ADMINISTRATIVE POLICY

Policy Type:	Jackson College Office 365 Policy
Policy Number:	1602
Date Adopted:	1/11/12
Version:	1.0
Review Cycle:	Annually
Date Last Reviewed:	07/16/2016
Office Responsible:	Information Technology
Reviewing Committee:	Measurement, Analysis, & Knowledge Management
Related Policies:	Records Retention Policy. Information Security
Related Laws:	NA

Purpose:
The purpose of this policy is to ensure that the email/collaboration system used by the college community supports academic achievement and business functions to their fullest capacity.

Scope:
This policy applies to all users of the Jackson College Office 365 system (O365).

Definitions:
Electronic Mail (Email) System: The software and hardware used to support the transmission of email messages within and outside the JC network, including traffic over the Internet.

Folder: A subdivision of a user's mailbox, which is used to sort messages according to the message's status (Inbox, Sent Items, Deleted Items) or subject matter (user-defined folders).

Inbox: The folder in a user's mailbox that receives and temporarily holds new messages.

Mailbox: A message repository assigned to an individual user. A mailbox contains multiple folders that are either system-assigned (the Inbox, Sent Items, and Deleted Items), or are user-defined.

Message: An individual document created by or received through the O365 system that resides in a user's mailbox.

Third Party: Any person, company or service who has access to the 0365 system who is not affiliated with JC.

User: An authorized user of the O365 system; either a JC employee, JC Student or third party.

Personal electronic device or account: Includes, but is not limited to, a personally owned, cell phone, smart phone, jump/flash drive, computer, notebook, and personal e-mail account (ex. Yahoo, Hotmail).

JC issued electronic device or account: Includes, but is not limited to, JC issued cell phone, smart phone, jump/flash drive, computer, notebook, and e-mail account, or any electronic device or account paid for by JC funds.

JC data: Any electronic data that is created in the course of conducting JC business on either a personal electronic device or account or a JC issued electronic device or account.

Archive: Saving data contained in messages so it can be accessed quickly at a later date.

Attachment: An electronic file(s) sent along with a message. Very large attachments may cause the email users mailbox to exceed its quota or be rejected by the senders/recipients email server. (see Message Size Restrictions)

SPAM: Unsolicited bulk email sent to a large number of email addresses. May also be referred to as junk-email.

Blacklisting: Systems put in place to block messages considered SPAM.

Mobile Device: For the purpose of this policy, a mobile device is defined as any mobile technology used to connect to the O365 system data (example: smartphone, iPad).

Policy Statement:

Certain limitations and guidelines are set forth in order to ensure that the employee email is being used to support business functions and academic achievement. Responsibility is placed on the users of the system to appropriately manage and maintain the information communicated via email.

JC considers email to be primarily a communications system. Although some email messages are records of JC business and evidence of business decisions, the email system itself is not the appropriate place for long-term storage or archiving of important electronic records.

Electronic Correspondence

Employees must use their College e-mail address for all College business. Information Technology does not recommend email forwarding. Email forwarding may cause security and legal issues. Some of those threats may include:

- Intentionally forwarding email to a service on the internet that is no longer controlled by IT, could be putting the institution's data at risk. Sensitive information is no longer under the institution's control. See Information Security Policy.

Message Retention Limits

It is the responsibility of each employee to ensure that records are retained according to JC retention policies, in an appropriate format, and that records of JC business are not destroyed due to mismanagement or neglect.

Email Archiving

JC employees are encouraged to archive their email by completing a data back-up to a .pst file. IT does not have the ability to retrieve archived data. See below for email system backup for disaster recovery purposes.

E-Mail System Back-up

Office 365 System back-up is defined by Microsoft licensing and may vary based on terms of the agreement.

Messages that have been saved to a separate network drive (G:, Q:) are backed up daily and may be recovered through normal file recovery processes. Users are encouraged to store business related files in these network folders.

Using JC O365 System on College Owned and Personal Devices

This section refers to JC Employees using a mobile device to access O365.

JC is under no obligation to allow employees to use personal devices to access its institutional O365 system. Allowing such access is a convenience to the employee. JC may withdraw its consent to such access at any time without notice.

JC employees are responsible for preventing unauthorized access to JC's data and information on any device. Devices must install security measures such as password protection in order to connect with the O365 system. Those that do not have security measures in place may access email on their device using Outlook Web Access on their internet browser.

Human Resources may direct IT to remove JC data from a personal device upon termination of employment. If a personal or JC owned device is lost or stolen, Human Resources and the employee will determine if the data should be removed from the device. In all cases the device would likely be reset to its original factory settings and all personal information would be lost.

Employees that believe the data on their device could be compromised due to loss, theft, or an operating system hack, should notify Human Resources immediately.

IT has not acquired the technical resources to access or recover data on mobile devices and has not been directed to do so at this time.

Change Log:

Date of Change	**Version**	**Description of Change**	**Responsible Party**
01.11.2012	1.0	New Release	J. Dobbs
07.16.2016	**2.0**	**Review**	**J. Dobbs**