Web filtering and monitoring considerations for the higher education sector in the context of the Prevent duty

Purpose

This document aims to provide suggested policy considerations and technical guidance to inform providers' approaches to meeting the requirements on information technology (IT) as set out in the Prevent statutory guidance. It is not a legal document or an extension of the statutory Prevent guidance, but seeks to respond to sector feedback and provide further advice and examples of effective practice to support providers in implementing the Prevent duty.

This document has been produced following discussion between the Department for Education (DfE), the Higher Education Funding Council for England (HEFCE) and Jisc, and complements other resources and materials available. It includes:

- case studies (**Annex A**)
- links to additional resources (**Annex B**).

It is aimed at practitioners with responsibility for the implementation of the Prevent duty in relevant higher education bodies (RHEBs)[1], including:

- IT professionals
- staff with operational oversight of institutional IT strategies
- Prevent duty leads
- Prevent duty working groups.

This document only applies to higher education providers in England. Alternative monitoring arrangements and supporting guidance in relation to Prevent are in place in Wales and Scotland.

[1] The terms 'RHEBs', 'providers' and 'institutions' are used interchangeably in this document.

Contents

Statutory requirements

Under the Counter Terrorism and Security Act 2015, RHEBs must have due regard to the need to protect people from being drawn into terrorism (the 'Prevent duty'). This places a specific set of responsibilities onto higher education, further education and skills providers among other sectors.

There are **two specific IT requirements** detailed in the Prevent duty and associated guidance, reproduced below. These are the consideration of the use of filters as part of an overall strategy to prevent people from being drawn into terrorism, and the implementation of clear policies for students and staff working on sensitive or extremism-related research.

27. We would expect RHEBs to have policies relating to the use of their IT equipment. Whilst all institutions will have policies around general usage, covering what is and is not permissible, we would expect these policies to contain specific reference to the statutory duty. Many educational institutions already use filtering as a means of restricting access to harmful content, and should consider the use of filters as part of their overall strategy to prevent people from being drawn into terrorism.

28. To enable the university to identify and address issues where online materials are accessed for non-research purposes, we would expect to see clear policies and procedures for students and staff working on sensitive or extremism-related research. Universities UK has provided guidance to help RHEBs manage this.

The **consideration** of a web filtering and monitoring system is a requirement of all RHEBs in relation to the Prevent duty. All providers have now confirmed to HEFCE through the annual report process their approach to using filters. All providers have also either shared or explained their **policies relating to the use of their IT equipment**, and the consequence for users of failing to adhere to these policies.

The challenge for providers will continue to be whether these decisions and policies work and are effective in practice, as well as their cost and resource implications.

A number of case studies illustrating positive examples of effective practice have been included at Annex A.

Implementation of the duty

Baseline considerations

Providers should have appropriate IT policies and procedures in place which safeguard users effectively and are proportionate to their context. For example, as a baseline, it is recommended that all RHEBs should:

- ensure all users have unique user accounts
- reflect risks specific to IT in their Prevent and broader institutional risk assessments
- review decisions regularly.

Decisions relating to IT and the Prevent duty should not be taken in isolation. Below are some further examples of issues providers may wish to reflect on when implementing a suitable IT system and reviewing existing arrangements:

- links to safeguarding and welfare policies and processes
- impact on broader legislative responsibilities, including freedom of speech and academic freedom
- acceptable usage policies and related policies, for instance disciplinary policies, social media policies
- staff training programme
- users' e-safety programme
- Prevent duty risk assessments and broader institutional risk assessments
- regular review of strategies and supporting policies.

Considerations and prompts

- How do our IT policies and related processes link in with our safeguarding and welfare policy? What opportunities are there to share concerns and develop our strategies further?
- Is there a designated Prevent or safeguarding link person in the IT team? Where do our IT acceptable use policy and other related policies refer to the Prevent duty?
- How is IT covered in our Prevent staff training programme? Is this sufficient?
- What is covered in our learner e-safety programme? Are we covering this as early as possible in the course?
- How does our Prevent duty risk assessment influence the technical response?
- How do we review our existing arrangements and subsequent policies, and ensure they remain fit for purpose?
- Is there suitable IT representation and expertise on Prevent working groups?

