

---

OFFICE OF RECORD: Computing Services  
ISSUED BY: CIO / Director of Computing Services  
EFFECTIVE DATE: 6/04/13  
APPROVED BY:

01-95-00

## **DSU Email Policy**

### **Policy**

The purpose of this policy is to outline the administration, use, and operation policies regarding services provided by Dakota State University (DSU) for email.

Employees shall use email in an appropriate manner. Reasonable and appropriate personal communications are allowed. Under no circumstances are employees allowed to use DSU's technology to engage in outside business interests, inappropriate, offensive, or illegal activities. Abuse of the system is not acceptable. Employees should not expect privacy or confidentiality when using DSU's resources. Use common sense. If in doubt, do not use DSU resources.

**Notice:** This policy may change at any time. Dakota State University will provide final authority in the interpretation of these policies.

### **Procedures for Email**

#### **Email Usage:**

- The DSU email system is intended to be used for educational and/or other valid DSU related purposes.
- Faculty and staff may use DSU's email system for personal use, as long as that usage is reasonable and the content is appropriate. DSU's email system cannot be used for personal business or personal gain.
- Illegal, harassing, lewd, or other behavior deemed inappropriate by DSU will not be permitted.
- Faculty/Staff must use DSU email for all DSU official email correspondence, such as course requirements, tuition bills, etc. (Email to students should not be done via a 3<sup>rd</sup> party email account such as Gmail or DSU email should not be forwarded to a 3<sup>rd</sup> party email account. Learning Management System email is acceptable).

#### **Email Archiving:**

- All email sent or received by users on the system is archived for 60 days. After 60 days, the archived email is automatically deleted. The archived email can be accessed when approved by the procedures listed under the "Administrative Email Monitoring" or "Request Email Monitoring" sections listed below.

- 
- A vice president or the president may request that email of employees who have resigned or retired be archived for a longer period of time to facilitate the transition to a new employee in the position being vacated.

### **Unsolicited Email Policy**

- DSU has a zero-tolerance policy with respect to unsolicited or spam email originating from DSU email accounts.
- DSU email accounts may not send email to any person who does not wish to receive it, whether on the DSU email system or elsewhere.
- DSU email accounts found to be violating the unsolicited email policy will be disabled immediately by DSU.
- In the event that a virus or other malicious software causes a user's account to be compromised and send unsolicited email, the account will immediately be disabled and the password changed. The user must communicate with IT Services to determine that the virus or "hack" of their account has been remediated before their account can be reactivated. User negligence resulting in damage to DSU's systems, software, or hardware may be subject to disciplinary action.

### **Administrative Email Monitoring:**

- