Purpose

To provide guidance on how to successfully send bulk emails either from lehigh.edu email accounts or from 3rd party vendors.

Scope

This policy applies to all Lehigh University departments and the staff and faculty within those departments as they enter into contracts and agreements with 3rd party vendors.

Sending bulk email from lehigh.edu accounts

Lehigh University is a G Suite institution and we use Gmail as our email solution. Gmail places limits on the number of emails that can be sent per day from an individual Gmail email account. Those limitations can be found here: https://support.google.com/a/answer/166852?hl=en.

An alternative approach that can help get around email limitations for individual accounts is to use Google Groups to send emails. Google Groups has options for setting up both simple email mailing lists - https://support.google.com/a/answer/9400082 or more advanced groups that support message moderation, email subscription settings, and message archiving - https://support.google.com/a/answer/9400060.

Sending bulk email from a 3rd party vendor

Another alternative is to partner with a 3rd party bulk email provider in order to distribute emails on behalf of Lehigh University. This document outlines the specific guidance that should be followed if you are using a 3rd party bulk email provider or if you are working with any 3rd party vendor that wants to send email on behalf of Lehigh University.

Lehigh University cannot add the vendor to the Sender Policy Framework (SPF) record. Every vendor asks us to do this but we cannot accommodate those requests because of limitations to the number of characters we can have in the SPF record.

Please follow these guidelines in order to ensure that emails sent by a 3rd party vendor on behalf of Lehigh University are received as expected:

1. If you are using the vendor for the first time, Submit a help request to whitelist both the IP addresses and sender email to ensure that the emails are not marked as SPAM. This process can take up to 24 hours to complete so please put in the request as soon as possible.
2. In order to avoid emails being marked as suspect, never use specific names of individuals or departments in association with an email address that is not their Lehigh email address. For example: Sending a message from the Lehigh University President

or Lehigh University Admissions with any sender email address other than the president or admissions lehigh.edu email address will be flagged as suspect. This is intentional to protect those individuals and offices from spoofing as they are often targets of those types of attacks. LTS recommends working with us to come up with a sender name that will not be marked as suspect and to re-use those names so that the Lehigh Community gets used to seeing those senders and knowing that the emails are legitimate. An example would be using OIRSA Official Survey as the sender title for all surveys that are sent from the Lehigh Office of Institutional Research & Strategic Analytics. The signature within the actual email can be signed by any office or individual.

3. Send a test message with the exact content to see how it looks. That will alert you to issues like links that cause problems, or incorrect formatting. Have someone else proofread your message before you send it to 1000's of people.

Review

This policy should be reviewed annually and modified if necessary.

Compliance and Enforcement

This policy will be enforced by the Library & Technical Services (LTS) CTO

Referenced Documents