GOV.UK Topics Departments Government activity

→ Coronavirus (COVID-19) | Guidance and support

Home > Education, training and skills > Further and higher education, skills and vocational training > The Prevent Duty and ICT policies in higher education (HE)

Department for Education

Guidance

The Prevent Duty and ICT in higher education (HE): guidance on effective policies to manage risk

Published 20 October 2021

Contents

Organisations whose ICT systems comply with good practice should be in a good position to meet the requirements of the Prevent statutory guidance. You need to balance logging and filtering traffic within a Prevent context with users' privacy rights under general data protection regulations (GDPR).

The Prevent duty asks HE institutions to consider the use of web filtering. The National Cyber Security Centre (NCSC) provide guidance on how organisations can protect themselves in cyberspace.

Further information

Print this page

The use of information in higher education settings

Information and the underlying technology used to store and process it are critical to effectively running an education setting. Confidential or sensitive information, and intellectual property, are an important part of an education provider's operations. At the same time the need to access and share information more widely, using a broad range of connecting technologies, can present settings with risks.

Identifying potential threats

Being aware of potential threats is a normal part of risk management across the education sector. Alongside financial, legal, HR and other business risks, providers need to consider threats to their critical information assets and what the impact on complying with the Prevent statutory duty would be if those assets were compromised. Providers should work to mitigate risks to critical information assets and be able to reduce the impact of, and recover from, problems as they arise.

What are the threats?

The internet is used by terrorists and extremists to spread propaganda, radicalise potential supporters, raise funds, communicate and plan. While terrorists can be expected to continue to favour high-profile physical attacks, there is a growing threat that they might also use cyberspace to radicalise vulnerable people to facilitate or to mount attacks against the UK.

The threat to the UK from politically motivated activist groups operating in cyberspace is real. Attacks on public and private sector websites and online services in the UK orchestrated by 'hacktivists' are becoming more common, aimed at causing disruption, reputational and financial damage, and gaining publicity.

All these different groups – criminals, terrorists, extremists, foreign intelligence services and militaries – are active today and working against the UK's interests. The borderless and anonymous nature of the internet means that precise attribution is often difficult and distinguishing threats is increasingly difficult.

Organisations that do not produce user security policies or train their users in recognised good security practices will be vulnerable to numerous risks. Providers can:

- produce policies covering the acceptable and secure use of the organisation's systems

- establish a staff induction process to ensure new users receive training on their personal security responsibilities
- maintain user awareness of the threats and ensure they receive regular refresher training on the cyber risks to the organisation

Monitoring in the Prevent context

Monitoring ICT activity allows relevant higher education bodies (RHEBs) to detect attacks and react to them appropriately while providing a basis upon which lessons can be learned to improve their overall security. In addition, monitoring the use of ICT systems allows providers to ensure that systems are being used appropriately and in accordance with organisational policies that help them comply with the Prevent duty.

Monitoring is a key capability that can help providers comply with security, legal and regulatory requirements.

Providers can:

- establish a monitoring strategy and supporting policies based on an assessment of the risks
- monitor all ICT systems and ensure that this covers all networks and host systems (for example, clients and servers)
- monitor network traffic to identify unusual activity or trends that could indicate an attack

Jisc advice on Prevent

In response to questions about the Prevent duty's implications for ICT, which is part of the Home Office guidance, Jisc states:

> “ 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 being drawn into terrorism.”

The Home Office guidance emphasises that the duty builds on existing good practice and doesn't call for significant changes. If providers already use filtering to protect users from other types of harmful material it suggests they consider whether this can also contribute to their Prevent duty, but there is no expectation that organisations will start to use filters just for this purpose.

There is a recommendation that the statutory duty be mentioned in IT policies.

Although Jisc has not provided further guidance on this, it seems most likely that the duty would be one of the factors influencing organisations' acceptable use policies (AUPs), rather than a specific requirement on individual users. Many AUPs state their purpose as ensuring that ICT services are used to further the organisation's education and research purposes, and in accordance with the law.

> In this context our advice is that RHEBs should consider updating their acceptable use policy to refer specifically to the organisation's legal duty to "have due regard to prevent people being drawn into terrorism".

Institutions should also reference what is and is not permissible in the context of Prevent.

Jisc web filtering

Jisc provides access to a web filtering service which any organisation with a Janet Network connection is eligible to use.

Further information

Other useful websites include:

- UCISA resources
- Jisc acceptable use policy
- Jisc security policy
- National Cyber Security Centre's cyber security advice and guidance

Is this page useful?

Yes No

Report a problem with this page

Coronavirus (COVID-19): guidance and support

Check what you need to do

Services and information

- Benefits
- Births, deaths, marriages and care
- Business and self-employed
- Childcare and parenting
- Citizenship and living in the UK
- Crime, justice and the law
- Disabled people
- Driving and transport
- Education and learning
- Employing people
- Environment and countryside
- Housing and local services
- Money and tax
- Passports, travel and living abroad
- Visas and immigration
- Working, jobs and pensions

Departments and policy

- How government works
- Departments
- Worldwide
- Services
- Guidance and regulation
- News and communications
- Research and statistics
- Policy papers and consultations
- Transparency and freedom of information releases

Help Privacy Cookies Accessibility statement Contact Terms and conditions
Rhestr o Wasanaethau Cymraeg Government Digital Service