Brunel Email Use Policy

Brunel University London

An ISO/IEC 27001:2013: *Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

Mick Jenkins
Chief Information Security officer

Document History

Version	Author	Comments	Date
V 1.0	Andrew Clarke	Initial Draft	19/03/2018
V 1.1	Andrew Clarke	Format Changes – Strategy & Governance	03/05/2018
V 1.2	Andrew Clarke	Replace references to newsgroup with social networks	18/07/2018
V1.3	Andrew Clarke	Syntax amendments - Head of Infrastructure and Operations	31/07/2018
V1.4	Andrew Clarke	CISA approval (syntax amendments)	07/09/2018
V1.5	Andrew Clarke	InfoSub Committee – Dr Stephen Swift exceptions for legitimate research and teaching for the sending of emails that may breach policy guidelines (p7)	12/02/2019
	Andrew Clarke	Annual review	05/03/2020

Document Approval

The contents of this document are classified as Protect to Brunel University London (BUL) information classification. Proprietary information presented in this document may not be used without written consent from BUL and remains the exclusive property of BUL unless otherwise agreed to in writing.

Owner: Michael Jenkins	Chief Information Security Officer
Signature: MGJ	Date: 12 Feb 2019
Approver: Pekka Kahkipuro	Chief Information Officer
Signature: PK	Date: 12 Feb 2019
Distribution:	

This document requires the approval from BUL as defined in the ISMS Compliance document.

Contents

1. About this document

1.1 Purpose of Document

The purpose of this policy is to outline the acceptable use of electronic mail within Brunel University London, and while using email and allied facilities using an account provided by Brunel University London or managed on behalf of Brunel University London by a third party. It should be clear that policy is not immutable: in particular, in a field such as this, where emerging technology is interwoven with emerging law, we must be able to react to changes. In the formulation and continuous reformulation of policy, we must be guided by advice from within Brunel University London and beyond, taking due consideration of legal precedent, and having due regard to the practices and experiences of other HE institutions.

Please refer to Brunel University London ISMS Document *BUL-GLOS-000 - SyOPs Glossary of Terms* for the glossary of terms, acronyms and their definitions for the suite of Brunel University London ISMS documentations.

1.2 Responsibilities

Table 1 – responsibilities

Title / Role	Description
Cyber & Information Security Manager	Is responsible for maintaining the Email Use Policy and to ensure that the Policy continues best practice and ensuring compliance with legislative and regulatory requirements.
All Users	It is the responsibility of all users of the Brunel University London's IS services to read and understand this policy. This policy may be updated from time to time, in order to comply with legal and policy requirements.

1.3 ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	SOA – Number A8 – Asset Management
ISO 27001:2013 Conformance Control	Information Classification Objective A.8.1.3 Acceptable use of assets

1.4 Scope

This Policy sets out the accepted use and management of Brunel University London's email services and facilities: in conjunction with other policies of good practice, it will enshrine good management practice and will help to ensure that Brunel University London is compliant with all relevant legislation and accepted good practice and that it adheres to the Seven Principles of

Public Life in the United Kingdom (popularly known as the Nolan Principles)[1] and to high standards of ethical value, in its management of network computer accounts.

This policy applies to employees, contractors, consultants, temporaries, other workers, students and affiliates at Brunel University London, including all personnel affiliated with third parties.

This policy applies to all equipment that is owned or leased by Brunel University London and to the use of information, electronic and computing devices and network resources to conduct Brunel University London business or interact with internal networks and university systems, whether owned or leased by Brunel University London, the employee, or a third party. It also extends to information held on behalf of third parties and partners.

This policy also applies when using your own device to store, access or process information on Brunel University London Information Systems.

This policy applies at all times when using Brunel University London information Systems and not just during your normal working hours.

All employees, contractors, consultants, temporaries, other workers, students and affiliates at Brunel University London and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Brunel University London policies and standards, and local laws and regulation.

Electronic mail which passes through accounts provided by the University but managed on behalf of Brunel University London by a third party is deemed to fall within the scope of this Policy with the same underpinning principles as for locally-managed mail.

