attempts to evade network security controls through VPNs, proxy servers, or other anonymisation methods.

9. Incident Reporting Procedures

Any suspected breach or unauthorised attempt to access restricted material must be reported immediately to the IT team, with no further action required from the user.

The IT team will carry out an initial review and escalate serious cases to the Designated Safeguarding or Prevent Leads, or Senior Management if necessary. Where a critical security or safeguarding risk is identified, urgent measures will be implemented and the relevant procedure followed.

For severe incidents requiring external involvement, such as law enforcement, reports will be made in line with William College's Data Protection Policy and Safeguarding and Prevent Policy.

10. Data Protection and Privacy

Web activity records will be securely stored and accessed only by authorised staff. William College will adhere to GDPR and the Data Protection Act 2018 to ensure responsible handling of personal data. Secure disposal processes will be applied to guarantee that logs and other stored data are permanently erased in compliance with data protection laws.

11. Policy Review

This policy will undergo review at least every 18 months to remain aligned with Prevent and Safeguarding obligations, emerging cybersecurity risks, and legal requirements. Should regulatory or legal frameworks change, William College reserves the right to update this policy at any time.

© William College. All rights reserved

12. Related Policies and Legislation

Related Policies:

- Acceptable Use of IT Services Policy
- Data Protection Policy
- Anti-Malware Policy
- Staff Bring your Own Device Policy (BYOD)
- Safeguarding and Prevent Policy
- Academic Freedom and Freedom of Speech Code of Practice

Relevant legislation:

- UK General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- Counter Terrorism and Security Act 2015
- Prevent

© William College. All rights reserved