Effective Date: **September 1, 2017** Revised: **August 3, 2018**

POLICY

INFORMATION MANAGEMENT, PRIVACY AND SECURITY, STUDENT LIFE

Digital Privacy Statement

RESPONSIBLE OFFICE

Information Services and Technology

This Digital Privacy Statement explains information gathering and use practices for websites on the domain, www.bu.edu, and Boston University's other digital properties, such as BU mobile applications (each a "Site" and, collectively, the "Sites"). The Sites are controlled by Trustees of Boston University (the "University"). The University is committed to the online privacy of its visitors to and users of the Sites.

The types of information that the University collects may vary depending on the Site or application. As a result, if a Site has its own privacy statement posted, such privacy statement supersedes this Digital Privacy Statement to the extent that it conflicts.

Related BU Policies

The University maintains other policies which relate to this topic, including but not limited to:

- Conditions of Use and Policy on Computing Ethics, which applies to the acceptable use of the University's computing facilities,
- Policy on Network Security Monitoring, which describes the technologies and practices used to detect and prevent network intrusion,

- Information Security Policy, which sets administrative, technical, and physical safeguards for faculty, staff, and students who collect, store and use Sensitive Information for the University's business and research purposes, and
- Gramm-Leach-Bliley Act Procedures, which require the institution to maintain an information safeguarding program.

Information Collection & Use

Personal Information

It is essential and necessary for Boston University to collect, process, use, and/or maintain personal information of visitors to the Sites, including students, faculty, staff, alumni, donors and members of the public (each a "Visitor" and, collectively, the "Visitors"), to ensure the functionality of the website, to achieve its charitable and educational mission, and to promote engagement with and giving to Boston University.

What Personal Information Is Collected?

Boston University may request and collect personal information from a Visitor if, for example, the Visitor uses a Site to ask a question, requests to be contacted, requests information for a particular program or activity, signs up for a mailing list, requests access to a protected portion of a Site, submits a form, or makes a payment. The University will also collect personal information about visitors' website use when visitors submit forms, through cookies and server logs, which track the IP addresses of visitors to the Sites and the pages they visit (see the section on Information Gathered Automatically, below).

Other than as described herein, the University does not collect personal information about Visitors when they visit the Sites unless they voluntarily provide that information.

Information Gathered Automatically

When a Visitor visits a Site or requests access to a protected portion of the Site, the University may collect and store digital information sent by the Visitor's web browser, such as IP addresses (i.e., the internet address of the Visitor's computer or device), geolocation, the web browser used for the connection, the device operating system, unique device identifiers, and

other digital property, such as pages visited, length of visit, and terms searched. When a Visitor submits a form via a Site, the University may capture and store the Visitor's IP address along with other information submitted to the University on the form. Otherwise, the University does not link IP addresses or cookies to any other Visitor personal information. In connection with protecting the University's electronic assets, the University routinely monitors its network for signs of malicious activity. While the University may investigate malicious activity, the University does not store Visitor personal information related to normal use of its network other than as described in this Statement and the Policy on Network Security Monitoring.

Cookies

In addition, the University uses cookies, which are text files placed on Visitor devices to evaluate usage patterns, so that the University can improve both content and distribution. The information can also be used to establish continuity between requests, to personalize a site to a Visitor's preferences, to authenticate a Visitor's log-in, to analyze web traffic, to monitor and ensure the security of the network, and to help diagnose problems with the University's servers. Visitors may refuse the use of cookies by selecting the appropriate settings on their browsers; however if the settings are adjusted, a Visitor may not be able to use the full functionality of the Sites.

Functional cookies

Visitors are sometimes requested to sign-up or log-in in order to use some of our online services.

When a Visitor enters their username and password, a cookie may be set identifying them as a logged-in user. This cookie is removed either when they log out, or when they have not visited the site for some time and their login expires. These systems are typically those that deal explicitly with personal data, transactions, purchasing or borrowing.

Though this cookie will identify the Visitor as a specific person on the system, the University does not pass any information to market research companies, advertisers or other third parties.

Web Statistics and Page Sharing

Many Sites use Google Analytics, which is a web analytics service provided by Google, Inc. ("Google"). Google Analytics uses persistent cookies to analyze how Visitors use a site. The information generated by the cookie about a Visitor's use of a Site (including the Visitor's IP address) will be transmitted to and stored by Google. Google will use this information for the purpose of evaluating the Visitor's use of the Site, compiling reports on Site activity for the University and providing other services related to website activity and internet usage.

Google may also transfer this information to third parties where required to do so by law, or where the third parties process the information on Google's behalf. Google will not associate the Visitor's IP address with any other data held by Google.

By using the Sites, each Visitor consents to Google processing of data about the Visitor in the manner and for the purposes set out above. Please visit the following pages for more information about Google Analytics Terms of Service and Google's Privacy Practices.

Information Security

The University has implemented reasonable physical, technical, and administrative procedures to safeguard and secure information it collects online against unauthorized disclosure, loss, or misuse, in accordance with the Data Protection Standards Policy. Under that Policy, the University has classified data according to its sensitivity, and set requirements for protection accordingly.

The University cannot provide an absolute guarantee as to the security of any information transmitted through its website or digital properties.

Digital Advertising

The University may contract with third-party vendors to show University advertisements on websites and digital properties that are not controlled by the University. The University and third-party vendors with whom the University contracts may use cookies and web beacons to serve ads based on a Visitor's prior visits to the Sites and to assess the effectiveness of those ads.

In addition, the University may allow prospective students and others to provide their personal contact information to the University through these digital ad platforms. The University treats

such information in accordance with this Digital Privacy Statement.

Retention of Information

The information collected through the Sites is retained in accordance with the University's Record Retention Policy and the Policy on Network Security Monitoring.

Third Party Websites

The Sites may link to or embed content from websites that are not controlled by the University ("Third Party Sites"). The University is not responsible for the privacy practices or content of Third Party Sites.

Children's Privacy

The Sites' content is not intended to attract children under 13 years of age and the University will not knowingly collect personal information from children under 13 years of age. If a Visitor is under 13 years of age, the Visitor should not use the Sites.

Acceptance of this Digital Privacy Statement

The University assumes that all Visitors to the Sites have reviewed the Digital Privacy Statement, as it may be modified and updated from time to time, and agree to its contents. If a Visitor does not agree with the Digital Privacy Statement, such Visitor should refrain from using the Sites.

Changes to this Digital Privacy Statement

The University may modify this Digital Privacy Statement. All changes will be made directly to this web page and will be effective on the date posted.

How to Contact Us

Questions about this Statement should be directed to Information Security, buinfosec@bu.edu.

END OF POLICY TEXT

Additional Resources Regarding This Policy

Related Policies

- Data Protection Standards
- Sensitive Data Incident Response
- FERPA Policy
- HIPAA Policy
- Access to Electronic Information Policy
- Conditions of Use and Policy on Computing Ethics
- Network Security Monitoring Policy
- Information Security Policy

- Listing of related BU TechWeb Policies

Related Guidance Documents

Data Use Guidelines: Use of Student Data for Upload to Third-Party Marketing and Matching Platforms

Related BU Websites

- Privacy at Boston University
- Techweb
- Information Security

Categories: Campus Visitors, Information Management, Privacy and Security, Student Life, University Policies Affecting Student Life Keywords: compile, digital privacy statement, gather, identity, information management, privacy, privacy disclaimer, privacy policy, privacy procedure, privacy statement, protect, security