



**INFORMATION TECHNOLOGY SERVICES
POLICIES AND PROCEDURES**

Policy Name: Resource Owner Policy **Policy Number:** ITS-GEN-007

Subject: Access & Changes to Digital Resources **Initial Effective Date:** 1/31/06

Approval: C. Durbin **Last Revision Date:** 10/06/2006 AJH

I. DESCRIPTION:

This Policy describes circumstances in which it is permissible to make changes to digital resources that are assigned a principal “owner”, or to the access rights for those resources.

II. PURPOSE:

This Policy’s purpose is to preserve the integrity of various degrees of data privacy in the Albright digital workplace.

III. SCOPE:

This Policy applies to all Albright employees and students, and to all digital resources assigned to a particular student, employee, department, committee, club, or other formally recognized group of employees or students. A digital resource is defined as including, but not limited to, accounts, access rights, shared space, data files, email, voice messages, or any other digitally stored information, or means of access to same.

IV. RESPONSIBLE PARTIES:

The IT Services department, as the only party with the potential to access any and all digital resources, is responsible for protecting the access rights of all resource owners by following the procedures outlined herein.

V. REFERENCES:

VI. PROCEDURE:

Before making any changes to a personally assigned digital resource (such as an interactive user account or shared folder), IT Services is required to acquire the written permission of the assigned “owner”. Such changes may include, but are not limited to, granting access to additional parties (including supervisors), forwarding email, or performing any search of stored data for purposes other than a disciplinary investigation or technical troubleshooting.

VII. EXCEPTIONS:

Former employees and students that are now separated from the College under non-hostile circumstances, whether permanent or temporary, are assumed to have cleaned up any personal information and secured or forwarded any important data to colleagues or instructors. Therefore, any data or accounts left behind may be accessed by their direct supervisor, for the purpose of transferring data only, after their last day if requested in writing by that supervisor. Interactive accounts may only be made available temporarily for use by new users after their owners have left the College, at the sole discretion of and until a date set by the Director of the IT Services department.

IT Services retains the right to access any and all digital resources without notice to the owner, but *only* in the course of diagnosing or repairing a problem, and then only to the extent required by that problem. For example, an email issue does not require ITS to access personal documents in that user's Home Folder.

In cases where there is reasonable evidence of tampering or misuse by one or more employees or students, Security or Human Resources may request access to or a survey of records, files, email, or other digital resources owned by an employee, student, department, committee, or other group, without notice to the suspected individual or group.