Department for Education

Guidance

The Prevent Duty and ICT in higher education (HE): trainer's notes

Published 20 October 2021

Contents

This presentation describes what the Prevent statutory guidance says about:

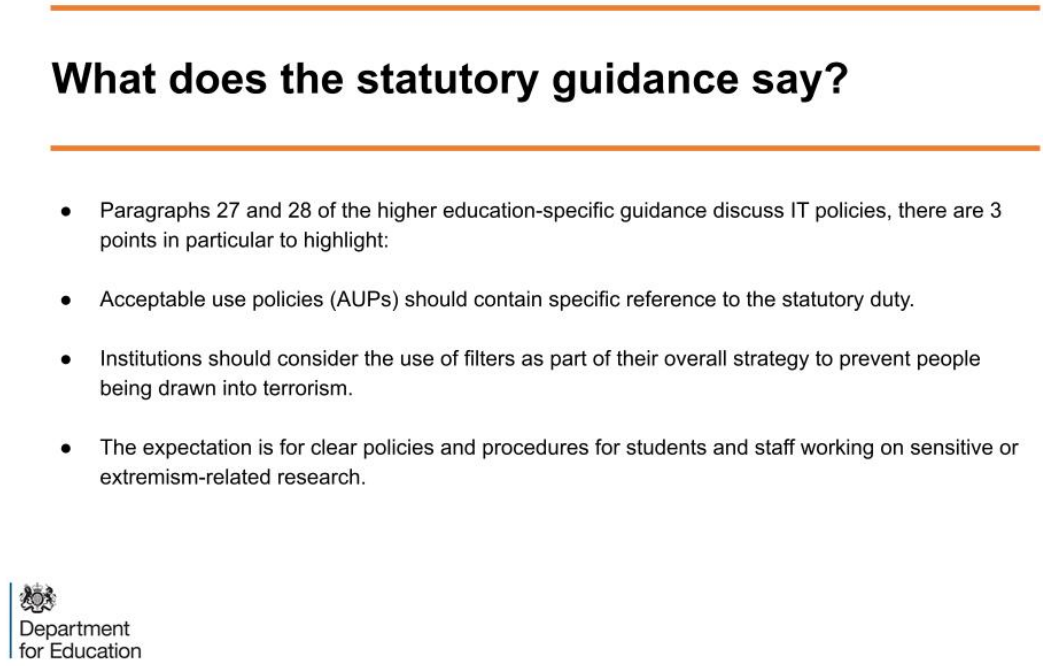
- ICT policies
- current practice in the context of acceptable use policies (AUPs) and policies on filtering
- good practice from UUK with regards to security sensitive research

These are all important to understand when developing policies and implementing the Prevent statutory duty.

Print this page

What does the statutory guidance say?

This refers to paragraphs 27 and 28 of the higher education-specific statutory guidance.



What does the statutory guidance say?

- Paragraphs 27 and 28 of the higher education-specific guidance discuss IT policies, there are 3 points in particular to highlight:
- Acceptable use policies (AUPs) should contain specific reference to the statutory duty.
- Institutions should consider the use of filters as part of their overall strategy to prevent people being drawn into terrorism.
- The expectation is for clear policies and procedures for students and staff working on sensitive or extremism-related research.

Department for Education

Acceptable use policies (AUPs)

These slides acknowledge the requirement to include reference to Prevent in AUPs, emphasising that reference alone to Prevent does not achieve compliance. AUPs should give examples of what is and is not permissible in the context of Prevent.

When considering Prevent and web filtering, Jisc offers a web filtering and monitoring framework. An online training package detailing how filtering can help is available from the Jisc website.

Policies also need to be communicated, applied and supported by appropriate policies on monitoring. Good practice will require institutions to ensure that other relevant procedures make reference to ICT policies. Staff and student induction should refer explicitly to AUPs.

Institutions should communicate any changes to policies effectively. They may find the model regulations produced by the Universities and Colleges Information Services Association (UCISA) useful.