It is suggested that e-safety should be covered in the first week of staff and student induction processes, or when user accounts are activated. It is recommended that good e-safety practice should be regularly covered throughout a learner's academic career or a member of staff's employment, and that opportunities can be naturally taken where the use of the internet is required.

Web filtering and monitoring

Web filtering specifically covers the filtering of content, generally to block access to inappropriate content, while **web monitoring** provides a system to log access to the internet. It is important to note that the measures implemented by a provider are only effective while users are actually accessing the internet via the organisations systems. Should a user switch to using a 3G or 4G mobile network on their own device, this web traffic will not be visible. It is important for providers to consider the implications of these limits on what they can monitor for corresponding institutional policies and processes, including acceptable usage, social media, arrangements for

brand management and similar. Providers should also consider how long they keep information that is attributable to an individual, and in what cases this information can be reviewed when developing related policies.

Web monitoring systems will record a user's web activity to differing levels of detail, but will normally record web pages visited, terms used on search engines and files downloaded or accessed. It is possible to retain this data for differing lengths of time, depending on the type of system in place. Most systems allow for automatic reports (sometimes called 'surface logs') to be generated, as well as of a specific user's activity, perhaps over a given time period. Many providers have demonstrated effective practice in reviewing these reports, logs and notifications, and staff reflect on this additional information when convening case conferences around student or staff welfare concerns.

Further detail regarding services available to members via Jisc and other helpful resources is given in Annex B.

Helpful questions to consider with IT staff

- Do all our staff and learners have individual user accounts?
- Do we have a web filtering system? Is it meeting our Prevent-related needs?
- Do we have web monitoring? Where in our policies is this noted? Are we actually doing what we say we are doing?
- Are we supporting the users (staff and learners) correctly? Do they feel comfortable coming to us? Do they understand we are looking out for them?
- Are we looking at our internet usage logs? What is being logged? Is this useful? Who is looking at the internet usage logs? Under what circumstances are the logs being reviewed? Have we communicated this appropriately (for instance, to the Prevent lead)?
- Are all our connected devices, including mobile devices such as iPads and Android tablets, subject to filtering and monitoring?
- Does the filtering and monitoring apply to 'Bring Your Own Device' (BYOD) devices joined to the guest wireless service?

Broader considerations in implementing IT policies

It is important that providers consider their IT strategy and the potential implications in the context of broader institutional policies and associated risks, which should be captured accordingly and subject to risk assessment procedures. This is because it is imperative that there is accountability. The points below highlight some further areas providers may wish to explore as part of the process for meeting the IT requirements of the statutory guidance.

IT strategy and related processes

- Ensure that the institutional IT strategies are clearly communicated to all. It is a legal requirement to inform users if the institution is using web filtering or monitoring, as the logs will constitute personal data under the Data Protection Act.
- Ensure, irrespective of whether or not a provider has decided to implement filtering and monitoring, that it creates a policy that fully reflects its institutional approach. Ensure that all agreements are updated to reflect this decision.
- Ensure that related policies and processes are clear and widely communicated.
- Communicate clearly how logs will be used to ensure the systems are not abused, including when and how an investigation would be conducted, and how information would be shared.
- Explain the rationale behind the IT strategy and related policies. It is important to explain why these measures are in place and to clarify what they are intended to prevent and detect. It is useful to make it clear and transparent that web filtering and monitoring are in place for the purposes of safeguarding and to discharge the Prevent duty.
- If the provider has decided to implement web filtering, use the policy to inform its configuration, rather than this being led by an internal or external IT service. It is important that the staff who administer web filtering and monitoring systems are operating under the terms of their institutional policy.
- Review strategy and related policies regularly, to ensure they are fit for purpose and effective. For instance, does the policy sufficiently address and manage risks associated with desktops, laptops, mobile devices, and devices using guest wireless systems including BYOD. It should be noted that to be considered effective, IT systems should be able to ascribe all web traffic to an individual, irrespective of the device it is generated from.

