Prevent Duty (Counter-Terrorism and Security Act)
Requirement to consider use of filtering

1 The Counter-Terrorism and Security Act 2015 places a statutory duty on specified authorities (including universities) to have “due regard to the need to prevent people being drawn into terrorism”. On the back of this the UK Government has issued Prevent Duty Guidance providing detailed information about what specified authorities need to do to comply with the duty. Birkbeck has considered the guidance and is in the process of undertaking the required actions to ensure compliance.

2 One aspect of the Prevent guidance relating to RHEBs (Relevant Higher Education Bodies) refers to IT policies. The guidance states:

“We would expect RHEBs to have policies relating to the use of their IT equipment. While all institutions will have policies around general usage, covering what is and is not permissible, we would expect these policies to contain reference to the statutory duty. Many educational institutions already use filtering as a means if 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”

3 The College Computing Regulations are available at: http://www.bbk.ac.uk/its/regulations/birkbeck-college-computing-regulations.pdf
These regulations have been updated to draw attention to Birkbeck’s statutory duty, under the Counter Terrorism and Security Act 2015, to aid the process of preventing people being drawn into terrorism. Reference to extremist material has been specifically highlighted in section 7.4 describing types of unlawful material.

“We must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist. The University reserves the right to block or monitor access to such material”.

4 We are now required to formally consider whether it is appropriate for Birkbeck to consider the use of web filtering to potentially block access to extremist material.

5 While the issue of web filtering has been periodically raised and is currently under active consideration on IT security grounds, for example to prevent the spread of malicious software, viruses, use of illegal filesharing (using BitTorrent), phishing sites etc., we have taken the view that content-filtering and blocking of specific websites at Birkbeck is not appropriate for the following reasons:

- Negative impact of content-filtering on academic freedom and operating within a culture of trust between staff and students (the majority of whom are working adults).
If awareness raising is a focus of the Prevent duty, this is more effectively achieved through promotion of acceptable use policies and safe use of the internet.

High overhead of administering content-filtering and possibility of endless discussions about what is permissible or not for academic / research purposes. Who takes responsibility for making these decisions?

No technical solution exists which can guarantee 100% accuracy in filtering illegal material, let alone extremist content. Manually adding or removing sites will add to the administrative overhead, even if they could be identified.

Ease with which users can bypass the university systems to access the internet via smartphones, social media and use of eduroam via other institutions). The introduction of content-filtering on university systems will only drive anyone wanting to access illegal material to use networks outside the scope of the institution.

Mechanisms already exist (through logs of computer activity and network traffic) for the investigation and support of anyone suspected of being radicalised or accessing illegal material. This is in keeping with our procedures for all types of computer misuse.

High cost of filtering high bandwidth networks with no clear business case for the introduction of filtering.

Our recommendation is that the introduction of content filtering is not an appropriate response for Birkbeck to undertake in consideration of the Prevent Duty guidance.

The Strategic Planning Committee and the IT Advisory Group are requested to consider endorsing the above recommendation.

Jasbir S Gill
March 2016