Acceptable Use Policies (AUPs)

- Reference to the Prevent statutory duty in AUPs is relatively straightforward and submissions to OfS (previously HEFCE) so far show that the sector has complied with this expectation.
- Jisc's advice is that many AUPs already state that ICT services must be used to further the organisation's education and research purposes and in accordance with the law.
- Institutions should update AUPs to refer to the Prevent duty to prevent people (students and staff) being drawn into terrorism.

Communicating AUPs

- Policies alone are not sufficient to achieve compliance – they must be properly communicated and applied.
- Reference to AUPs needs to be explicit and form part of staff and student induction as well as being contained within other procedures (staff and student discipline for example).
- It is important that any changes to policies and procedures are communicated effectively

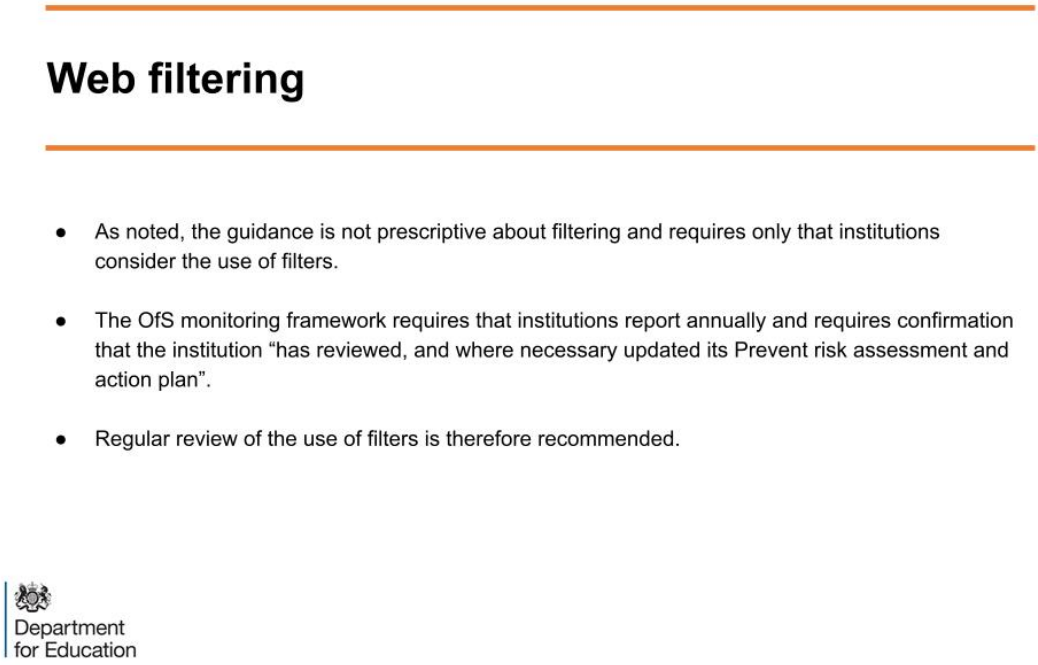
Web filtering

This slide introduces the issue of web filtering. The guidance requires all relevant higher education bodies (RHEBs) to consider their use of web filtering and reporting to Office for Students (OfS) as part of the monitoring framework.

It is noted that how an institution approaches filtering is not an entirely new issue.

For example, the filtering and blocking of sites deemed malicious or undesirable in the context of pornographic materials is common.

Many institutions will already have in place policies and procedures on web filtering, even if their stated policy is to employ only limited filtering.



Web filtering in the HE context

These slides look at the complexity of filtering in the HE context.