This Email Use Policy is taken to include the JISC Acceptable Use Policy and the JISC Security Policy published by JISC (UK)[2], the Combined Higher Education Software Team (CHEST) User Obligations, together with its associated Copyright Acknowledgement, and the Eduserv General Terms of Service.

The University also has a statutory duty, under Section 26 of the Counter Terrorism and Security Act 2015, termed “PREVENT”. The purpose of this duty is to aid the process of preventing people being drawn into terrorism.

[1] https://www.gov.uk/government/publications/the-7-principles-of-public-life/the-7-principles-of-public-life--2
[2] See http://www.ja.net/documents/publications/policy/aup.pdf

2.0 Email Use Policy

When using University resources to access and use email, users must realise they represent the University. Whenever employees state an affiliation to the University, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the University".

2.1 Unacceptable email practices:

- Automatic forwarding of emails from a University owned email account to an external email address, be it a private address, an address of a public service or of a third party unless an approved exception is authorised by the CISO.
  Such an exception will only be granted for clear and compelling business reasons, and where all alternatives have been considered carefully and proved inappropriate
- Sending or forwarding any University Confidential information to your personal communication systems (such as instant messaging, email, video communications), or use such an account for Brunel University London business.
  If you have a requirement to work from home you should use Brunel University London Office365 facilities or request the approved remote working solution from your local IT Service Desk
- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam)
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages
- Unauthorised use, forging or tampering of email header information by any user for the purposes of personation, deception or other action unnecessary for the free flow of primary-purpose mail is deemed to be unacceptable use of a mail account
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies
- Creating or forwarding "chain letters", "Ponsi" or other "pyramid" schemes of any type
- Use of unsolicited email originating from within Brunel University London's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Brunel University London or connected via Brunel University London's network
- Posting the same or similar non-business-related messages to large numbers of Social network sites (spam)
- Sending unsolicited “nuisance” emails
- Sending email messages that could be construed as harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, disability or religious or political beliefs
- Forwarding chain and spam communications
- Sending email messages containing University Confidential information (e.g. Student or staff personal information or financial data) outside of the University unless encrypted by

a product validated by University IS (ask your Cyber & Information Security Officer for the current products validated for the use within University)

- Sending of email messages containing unacceptable content:
  Examples of unacceptable content include:
  - Sexually explicit messages, images, cartoons, or jokes
  - Unwelcome propositions, requests for dates, or love letters
  - Profanity, obscenity, slander, or libel
  - Ethnic, religious, or racial slurs
  - Political beliefs or commentary

  The sending of emails for legitimate research and teaching may involve the sending of unacceptable content and is provisionally exempt from this Policy control.

- Opening suspicious emails which may introduce malicious software or trick you into giving up confidential information (phishing) e.g. your password, username or banking details. This applies to emails from unknown sources, or unexpected communications from known sources. You must immediately report any suspect electronic communications to the IS Service desk or your local IT Service Desk
- Postings from a Brunel University London email address to social networks without a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Brunel University London, unless posting is in the course of business duties

Brunel University London may apply sanctions to the use of any email account connected with any person under suspicion of such activities listed above, and may pursue such a person through Brunel University London disciplinary process and/or legal procedures as appropriate.

2.2 Each user of email at Brunel University London has a duty of care:

- to ensure that appropriate and proper email use and management is practised at all times
- to understand all personal and group responsibilities with regard to email use and management
- to maintain current awareness of policies, practices, threats and problems relating to email at (and where relevant, beyond) Brunel University London
- to maintain up-to-date knowledge of Brunel University London’s preferred messaging software as it evolves, to take full advantage of its facilities to aid the use, management, storage and retrieval of messages, and likewise to take full advantage of other facilities of the said messaging software (in calendaring, task management, etc.), to enhance the efficiency and productivity of Brunel University London in the transaction of its business
- to be responsible and accountable for the email sent from any email account issued to that user or for the use of that user
- to ensure only correct recipients are included and that auto-complete recipients are selected correctly
- to take care before using “Reply All” to email as this can generate very high levels of unnecessary traffic, or can lead to the dissemination of University Confidential information to recipients who do not have a legitimate reason to see it. Only use “Reply All” if every person copied into the email needs to receive it