BLOOMSBURY INSTITUTE LONDON

Internet Acceptable Use Policy

Index

Document Version Control

Committee	Committee Action	Date
SMLT	Approved	7 July 2021
Date in force		**1 August 2021**

The Internet Acceptable Use Policy will be reviewed annually by our Senior Management and Leadership Team (SMLT). Any amendments will be subject to approval by the Senior Management and Leadership Team.

1. Introduction

This policy applies to all Bloomsbury Institute staff (including temporary staff), Student Guild, visitors, contractors, and students who are using our IT facilities and resources and those of Birkbeck[1] College to access the internet. This policy sets out the rules which govern the use of the internet if accessed using our IT facilities and resources and applies therefore to access both on site and remotely. This policy should be read in conjunction with the policies of Birkbeck College. For the purposes of this policy the 'internet' is defined as web services, chat rooms, bulletin boards, newsgroups, peer to peer file sharing and instant messaging software.

This policy has been drawn up within the legislative framework set out in Appendix A and should be read alongside our other key policies (including our Email Acceptable Use Policy[2]) and those of Birkbeck College. Please note that the contents of this policy are not intended to contradict or contravene UK or international law.

2. Purpose

The main purpose of this policy is to set out the rules which relate to acceptable use of the internet if accessed using our IT facilities and resources for the mutual benefit of the organisation and all other users.

This policy:

- reduces online security risks
- guides users about what they can and can't do online
- ensures users do not view inappropriate content
- helps satisfy our legal obligations including those set out in the Prevent Duty Guidance 2015 last revised in April 2021.

3. Scope

This policy applies to any person who uses our IT facilities and services to access the internet. For the purpose of this policy, IT facilities and services include:

- physical and virtual computers (desktops) or servers, and mobile devices
- peripherals such as monitors, keyboards and printers
- computer networks, including wireless and telecommunication networks
- software and data stored on the above

4. General internet guidelines

Use of the internet is monitored for security and network management reasons. We do not provide any guarantee regarding a user's privacy or security with regards to use of the internet when accessed through our IT facilities and services. Users may be subject to limitations on their use of IT facilities.

The Head of IT Services will refer any suspected illegal use of the internet to the Managing Director and Academic Principal for investigation and (where appropriate) action. In the case of usage relating to

[1] We have a service agreement with Birkbeck College whereby all staff and students have access to Birkbeck College's IT resources and facilities.

[2] www.bil.ac.uk/qem/policies/

extremism or terrorism, the suspected illegal use will be referred also to the Prevent Lead or the Head of Governance and Legal Services.

4.1 Acceptable use

IT facilities and services are provided to all users primarily for the Institute's related activities. Personal use of the internet should be limited to 'essential' matters and must not affect the internet service available to other users, e.g. downloading large files and continuous streaming of video and music sites.

Users must always consider the security of the systems and data when using the internet. Users must always comply with the JISC's Acceptable Use Policy (https://community.jisc.ac.uk/library/acceptable-use-policy)

4.2 Unacceptable use

The following constitute unacceptable use of IT facilities and services when accessing the internet [the list is not exhaustive]:

- Unauthorised distribution of login and/or password information, including using or disclosing (without authorisation from the Head of IT Services) another user's login and/or password information.

- Visiting and/or distributing inappropriate content or material [unless permitted on the ground that it comes within the scope of the principle of academic freedom as set out in Regulation 3(e) of our Articles of Association].

- Inappropriate content includes: pornography and obscene or indecent images, racial or religious slurs designed to promote and incite race or religious hatred, content targeting any group with the intention of promoting or inciting hatred, offensive comments in relation to anyone with any of the 9 protected characteristics outlined in the Equality Act 2010, information encouraging criminal skills, websites that are linked to a proscribed terrorist organisation and information that generally promotes or incites acts of violence or terrorism[2,] or materials relating to cults, gambling and illegal drugs. Please note that this list is not exhaustive.

- Making or posting indecent remarks, proposals or materials, including racist or sexist jokes and defamatory comments.

- Any type of illegal or criminal activity.

- Uploading, downloading or otherwise transmitting commercial software or any copyrighted materials belonging to parties outside of the organisation.

- Uploading, downloading or otherwise transmitting commercial software or any copyrighted materials belonging to the organisation unless such is covered or permitted under a commercial agreement or other such licence.