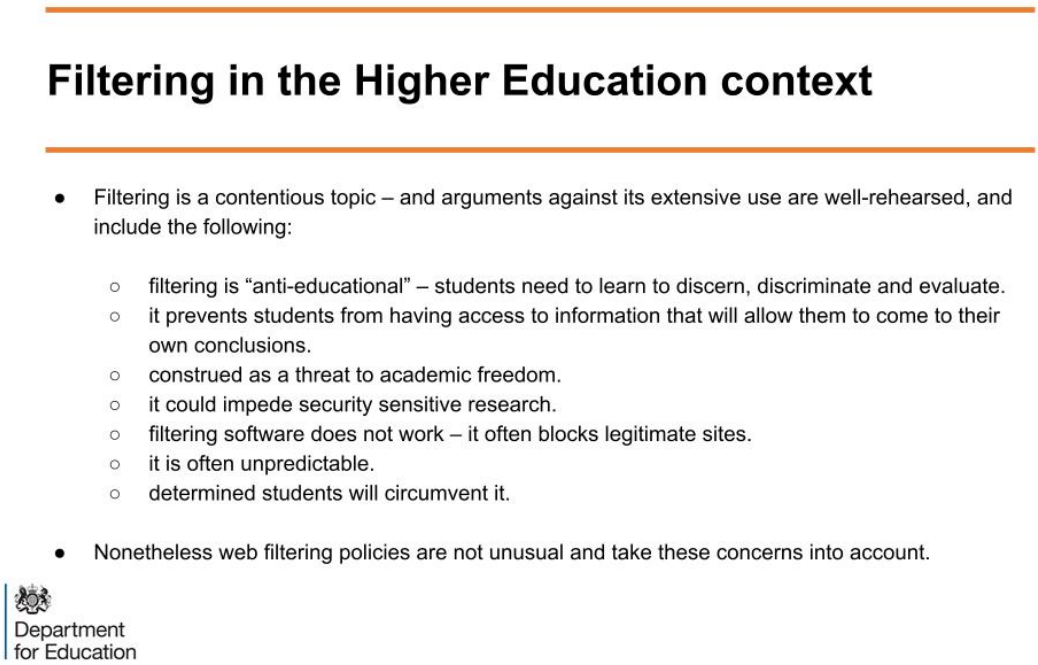
There are many concerns within academia in respect of web filtering. They are, to some extent, shared by representatives from other professions.

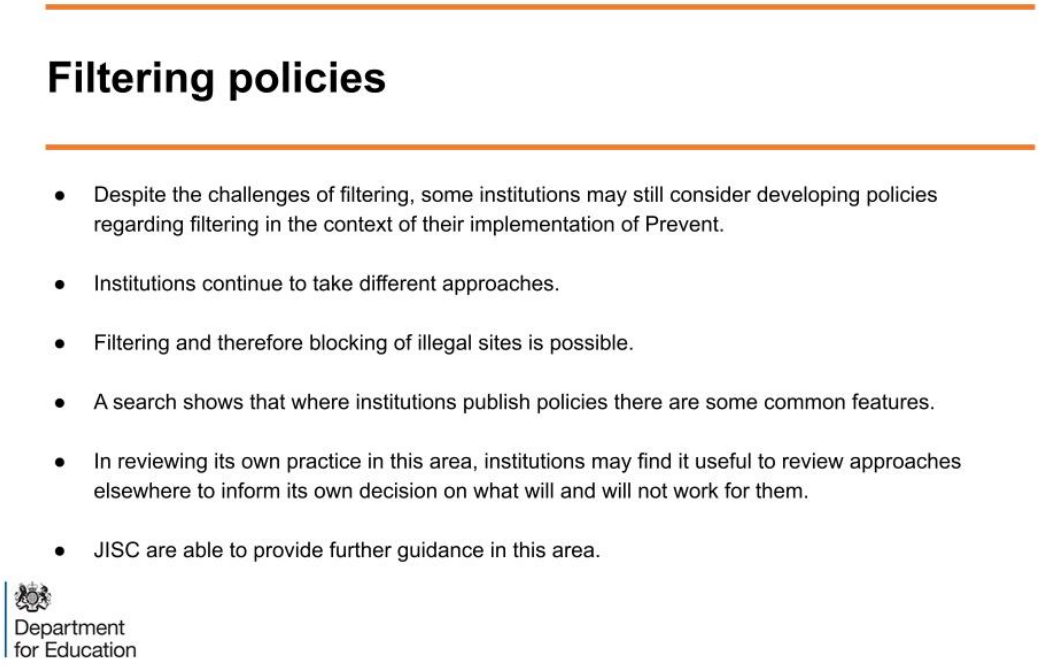
Freedom of information is also an issue to consider. However, an approach which limits access to proscribed sites or, in the context of public libraries, materials that might be harmful to young people may be a relevant approach for some organisations.