Accountability

- Ensure that all users are informed of appropriate policies and related procedures, and that all communications are clear and repeated throughout period of study or employment.
- Ensure good accountability from the institution for its users' internet access.
- Consider whether all users are easily able to manage their own account passwords. If not a simplified password option could be used or, in exceptional circumstances, designated staff members could have access to student passwords to provide access support. If the password policy is modified for use or another method of login is utilised, record and manage this in accordance with robust policy guidance to minimise the associated risks.

- Manage such breaches appropriately and according to related policies, for instance on the basis of standard disciplinary procedures
- Ensure that all users have their own user accounts, as accountability is not possible if group accounts are in use.

Risk assessments

- Ensure that a full institutional risk assessment has been completed to determine whether, and at what level, filtering and monitoring may be appropriate.
- Ensure that the risk assessment reflects the risks identified in the Prevent risk assessment. It may be useful to undertake individual or group risk assessments for learners with additional support needs and apply a different filtering profile to those learners, should the infrastructure allow this.

Safeguarding and welfare

- Consider its IT strategy as part of a broader safeguarding and welfare approach for users.
- Ensure regular review of set 'filters'.
- Ensure regular reporting directly to a designated member of staff for review.
- Ensure regular review of notifications, alerts and subsequent reports by a competent or designated member of staff who has had relevant safeguarding, welfare or Prevent-related training. Ensure this staff member knows who to contact and how to share concerns appropriately should a concern arise.
- Ensure clear processes for logging and reporting unintended access to inappropriate content, and that these are well communicated. This is particularly relevant where staff have a duty of care for vulnerable users.
- Consider how data is handled and stored.

Sensitive or extremist-related material

A provider may also need to consider the impact of web filtering on legitimate research into sensitive or extremist-related material. It is a requirement of the duty that RHEBs have clear policies and procedures in place for students and staff researching these areas. It is the responsibility of every institution to understand the risk of any given piece of research, to work with appropriate partners and identify the support required for researchers and those with responsibility for guiding and approving sensitive or extremism-related research. Universities UK has produced guidance to help providers manage this.

A number of providers have found it useful to create flowcharts which illustrate how permissions may be requested for legitimate research, or which show how a concern, incident or report by

exception procedure might be dealt with. These demonstrate the decision-making points, who makes such decisions and the options for progressing the request or incident. Such a flowchart can usefully demonstrate where existing safeguarding or human resources processes can be activated, and when external bodies such as the police should be contacted for assistance. Working with Jisc, we intend to develop a flowchart template to supplement this guidance note for providers that may find this useful.

Further considerations

- Specially designated university devices and servers should be supervised by university ethics officers or their counterparts.
- Ethics officer or their counterparts should be the first or an early point of contact for internal enquiries and police enquiries about suspect security-sensitive material.
- In relation to storage, comprehensive advice should be provided to all users, highlighting the legal risks of accessing and downloading files from sites that might be subject to provisions of counter-terrorism legislation. It is suggest that reading this advice should be among the terms and conditions of user access.
- Appropriate training for ethics officers or their counterparts, and for IT Officers.
- Appropriate training for staff involved in Prevent-related processes, for instance those accessing information in relation to potential speakers.

Annex A: Effective practice case studies

Referenced below are five case studies illustrating a range of effective approaches taken by particular providers in relation to the IT requirements detailed in the Prevent duty. It is important to note that there will be contextual factors which make these approaches appropriate approach for these individual providers, and that these will have been considered in line with the appropriate institutional procedures. RHEBs should always consider their individual risks and circumstances.

Case study: University of Sunderland

The institution decided to introduce web blocking across all its networks, and extended this approach to include student residences and third-party tenants. It was agreed, following extensive consideration, that the university would block access to extremist-related material as well as to two other categories.

As part of its strategy, the institution revised its acceptable IT use policy to ensure it aligned with the requirements of the duty, including explicit reference to the statutory duty and the consequences of accessing, promoting or supporting Prevent-related material.

The institution also established a clear process to authorise access to restricted content for legitimate research purposes for staff and students, including a decision log and a review of access.

The institution is committed to reviewing the efficacy of the arrangements and will do so at set points. It has also committed to establishing links to existing external projects, such as those facilitated by Safe Campus Communities.

