Draft Protocol: Removal of Websites

The Home Office website notes that the Terrorism Act 2006 (http://www.opsi.gov.uk/acts/acts2006/20060011.htm) aims to make it more difficult for extremists to abuse freedoms, in order encourage others to commit terrorist acts. The Act creates a number of new offences: acts preparatory to terrorism; encouragement to terrorism; dissemination of terrorist publications; and terrorist training offences. It also makes amendments to existing legislation. Section 1 of the Act makes it an offence to publish a statement which encourages acts of terrorism and Section 2 creates an offence of disseminating a terrorist publication. Dissemination includes certain conduct relating to material on the internet. Terrorist publications are publications the content of which encourages people to engage in terrorism, or provide information that could be useful to terrorists.

Below is the University's protocol of what to do to remove or modify offending websites. Action to remove or modify the websites needs to be taken within two working days of receipt of notices which are issued under the Terrorism Act 2006. In operating this protocol, the University is mindful of the need to appropriately maintain sensitive materials which are held legitimately for learning, teaching, research and educational purposes.

Some of the following steps can take place concurrently as they involve different areas or individuals. In the case of absence of any individuals involved in the process, the relevant deputies will participate.

Step 1 The University is issued with either a Voluntary Notice or a formal Notice under Section 3 of the Terrorism Act 2006 which requires us to ensure that, within two working days, the website is not available to the public or is modified so as not to be unlawfully terrorism-related. If the notice is voluntary the University has scope to discuss with the police the removal of the site and related material or evidential issues.

Either form of Notice would be issued to the University Secretary in person or to the University Secretary's office (or the Principal's office) by recorded delivery. It is important to log the Notice **immediately** as action needs to be taken within two working days.

Step 2 The following should be informed immediately about the Notice: the University Secretary, the Chief Information Officer, the Director of IT Infrastructure, the Director of Applications, the Audit and Security Manager and the Director of Communications and Marketing. The Principal should also be notified for information.

Step 3 The University Secretary and the Chief Information Officer (CIO) consider the Notice rapidly to make an initial assessment of the complexity of the case; the seriousness of the issue; the scope of the work to remove or block the website; and the extent of any consequential effects.

The University Secretary and CIO will decide whether:

1. the urgency of the situation requires immediate central action to block access to the relevant website (which might affect other websites); or
2. an attempt can be made to remove or modify the website through the School or other unit managing the website and to inform key colleagues before central action is taken.

If an Informal Notice has been issued, the University Secretary and CIO will also consider the further option:

3. the University may decide to take no action under the Voluntary Notice, in which case, the University lawyers are consulted before discussions with the police take place. This is expected to be an extremely rare occurrence.

Step 4 Under 3.1 above, the University takes rapid central action to block access to the web pages. This may involve blocking access to specific pages, an individual website, or a range of websites, some of which are not covered by the Notice. The initial blocking of the website is then followed by relevant elements of the following steps, to narrow the focus to removal or modification of the relevant website, and to involve the respective areas. If a significant amount of the University's website needs to be blocked temporarily by the action then a notice is put on the University's homepage explaining that the website is experiencing difficulty.

Step 5 An action officer is assigned to deal with the Notice. The action officer takes responsibility for ensuring that all appropriate action is taken by the deadline. In particular, the action officer notifies the University Secretary and CIO once the 24 hour point is reached. If the website has not been removed, modified or had access blocked by the time 24 hours has elapsed since receipt of the Notice then the University takes rapid central action to block access to the website, as in Step 4 above.

Step 6 The Chief Information Officer, the Director of IT Infrastructure and the Director of Applications identify where the website is located; in which Head of College/Support Group and School/Administrative Department's area; and who is the website owner.

Step 7 Under 3.2, the relevant Head of College or Support Group, Head of School or Administrative Department and website owner are informed about the Notice and involved in action to remove or modify the website. If the website is in another domain, e.g. EUSA, then the relevant Head of Unit and website owner are similarly informed and involved.

Step 8 The Chief Information Officer informs JANET (UK) about the Notice and that the University is taking responsive action.

Step 9 The website is removed or modified, if necessary with the co-operation of the relevant area.

Step 10 The Director of Communications and Marketing considers what internal and external communications are needed.

Step 11 The action officer ensures that the University Secretary confirms to the police that the website has been removed or modified within the two working days.

Step 12 Disciplinary action is pursued through the appropriate channels, using existing procedures.

Step 13 IS:AD or the relevant School or Department put arrangements in place to ensure that the information is not repeated/remounted on the web and that appropriately robust procedures are in place to ensure the security of machinery and the appropriate mounting of websites.

Step 14 The CIO initiates an investigation into how the incident occurred, to establish what lessons can be learnt.

Step 15 The University formally logs and records the website removal or modification and reports to the Knowledge Strategy Committee and the Central Management Group.

SMW, 28.2.08

Appendix 1 Background Information

1 References

Terrorism Act 2006: http://www.opsi.gov.uk/acts/acts2006/20060011.htm
Explanatory Notes to Terrorism Act 2006: http://www.opsi.gov.uk/acts/en2006/2006en11.htm
Guidance on Notices Issued Under Section 3 of the Terrorism Act 2006, version issued August 2007: http://security.homeoffice.gov.uk/news-publications/publication-search/terrorism-act-2006/2007-05-24-s3-guidance.pdf?view=Binary
University of Edinburgh Computing Regulations: http://www.ucs.ed.ac.uk/EUCS/regs.html

2 Summary

The Home Office website notes that the Terrorism Act 2006 aims to make it more difficult for extremists to abuse freedoms, in order encourage others to commit terrorist acts. The Act creates a number of new offences: acts preparatory to terrorism; encouragement to terrorism; dissemination of terrorist publications; and terrorist training offences. The Act also makes amendments to existing legislation.