These slides indicate that while a number of institutions continue to consider and reassess their filtering policies in respect of their Prevent statutory duty, some RHEBs already have filtering policies in place. Institutions will want to review approaches across the sector to inform local decisions on what will and will not work for them.

Institutions should review their Prevent risk assessments at least once a year and take the opportunity to review the filtering position as part of that process.

Like AUPs, filtering policies need to be transparent and well communicated. They also need to include a procedure to deal with examples where access to sites has been blocked for being inappropriate.





Referring to filtering in AUPs

It is important that AUPs cross reference policies on filtering, ideally within the

section that deals with use of the internet. Institutions should identify the types of sites that may be blocked and what will happen in the event where someone tries to access a blocked site – an example statement is included. Ensuring due process has been undertaken for security sensitive research is key.

Reference to filtering in AUPs (1/2)

- Where filtering is employed, it is good practice to refer to such policies in AUPs as well as in filtering policies.
- This is usually within the section of the AUP which relates to appropriate use of the internet.
- Typically, users are warned that filtering is in place and examples of inappropriate use are listed, usually relating to access, storage and dissemination of materials from sites that reflect the institution's policy on filtering. This can include content that is:
    - illegal (including sites that encourage illegal activity)
    - contains obscene or deliberately offensive material
    - contains discriminatory material
    - likely to result in harassment or bullying of others.
    - likely to draw people into terrorism.

Department for Education

Reference to filtering in AUPs (2/2)

- In the event that users attempt to access sites that are blocked, an appropriate message is usually transmitted, typically along the lines of:
    - "the access to this website has been denied in accordance with the IT acceptable use policy. Please check section access to the internet. Should you feel unduly unable to access a legitimate website, please contact the IT Support Centre."