Case study: University College London

The university reserves the right to monitor internet activity if it believes in grounds to suspect that there has been a breach in its computer regulations or that an individual is acting unlawfully.

The university's computing regulations state that staff and students have an obligation to abide by the Counter-Terrorism and Security Act 2015. This policy applies to the use of all IT facilities and sets out clear definitions of acceptable and unacceptable use. The policy specifies that university websites shall not link to unacceptable external sites. The regulations identify a route for reporting non-compliance and the disciplinary action that may follow.

Additionally, access to the internet from any IT system connected to the campus network is recorded, and the logs are retained to allow suspected misuse to be investigated in accordance with UK law. This has allowed the university to maintain strong relationships with academics and students alike, assuring them that every measure is being taken to reduce the risk of academic freedoms being infringed.

Case study: London Metropolitan University

The university has ensured that the IT system includes a pop-up on blocked sites, directing users to contact the University Secretary's office if they need access for approved research purposes.

The university is working with its IT team in a number of ways to maintain vigilance. A weekly spreadsheet of hits in the extremism category is provided to the University Secretary's office. It is intended that a one-off attempt to access these websites prompts an email to the user which explains why it was blocked and refers to the acceptable IT usage policy. Serial attempts to access blocked material will be treated as a concern under the university's wider safeguarding policy.

Case study: University of Bristol

In considering whether to implement web filtering, the university consulted, ensuring staff and students had the opportunity to comment and to shape the institution's approach.

The IT Services department identified and produced a statement on each of the themes presented in the duty, which included:

- policies for acceptable use and processes for managing misuse
- access
- management of websites and social media by affiliated groups
- consideration of filtering and monitoring.

The university considered effectiveness and cost of blocking, use of social media, impact on network performance, and potential effects on academic freedom.

On the basis of the information gathered through this approach, the university has agreed to continue with its current approach and refine processes where necessary. The institution has, however, committed to becoming 'filtering ready'.

Subsequently, the acceptable use policy and the social media policy were revised to include clear definitions of what is and is not permissible in relation to extremist-related material, the approval route if access is required for legitimate research, and the consequences of any breach.

The processes for managing legitimate research were also updated. The amendments were made in collaboration with the key parts of the university, including staff from Student Welfare, Legal Services, IT, Human Resources and the students' union.

The university will continue to review its decisions and the available alternative options on a regular basis, and to engage with the university community as part of its decision-making process.

Case study: University of Buckingham

If a user is visiting a site of concern, they will be greeted by a notification prompt advising them that access to the specific webpage is not recommended and further access will result in a digital footprint. The Prevent lead reviews corresponding reports on a daily basis, which enables the university to build up a profile of web activity which may need to be considered alongside other institutional policies such as safeguarding. While filtering was introduced in response to the duty, as part of the university's IT strategy, these full and frequent reviews have positively impacted on the user experience as key terms have been revised accordingly, resulting in a reduction in the number of notifications.

Annex B: Support and resources available to the sector

Jisc

Jisc provides digital solutions to its members including access to the Janet network. The Jisc website offers a range of options including web filtering support, information about Prevent and training materials.

Further information regarding all of the services available to members and guidance documents can be located on the Jisc website. Some examples of these services and areas of guidance include:

- Janet network Computer Security Incident Response Team – with a primary function to monitor and resolve any security incidents that occur on Janet. This function is only available to those who have subscribed to Janet.
- Web filtering and monitoring framework – solutions enabling member institutions to apply their web use policies with the most appropriate technology and toolset. Frameworks are open to all public sector organisations.
- Vulnerability assessment and information framework – detecting and managing internal and external vulnerabilities, to help members to manage their security risks, compliance and quality. Frameworks are open to all public sector organisations.
- Penetration testing – helping members reduce the risk of information security breaches and the costs of prevention, management, remediation and audit activities. Penetration testing is open to all public sector organisations.
- Safe Share – an overlay security service, transferring data securely between partners via the internet. Safe Share is open to all public sector organisations.

Security blacklists and whitelists

- Simulated phishing and associated training framework (open to all public sector organisations).
- Training on Filtering and Monitoring: how can they help? (Open to all public sector organisations)
- Jisc certificate service
- See also:
  - Jisc guide to Network monitoring
  - Jisc's Acceptable use policy
  - Janet's Security policy and Eligibility policy.