- Unauthorised download of any software or electronic files without any precautionary virus protection measures.

- Intentionally interfering with the normal operation of the network, including the propagation of computer viruses and sustained high volume network traffic that substantially hinders others in their use of the network.

- Monitoring Network Traffic Content or scanning devices connected to the network.

[3] We have a statutory duty to prevent individuals from being drawn into extremism and terrorism, and to report any attempted access to, or dissemination of, extremist material.

- Sending or posting messages or material that could damage our image or reputation.
- Use of IT facilities and services and/or the internet to perform any tasks which may involve breach of copyright law.
- Breach of our Information Control Procedures[4] [Applicable to staff only]
- Breach of our Social Media Communications Policy[5] [Applicable to staff and students]

4.3 Safe use

- Ensure personal login and password details for any IT data systems and personal desktops are kept secure.
- Users should notify IT Services (ITS) immediately of any unauthorised access, or suspicion thereof, to their computer.
- Report any accidental access[6] to inappropriate sites.
- Always logout or lock office devices when finished.
- Check for any required permissions to publish or distribute copyrighted information.
- If, in the course of recognised research or teaching (permissible under UK and international law), users need to access inappropriate content or material as outlined above they should approach the Research Ethics Committee (ethics@bil.ac.uk) for information and support. Without written approval from the Research Ethics Committee to access materials online that are highly controversial or sensitive, users could find themselves in breach of the law.

5. Filtering

Although we do not currently block any sites based on URLs, there is a content filtering for the following:

- Adult/Sexually Explicit Material
- Advertisements & Pop-Ups
- Chat and Instant Messaging
- Gambling
- Hacking
- Illegal Drugs
- Intimate Apparel and Swimwear
- Peer to Peer File Sharing
- Personals and Dating
- Social Network Services
- SPAM, Phishing and Fraud
- Spyware

- Tasteless and Offensive Content
- Violence, Intolerance and Hate

6. Monitoring

IT facilities and services are provided for legitimate business use only. As such, ITS reserve the right to monitor use of the internet, to include:

- The volume of internet and network traffic and internet sites visited.
- The specific content of any transactions if there is a suspicion of unacceptable use.

Current filtering procedures filter default websites [defined within the software] to industry standard. ITS also maintain monitoring logs which are used primarily to produce statistics on the service, and also to investigate any cases of suspected unauthorised use, or illegal activity that are reported. To support trend analysis, daily logs are aggregated into monthly logs. The daily raw log file (which is retained for 180 days) records the following information:

- IP address of requestor
- Time stamp
- Time to download a page
- Status code
- Size
- URL

7. Potential sanctions

Incidents which may be in contravention of this policy (e.g. unacceptable use) will be referred to the Head of IT Services for investigation, and, where appropriate, the Prevent Lead. Investigation of such incidents may require the collection and evaluation of user related activity and evidence.

Depending upon the severity of the potential contravention, the Head of IT Services may refer the issue to the Head of Governance and Legal Services for further investigation and (where appropriate) disciplinary action.

8. Related policies and procedures

- Email Acceptable Use Policy
- Information Control Procedures
- Information Security and Management Policy
- Prevent Policy
- Information Security and Management Policy
- Research Ethics Code of Practice
- Staff Disciplinary Procedure

- Social Media Communications Policy

9. Review

The Internet Acceptable Use Policy will be reviewed annually by our Senior Management and Leadership Team (SMLT). Any amendments will be subject to approval by the Senior Management and Leadership Team.

Appendix A: Legislative Framework for our Internet Acceptable Use Policy

The following list is not exhaustive:

- Communications Act 2003
- Computer Misuse Act (1990)
- Copyright, Designs and Patents Act 1988
- Counter-Terrorism and Security Act 2015
- Criminal Justice and Public Order Act 1994
- Criminal Justice and Immigration Act 2008
- Data Protection Act (2018)
- Equality Act 2010
- Freedom of Information Act (2000)
- Human Rights Act (1998)
- Malicious Communications Act 1988
- Obscene Publications Act 1959
- PREVENT Duty Guidance (2015)
- Regulation of Investigatory Powers Act (2000)
- UK General Data Protection Regulation (2021)