
	<b>BRANDEIS UNIVERSITY POLICE DEPARTMENT</b>  <b>EMAIL &amp; INTERNET USAGE</b>	
<b>Policy Number:</b>	<b>2.5</b> <span style="float: right;">AGE: 1 of 4</span>	
<b>Policy Type:</b>	<b>RULES AND REGULATIONS</b>	
<b>Issue Date:</b> 10.29.2021 <b>Review Date:</b> 6.12.2024 <b>Revised:</b> 06.12.2023	<b>Issuing Authority:</b>  <b>Chief Matthew T. Rushton</b>	
<b>Accreditation Standards (6<sup>th</sup> Edition)</b> <ul style="list-style-type: none"> <li>● New</li> <li>● Revised</li> <li>● Amended</li> </ul>		

**I. PURPOSE**

The Brandeis University Police Department provides email service and internet access to conduct department business. The guidelines in this section are not exclusive. They provide a general framework of prohibited and acceptable email and internet use.

This section applies to all employees and their access to the internet while on department equipment or while on-duty and their use of Brandeis email by any means.

**II. ALL EMAIL AND INTERNET COMMUNICATIONS MUST BE PROFESSIONAL, APPROPRIATE, AND LAWFUL**

- A. All email communications and internet use must comply with department and Brandeis policies on professionalism and harassment in the workplace.
- B. All internet use on department computers must comply with all laws and policies. This includes policies on privacy issues, any release of confidential, sensitive, or classified information, or information exempt from public disclosure.
- C. Employees will use email signatures consistent with Brandeis Brand Guidelines. Email signature templates and instructions are available on the Brandeis website.

**III. EMPLOYEES WILL NOT SEND CRIMINAL JUSTICE INFORMATION (CJI) VIA EMAIL WITHOUT ENCRYPTION**

- A. Employees may only send encrypted emails containing CJI to recipients that are members of a Criminal Justice Agency and are allowed to receive CJI information.
- B. Examples of common CJI Data include:

- WACIC/NCIC hits
- SID number
- FBI number
- DOL photos obtained via ACCESS (OMNIXX)

**IV. EMPLOYEES WILL READ EMAIL AT LEAST ONCE PER SHIFT AND RESPOND APPROPRIATELY**

- A. Employees are not required to read or respond to email when off-duty or during a system outage or technical failure that prevents the receipt or sending of email.
- B. Unless off-duty, employees will respond to emails no later than 24 hours after receipt, or sooner if required by the subject matter.
- C. Employees upon arriving at work have the responsibility to read department emails within the first hour of their shift - ***in most cases the recipient shall receive a reply email indicating acknowledgment of the email.***
- D. Emails classified as High Importance are marked with a yellow Google Star and include the following subjects:
  - Command staff communications
  - Directives
  - Special Orders
  - Training Digests
- E. Employees will acknowledge calendar invites by accepting (check YES) or rejecting (check NO) in a timely manner. If an employee rejects a calendar invite where attendance is mandatory, they shall immediately notify the sender and give a reason for the rejection.
- F. All other emails that are job-related, time-sensitive, and mandatory for the recipient
  - *These include subpoenas, wanted bulletins, information bulletins, investigative follow-up requests, statement requests, pre-trial discovery requests, and seizure hearing notices.*

**V. EMPLOYEES WILL ACTIVATE AUTOMATIC EMAIL REPLIES FOR EXTENDED ABSENCES**

- A. Employees will activate their email Automatic Replies (Out of Office) in Google when they expect that they will be unable to respond to email for a period that exceeds 7 business days.

**VI. EMPLOYEES MUST USE CAUTION WHEN OPENING EMAIL ATTACHMENTS**

- A. Employees may contact Brandeis ITS if they have questions about an email attachment. Due to the risk of computer virus attacks, employees should not open email attachments from an unknown source.

**VII. EMPLOYEES WILL NOT USE DEPARTMENT EMAIL, INTERNET, COMPUTERS, CELL PHONES OR ELECTRONIC DEVICES TO CONDUCT A PERSONAL FOR-PROFIT BUSINESS**

**VIII. EMPLOYEES WILL NOT USE DEPARTMENT EMAIL, INTERNET, COMPUTERS, CELL PHONES OR ELECTRONIC DEVICES TO REVIEW PERSONAL INVESTMENTS OR TO TRANSACT ANY INVESTMENT BUSINESS**

- A. These types of transactions include trading in stocks, bonds, or mutual funds.

- **Exception:** Employees may conduct infrequent, brief checks of their investments in the Brandeis Retirement Compensation Program since this is a Brandeis-sponsored and maintained program.

**IX. EMPLOYEES WILL NOT USE DEPARTMENT EMAIL, INTERNET, COMPUTERS, CELL PHONES OR ELECTRONIC DEVICES TO PARTICIPATE IN ANY CAMPAIGN FOR ELECTED OFFICE OR FOR ANY OTHER POLITICAL ACTIVITY.**

- A. This includes a prohibition on making any campaign contributions via a credit card and using a department computer to do so. Similarly, employees may not "lobby" elected officials through department computers.

**X. EMPLOYEES WILL NOT USE DEPARTMENT EMAIL, INTERNET, COMPUTERS, CELL PHONES OR ELECTRONIC DEVICES TO ENGAGE IN DEMEANING OR DEFAMATORY CONDUCT.**

- A. Examples of such prohibited activities include knowingly accessing pornographic materials or sites that promote exclusivity, hatred, or positions that are contrary to the Brandeis values on cultural diversity.
- B. If an employee accidentally accesses a website that contains pornographic, sexually explicit, inappropriate, or illegal materials, they must immediately leave the site and notify a supervisor. The information regarding the inadvertent access shall be recorded via an email to the Chief of Police.

**XI. EMPLOYEES WILL NOT ACCESS SITES THAT INCUR A COST TO THE DEPARTMENT WITHOUT PRIOR SUPERVISOR APPROVAL**

**XII. EMPLOYEES WILL NOT KNOWINGLY ACCESS OR COMMUNICATE ANY MATERIAL OF AN OBSCENE, HARASSING, DISCRIMINATORY OR DEROGATORY NATURE**

- A. Examples of such material include sites or email containing racial or sexual slurs or jokes, or containing harassing, intimidating, abusive, or offensive material to or about others.
- B. Certain Assignments May Require Access to Sensitive Sites
  - The department recognizes that certain employees, such as detectives, may have a legitimate business purpose for accessing sites and information otherwise considered inappropriate or illegal.
- C. If employees need to access such "sensitive sites", employees will abide by the following:
  - Employees accessing such sites should exercise courtesy to others that may be present when doing so. This may include closing the door, turning the screen away, or notifying other employees beforehand.