SECONDARY EDUCATION

OFFICE OF POSTSE

- Searches for records in electronic form should include searches of all relevant mobile devices, hard drives, network drives, offline electronic folders, thumb drives, removable drives, records stored in the cloud, and archive files, including, but not limited to, backup tapes. Do not time stamp or modify the content, the create date, or the last date modified of any record and do not scrub any metadata. Electronic records should be produced in native format. For e-mails, please place responses in one .pst file per employee. For .pdf files, please provide searchable file format and not image file format.
- All email and social media searches should be conducted by the agency's information technology department, or its equivalent, and not by the individuals whose records are being searched. Please provide the name and contact information of the individual(s) who conducted the search, as well as an explanation of how the search was conducted.
- To the extent practicable, please produce all records in a searchable electronic format and not hardcopies. Should you have any questions about the method or format of production please contact the undersigned to coordinate.
- The only applicable privilege is attorney-client privilege. A log of all such records, describing in detail the contents of the record and the grounds for the claimed privilege.

II. Transcribed Interviews

Please make the following individuals available for transcribed interviews:

1. Gene D. Block

2. A duly authorized corporate designee to testify regarding (a) policies regarding free speech, free inquiry, and the First Amendment; (b) the contents, history, and application of the Code; (c) policies regarding faculty discipline for classroom-related conduct; and (c) all specific cases of faculty discipline from January 1, 2016 to the present.

3. [redacted]

4. [redacted]

5. [redacted]

6. [redacted]

This investigation will be conducted by the Department's Office of the Postsecondary Education, with support from the Office of General Counsel. Your legal counsel will be contacted by Paul R. Moore, the Office of the General Counsel's Chief Investigative Counsel, to schedule the transcribed interviews, and by the Office of the General Counsel's E-discovery attorney, Kevin Slupe, to arrange for record transmission.

June 23, 2020

EXHIBIT A

RECORD PRESERVATION REQUIREMENTS

This investigation requires preservation of all information from your institution's computer systems, removable electronic media, filing systems, and other locations relating to the matters that are the subject of the Notice of Investigation. You should immediately preserve all data and information about the data (i.e., backup activity logs and document retention policies) relating to records maintained in the ordinary course of business and that are covered by the Notice of Investigation. Also, you should preserve information available on the following platforms, whether in your possession or the possession of a third party, such as an employee or outside contractor: databases, networks, computer systems, including legacy systems (hardware and software), servers, archives, backup or disaster recovery systems, tapes, discs, drives, cartridges and other storage media, laptops, personal computers, internet data, personal digital assistants, handheld wireless devices, mobile telephones, paging devices, and audio systems (including voicemail). You should also preserve all hard copies of records regardless of location.

The laws and rules prohibiting destruction of evidence apply to electronically stored information in the same manner that they apply to other evidence. Accordingly, you must take every reasonable step to preserve relevant records. "Reasonable steps" with respect to these records include:

- Notifying in writing all potential custodians and IT personnel who may have relevant records of their preservation obligations under this investigation.
- Discontinuing all data and document destruction policies.
- Preserving all metadata.
- Preserving relevant records and/or hardware unless an exact replica of the file (a mirror image) is made.
- Preserving passwords, decryption procedures (and accompanying software), network access codes, ID names, manuals, tutorials, written instructions, decompression or reconstruction software.
- Maintaining all other pertinent information and tools needed to access, review, and reconstruct necessary to access, view, and/or reconstruct all requested or potentially relevant electronic data.

You have an obligation to preserve all digital or analog electronic files in electronic format, regardless of whether hard copies of the information exist, with all metadata. This includes preserving:

- Active data (i.e., data immediately and easily accessible today).
- Archived/journaled data (i.e., data residing on backup tapes or other storage media).
- Deleted data (i.e., data that has been deleted from a computer hard drive but is recoverable through computer forensic techniques).
- Legacy data (i.e., data created on old or obsolete hardware or software).