RHODE ISLAND COLLEGE **OFFICIAL GUIDELINE**	***Disposal of Confidential Records***	**EFFECTIVE DATE:** *2014/03/24* **RELATED TO:** *College Records*
RESPONSIBLE OFFICE: *Office of Information Services*	**GUIDELINE OWNER:** *AVP Information Services*	**SUPERSEDES:** *College Policy Concerning the Disposal of "Sensitive Information" (1998/04/10) – not published online*

Disposal of Confidential Records

A. Confidential records - generally

1. Any printed or electronic document that contains confidential information concerning an individual should be destroyed in an appropriate fashion. Confidential information includes, but is not limited to, social security numbers, salaries, medical information, grades, and test scores. If any such information can be personally identified by name, it should be destroyed in an appropriate fashion. Personal notes, graded exams or written work, personnel forms, medical records, and the like should be disposed in a way that does not compromise the private nature of the information contained therein.

B. Paper Records

1. The most practical way of destroying such confidential information is by shredding the material. Offices or departments that must shred large amounts of information on a regular basis are advised to purchase appropriately sized shredders. A heavy duty shredder is located in Office Services in Craig-Lee Hall. This is available to the entire college community.

2. Chairs or directors of all offices that do not have immediate access to a shredder should develop procedures to secure confidential material in their work area until they are able to dispose of it appropriately. At that time, the material should be taken to Office Services for shredding. Office Services personnel will be available to provide directions on the use of the equipment, but because of privacy concerns, each office must shred its own material.

C. Electronic Records

1. Confidential records may be stored on machine-readable formats such as hard disk, floppy disk, back-up tapes, USB flash drives, CD/DVD or other portable storage medium. Special destruction methods have been devised for these formats:

   a. Hard disk – User Support Services can provide a data wipe that meets Department of Defense standards; it can also physically drill the disk, rendering it unusable.

   b. Back-up or VHS tapes – incinerate or contract with a vendor to shred. This media can also be degaussed with an NSA/CSS-approved degausser.

   c. USB flash drive – crack open drive, throw away casing materials, destroy the chip with a drill or hammer.

   d. CD/DVD – Many industrial-strength shredders will shred a CD/DVD.