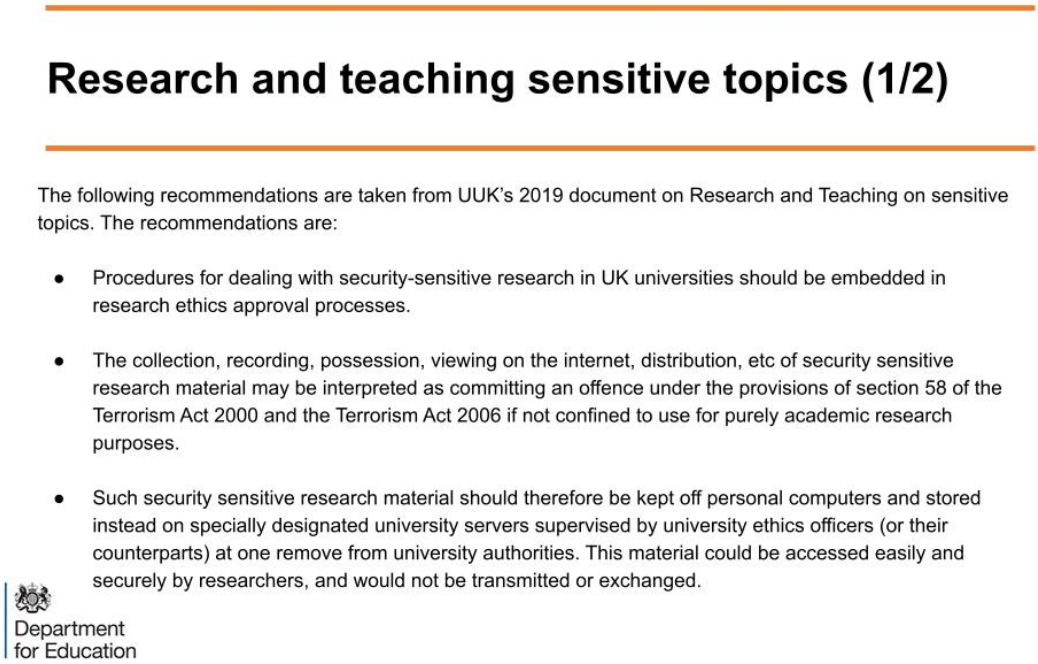
Department for Education

Research and teaching on sensitive

topics

These slides acknowledge the importance of having guidance in place to provide for research and teaching on sensitive topics, including matters relating to violent extremism and terrorism, and drawing on the recommendations of the UUK guidance on research and teaching sensitive topics. The statutory guidance refers to the UUK's 'Oversight of security-sensitive research material in UK universities' guidance.

Institution should have research ethics policies that include procedures where staff can request access to sites that might otherwise be blocked. This should be an issue that institutions have considered in a range of contexts.



Research and teaching sensitive topics (1/2)

The following recommendations are taken from UUK's 2019 document on Research and Teaching on sensitive topics. The recommendations are:

- Procedures for dealing with security-sensitive research in UK universities should be embedded in research ethics approval processes.
- The collection, recording, possession, viewing on the internet, distribution, etc of security sensitive research material may be interpreted as committing an offence under the provisions of section 58 of the Terrorism Act 2000 and the Terrorism Act 2006 if not confined to use for purely academic research purposes.
- Such security sensitive research material should therefore be kept off personal computers and stored instead on specially designated university servers supervised by university ethics officers (or their counterparts) at one remove from university authorities. This material could be accessed easily and securely by researchers, and would not be transmitted or exchanged.

Department
for Education

Research and teaching sensitive topics (2/2)

- Ethics officers (or their counterparts) should be a first, or early, point of contact for both internal university enquiries and police enquiries about suspect security sensitive material associated with a university or a university member. Such material should be treated as having a legitimate research purpose unless ethics officers (or their counterparts) cannot identify it or the relevant researcher responsible for it.
- The mechanism for storing security-sensitive material described above needs to be operated alongside comprehensive advice from universities to all university-based internet users, highlighting the legal risks of accessing and downloading from sites that might be subject to provisions of counter-terrorism legislation. Reading this advice should be a condition of getting a university email account.
- A training scheme should be offered to ethics officers (or their counterparts) and IT officers in universities about implementing the ethics review process and secure storage of sensitive material. Prevent leads should be involved in this training where relevant.

Summary

These slides seek to summarise the key points from the statutory guidance. The training slides have covered:

- how AUPs should include reference to Prevent and to filtering (if appropriate)
- to understand whether filtering is required
- good practice to follow to ensure that access to security sensitive material is appropriately managed

Summary (1/2)

- Acceptable use policies should refer to Prevent and what is and is not permissible.
- Students and staff should be made aware of these policies as part of induction and ongoing communications.
- RHEBs are required to regularly consider the use of filters as part of their overall strategy to prevent people from being drawn into terrorism – whatever decision is taken institutions will need to demonstrate that appropriate consideration has been undertaken.

Summary (2/2)

- There are significant concerns about extensive filtering that are well rehearsed but some institutions already have policies in place that pre-date the Prevent statutory duty so may decide to extend filtering for Prevent.
- If so, these need to be proportionate to ensure that legitimate sites are not inadvertently and inappropriately blocked.
- For many other institutions, a decision not to filter may be appropriate to protect security sensitive research.
- That policies need to include safeguards that protect academic freedom is widely recognised and understood.
- AUPs and policies on filtering and on sensitive research need to be well communicated so that their purpose and related processes are understood by staff and students.

Coronavirus (COVID-19)

Coronavirus (COVID-19): guidance and support

Brexit

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