Teaching Intensive, Research Informed

# INTERNET SECURITY POLICY

## 1. Introduction

### 1.1 Purpose and Scope

The University of Bolton has a duty to protect students, staff and visitors who use the University's IT systems and to protect all personal information held in University systems. The University has to ensure that its IT systems are operating effectively, efficiently and securely for the benefit of all stakeholders.

The University also has a duty to comply with all statutory responsibilities laid down in relevant legislation and guidance relating to the use and control of information and Information Technology including, but not limited to:

- Data Protection Act (1998)
- Counter-Terrorism and Security Act 2015
- Regulation Of Investigative Powers Act (2000)
- Freedom Of Information Act (2000)
- Human Rights Act (1998)
- Computer Misuse Act (1990)
- PREVENT Duty guidance (2015)

To meet these objectives effectively, the University IT systems filter or block certain network traffic and content that poses serious risks; the systems and services retain transaction information in log files.

This Internet Security Policy applies to all staff, students, consultants, contractors and collaborative partners of the University.

## 2. Policy statements

2.1 The University filters internet traffic into and out of the University to protect users and systems and to help meet its statutory duties.

2.2 The University IT systems routinely retain transactional information relating to network traffic and internet based communication and this information may be used in diagnostic, preventative or investigative analysis.

## 3. Controls and processes

3.1 The University has the technological capability to filter internet traffic to and from the University network and does so for the following purposes:

- to block malicious email, including email born malware or phishing
- to reduce spam email
- to prevent external IP borne attacks on University systems and users
- to prevent access to sites, IP addresses, content that has been notified by statutory authorities e.g. the Home Office, police
- to prevent malicious use of the Internet e.g. denial of service attacks on external sites
- to protect users and systems accessing and using known rogue websites

3.2 The University filters certain internet web traffic using policy-based access control, by categories, websites and individual pages. Category filters are set to filter web content which may be deemed illegal or extremist by law enforcement agencies, and for which there is no obvious academic profile in the University. In addition, the University utilises other techniques to protect users and systems not documented here for security reasons.

3.3 Web sites are categorised and the filters updated daily via an external service. It is possible that legitimate content may be inadvertently blocked. In such cases a user may appeal in writing or email to the Head of Information Systems and Technology (IS&T) for review of a blocked category or site. The Head of IS&T will make the final decision having consulted as appropriate and secured relevant technical, legal and policy advice.

**3.4 Monitoring**

3.4.1 The University IT systems routinely capture and retain transactional information in computer logs relating to:

- internal networking traffic
- data system transaction
- Wi-Fi connections
- Internet traffic into and out of the University via the Joint Academic Network (JANET)
- e-mail communication
- user login

3.4.2 Much of this data resides in system logs for the purposes of diagnosis, audit and IT performance monitoring. It may be used to investigate incidents or events including security breaches, equipment performance and failures of controls or violations of policy.

3.4.3 Users will be made aware that all internet traffic passing through the University network including email, is traceable through these logs and is retained for the following periods of time:

- Internet traffic up to 12 months
- e-mail up to 5 years

3.4.4 Logged data may be interrogated during the course of disciplinary investigations involving staff and students; access and use are subject to written authorisation by a senior University authority (normally the Vice Chancellor or her/his nominee).

3.4.5 Information in log files is not routinely disclosed to any third party and will be maintained as secure, in-line with data protection policies. However, the University has a statutory duty to co-operate with Law Enforcement Agencies in the course of an investigation, in which case release of information will be sanctioned at the level of Registrar or higher, subject to due process.

## 4. User Behaviour

4.1 Staff, students and all users must adhere to the 'Acceptable Use Policy' and must not engage in any online activity that is deemed illegal or breaches the University's policies or codes of conduct.

4.2 Under the Counter-Terrorism and Security Act (2015) Prevent Duty, the University has a statutory duty to take steps to prevent individuals being drawn into extremism and terrorism. Users must not create, access, transmit or download inappropriate or extremist materials, as defined within the Prevent Guidance (2015), using the University's IT systems or network. The University has a duty to alert and report attempted access to, or dissemination of, such inappropriate material.

4.3 Users must not install or use any device or software on University IT equipment that subverts or bypasses security controls including monitoring and filtering.

4.4 Staff and students must obtain explicit written and specific clearance from the University's Research Ethics Committee before engaging in research with materials on-line that are: highly controversial; sensitive; could expose the individual to harm or undue attention; or potentially breach University policies. For example, political extremist sites, pornographic material, or other material which might involve, or be likely to be inferred to involve criminal activity or activity which is likely to give rise to civil action against the University.

4.5 Where the Research Ethics Committee gives approval for a researcher (including research students) to access sensitive materials on-line, the University has a duty of care to provide a safe working environment. The

Head of School therefore needs to advise the Head of IS&T on access and provide a risk assessment and method statements for the research.

## 5. Related Policies and Procedures

The following policies and procedures are related to the Internet Security Policy:

- Prevent Policy
- Acceptable Use Policy for Students
- Acceptable Use Policy for Staff
- Data Protection Policy
- Processing Your Personal Data
- Code of Practice for Ethical Standards in Research
- Social Media Guidance – Think Before You Write
- Social Media Policy

## 6. Equality Impact Assessment

The University of Bolton is committed to the promotion of equality, diversity and a supportive environment for all members of our community. Our commitment to equality and diversity means that this Policy has been screened in relation to the use of plain English, the promotion of the positive duty in relation to the protected characteristics of race, sex, disability, age, sexual orientation, religion or belief, gender reassignment, marriage and civil partnership, pregnancy and maternity.

| **Internet Security Policy** | |
|---|---|
| Procedure Ref | UoB-ISP2.10 |
| Version Number | 1.0 |
| Version Date | 21/01/2016 |
| Name of Developer/Reviewer | P.O'Reilly/ P.McGhee |
| Procedure Owner (School/Centre/Unit) | IS&T |
| Person responsible for implementation (post holder) | Head of IS&T |
| Approving Committee/Board | Executive Board |
| Date approved | 19/02/2016 |
| Effective from | 19/02/2016 |
| Dissemination Method (e.g. website) | Website |
| Review Frequency | 3 years |
| Reviewing Committee | Prevent Working Group |
| Document History (e.g. rationale for and dates of previous amendments) | |