This paper focuses on the need for the University to have a protocol to remove or modify offending websites within two working days of receipt of notices which are issued under the Terrorism Act 2006. Such notices would be delivered to the University Secretary in person or to the Secretary's or Principal's Office by recorded delivery.

3 Timescale

The legislation came into force on 30 March 2006, with immediate effect.

4 Background

The Home Office's *Guidance on Notices Issued Under Section 3 of the Terrorism Act 2006* notes that "Section 1 makes it an offence to publish a statement which encourages acts of terrorism or Convention offences" (paragraph 5) and "Section 2 creates an offence of disseminating a terrorist publication. Dissemination includes certain conduct relating to material on the internet. Terrorist publications are publications the content of which encourages people to engage in terrorism, or provide information that could be useful to terrorists." (paragraph 6). Sections 1 and 2 would provide a defence to the University if we can show amongst other things that a "statement or terrorist publication" does not express our views and does not have our endorsement. However, if the University fails to comply with a notice served under section 3 of the Terrorism Act 2006 then, under the legislation, it would be deemed to have endorsed the offending statement or publication and if the University were prosecuted for either the section 1 or 2 offences, it would then be unable to take advantage of the defences in sections 1(6) and 2(9) respectively. The *Guidance on Notices Issued Under Section 3 of the Terrorism Act 2006* also notes that "Section 3 also provides that following service of a notice in relation to a statement, a person is taken as having endorsed any future re-publication of a statement that is the same or to the same effect as the original statement unless they have taken every reasonable step to prevent re-publication and, once aware of the publication, have taken every reasonable step to remove it." (paragraph 41).

The *Guidance on Notices Issued Under Section 3 of the Terrorism Act 2006* notes that "Where there is a possibility the content will be removed voluntarily and there is no suspicion that the potential subject of the section 3 notice is involved in encouraging publication of the material, a voluntary approach to removing the material will be taken rather than using section 3 notices. This is particularly the case where the material breaches the terms and conditions under which a service is provided or run (eg chatroom rules, Acceptable Use Policy)." (paragraph 27). The University's Computing Regulations state that "Users must comply with the provisions of any current UK or Scots law". Any University-hosted website which breaches the Terrorism Act 2006 may be considered to have breached the terms and conditions under which the University provides computing services to its users and an initial approach may therefore be voluntary.

5 University of Edinburgh Computing Regulations

The 16th edition of the University's Computing Regulations gives the University scope to remove inappropriate websites and take relevant disciplinary and legal action:

> "If the UoE suspects any breach or potential breach of the Regulations, it shall have full and unrestricted power to access all relevant computing facilities and files and to take all steps which it may deem reasonable to remove or prevent distribution of any material. UoE may also immediately suspend a user's access to computing facilities pending an investigation by an Authorised Officer or nominee of the University as defined in the relevant Discipline Code. The UoE reserves the right to access or require access to any files held on computing facilities. It may also require that any encrypted data is made available in human-readable form. Any such investigatory action shall not prejudice any final determination of whether a breach occurred."

> "Each user agrees that UoE has the right to take legal action against individuals who cause it to suffer loss or damage, including damage to its reputation, or be involved in legal proceedings as a result of their breach of these Regulations, and to seek reimbursement of such loss, or any associated costs including the costs of legal proceedings."

6 Working Day Definition

In the Terrorism Act 2006, section 3(9) "Working day" means any day other than

(a) a Saturday or a Sunday;
(b) Christmas Day or Good Friday; or
(c) a day which is a bank holiday under the Banking and Financial Dealings Act 1971 (c. 80) in any part of the United Kingdom.

Schedule 1 of the Banking and Financial Dealings Act 1971 (c. 80) lists the following bank holidays

(a) in England and Wales:
    Easter Monday.
    The last Monday in May.
    The last Monday in August.
    26th December, if it be not a Sunday.
    27th December in a year in which 25th or 26th December is a Sunday.
(b) in Scotland:
    New Year's Day, if it be not a Sunday or, if it be a Sunday, 3rd January.
    2nd January, if it be not a Sunday or, if it be a Sunday, 3rd January.
    Good Friday.
    The first Monday in May.
    The first Monday in August.
    Christmas Day, if it be not a Sunday or, if it be a Sunday, 26th December.
(c) in Northern Ireland:
    17th March, if it be not a Sunday or, if it be a Sunday, 18th March.
    Easter Monday.
    The last Monday in May.
    The last Monday in August.
    26th December, if it be not a Sunday.
    27th December in a year in which 25th or 26th December is a Sunday.

For background on "bank holiday" from the Banking and Financial Dealings Act 1971 (c. 80) see:
http://www.statutelaw.gov.uk/legResults.aspx?LegType=All+Legislation&title=Banking+and+Financial+Dealings+Act&Year=1971&searchEnacted=0&extentMatchOnly=0&confersPower=0&blanketAmendment=0&TYPE=QS&NavFrom=0&activeTextDocId=1369155&PageNumber=1&SortAlpha=0