As a matter of routine Janet Network is not filtered, but members are able to purchase a web filtering and monitoring via the Jisc procurement framework. There are a number of suppliers on the framework including:

- Comtact (ZScaler)
- Gaia Technologies (SmoothWall)
- iBoss Cybersecurity (iBoss)
- Insight (Smoothwall)
- Pinacl Solutions (SmoothWall)
- Softcat (CensorNet).

There is a 'buyers guide' available on the framework. The framework's scope of requirements is also available, detailing the stringent requirements that all suppliers on the framework have had to meet. Advice and guidance on the framework can be provided by contacting the Jisc service desk. Additional context can be provided by Jisc subject specialists via the Jisc account manager.

The framework offers a number of advantages:

- preferential pricing
- options for cloud-based, local hardware-based and hybrid products
- ability to monitor, both with and without filtering
- ability to create and export reports on user activity
- ability to set different rules and categories for what different groups of learners and staff can and cannot access.

Jisc web filtering framework offers filtering solutions that can be based on locally hosted appliances and virtual servers, which are likely to be suitable for providers depending on their size (number of computers, devices or users), their location and the nature of their internet connection. It is also possible to use a cloud-based solution, and this may have certain advantages for some multi-site or distributed providers.

Other web filtering and monitoring products exist outside of the Jisc Web filtering and monitoring framework.

- Standalone appliances
  - Lightspeed
  - Forcepoint (formerly Websense)
  - Sophos
- Firewall-based
  - Smoothwall
  - Fortigate
  - SonicWALL
  - Sophos
  - WatchGuard

Jisc can also provide advice to subscribers on policies and the security features of a providers' network. If support is required, members should contact their assigned account manager in the first instance. For further detail regarding membership, providers should email membership@jisc.ac.uk.

Workshop to Raise Awareness of Prevent

Jisc is accredited by the Home Office to deliver the Workshop to Raise Awareness of Prevent (WRAP), as a live online facilitated session. WRAP is a free specialist workshop, designed by HM Government to give institutions:

- an understanding of the Prevent strategy and the provider's role
- the ability to use existing expertise and professional judgment to recognise the vulnerable individuals who may need support
- local safeguarding and referral mechanisms and people to contact for further help and advice.

This workshop is an introduction to the Prevent strategy, and does not cover wider institutional responsibilities under the duty.

HEFCE

HEFCE has published a series of documents intended to provide practical guidance and illustrative examples of effective practice, including a blog post following IT workshops earlier this year and an updated advice note. These documents and case studies are available via the HEFCE website.

These documents are:

- Evaluation of monitoring of the Prevent duty in higher education in England (HEFCE 2017/12)
- Analysis of Prevent annual reports from higher education providers for activity in 2015-16 (HEFCE 2017/11)
- Framework for the monitoring of the Prevent duty in higher education in England: 2017 onwards (HEFCE 2017/10)
- Guidance for Prevent annual reports for 2016-17
- Monitoring compliance with the 'Prevent' duty in higher education in England: Advice note for providers

Leadership Foundation for Higher Education

The ICT Challenge: Effective ICT policies available via the Safe Campus Communities website. This teaching component addresses means of securing networks, including the role of Jisc; appropriate ways to incorporate the Prevent duty into IT policies; some of the concerns relating to web filtering and the development of institutional specific policies; and the importance of avoiding approaches which impact adversely on research and learning and teaching. Providers need to register with Safe Campus Communities to access the material.

Red Stop button

It may be useful for institutions to provide the 'Red Stop button' on their websites or intranets, so learners and staff can report online material promoting terrorism or extremism**.**

UK Safer Internet Centre

The UK Safer Internet Centre provides a set of criteria which enable providers to review the quality of their arrangements.

Useful Gov.UK pages

- Prevent duty guidance
- Counter Terrorism and Security Act 2015
- Keeping the UK safe in cyberspace
- 10 steps to cyber security
- Advice for small businesses.

Other sources of support

- Cyber Essentials
- Cyber Streetwise