Network Filtering Policy

Document Title: Network Filtering Policy			
Version No.	1.0	Policy Owner	Director, ITDS
Superseded version	N/A	Author Role Title	Director, ITDS
Approval Date	17/09/2019	Approved by	Vice-Chancellor
Effective Date	September 2019	Review Date	2 years

Network Filtering Policy

1. Purpose

1.1 This policy sets out the principles to maintain and support research, teaching and other business activities whilst protecting users, networks and computers from hostile or unwanted network traffic and illegal or other content in breach of the regulations of Teesside University.

2. Scope

2.1 This policy covers all employees, students, Governors, consultants, contractors, volunteers, interns, casual workers, agency staff and self-employed workers working for the University, and all other persons associated with and acting for the University, whether directly or indirectly. This definition includes external members of University Committees, representatives, agents, subsidiaries, individuals appointed as directors of any company, consultants, contractors and partners.

2.2 This policy applies to all communications between the University's networks and the Internet, including web browsing, instant messaging, file transfer, file sharing, and other standard and proprietary protocols. Server to Server communications, such as e-mail traffic, backups, automated data transfers or database communications are excluded from this policy.

3. Policy

3.1 Through the use of firewall and web filtering technologies, the University prevents access to certain categories of websites via its networks, as set out below. The University does this to:

> 3.1(a) protect its users, networks and computers from hostile or unwanted network traffic and illegal or other content where access or attempted access to it would either be unlawful and/or in breach of the regulations of Teesside University; and
>
> 3.1(b) comply with its Prevent Duty for Higher Education Instituions which requires relevant higher education bodies, including Teesside University, to consider the use of web filtering to deny University users access to extremism-related materials.

3.2 The current Content Classification System provided through the University's firewall vendor allows for automatic site blocking based on a range of categories e.g. 'Adult', 'Hacking', 'Extremism'. The list provides an objective categorisation of sites and is actively maintained by the firewall vendor; the University plays no direct role in deciding how individual sites are categorised. The current list of classifications can be accessed here.

3.3 Categories blocked under this policy are:

a) **Adult** - Sexually explicit material, media (including language), art, and/or products, online groups or forums that are sexually explicit in nature. Sites that promote adult services such as video/telephone conferencing, escort services, strip clubs, etc.
b) **Extremism** - Sites promoting terrorism, racism, fascism or other extremist views discriminating people or groups of different ethnic backgrounds, religions or other beliefs.
c) **Malware** - Sites containing malicious content, executables, scripts, viruses, trojans, and code.
d) **Phishing** - Sites that harvest personal information from its users via phishing or pharming.
e) **Essay Mills** – Sites which offer services in support of academic cheating, such as essay writing services

3.4 The University reserves the right at any time to amend, add or delete categories that are blocked under this Policy. In addition to sites identified by the Content Classification System provided through our firewall vendor, the Director of IT and Digital Services (ITDS) may block any site or protocol (set of rules governing the exchange or transmission of data between devices) temporarily and from time to time to protect the University IT facilities and its users from cyber threats such as computer viruses. Sites facilitating the delivery of malicious software (malware), spam e-mail, phishing, computer hacking, Denial of Service (DoS) and use of illegal file-sharing are highly dynamic and volatile in nature and necessitate an ad hoc approach. Sites blocked temporarily will be reviewed and considered for permanent blocking by the Director of ITDS.

3.5 In the interests of academic freedom, and for legitimate research, teaching and learning purposes, it is recognised that staff and students may require access to sites which are currently blocked. The University has a ‘whitelisting’ process detailed below to enable staff and students with legitimate requests to be granted access to websites and online material which have been blocked under this Policy and through the content filtering technologies in force for the duration of their research.

4. Whitelisting Process

4.1 A Whitelisting Request can be raised with the ITDS Information Assurance Team via two channels:

a) An email link on the ‘Blocked Page’, presented on attempting to access a blocked website; or
b) A call to the ITDS Helpdesk.

4.2 All whitelisting requests should be supported by evidence where appropriate e.g. School/committee approval to undertake research.

4.3 Whitelisiting requests relating to a “blocked page” will be security checked both for Malware, and in case it may have been miscategorised by the firewall vendor. If the website is considered to be unsafe and may cause harm to the University network the request will be declined by ITDS and details passed to the requester explaining the decision.

4.4 If the website passess ITDS checks in accordance with para 4.3, the details of the request will be passed to Executive Director of Legal and Governance Services (L&GS) (or nominee) for review and authorisation. In formulating a decision, the Executive Director of L&GS (or nominee) will consider the purpose and legitimacy of the request against the nature and type of site being requested. The decision whether or not to grant access shall be final and made within 14 days from the date of the request. If the request is granted, the decision will be passed to ITDS Information Assurance Team to action.

4.5 Whitelisting will occur on a user basis, so that only the requesting user will be granted access to the website and only for the duration determined by the Executive Director of Legal and Governance Services (or nominee) in response to the request.

Note: If the website has been miscategorised, the site can be Whitelisted by the ITDS Information Assurance Team while the re-categorisation request is made to the firewall vendor.

5. Roles & Responsibilities

5.1 Executive Director of L&GS and Director of ITDS are responsible for the implementation of this Policy.

6. Relationship with Existing Policies

6.1 This policy forms part of the Information Security Management Framework. It should be read in conjunction with the ICT Acceptable Use Policy, Information Security Policy, Research Ethics Policy, and the University Prevent Strategy.

7. Dissemination and Communication Plan

7.1 This Policy will be disseminated through MyComplaince to all staff and made available on the University’s Regulation Repository.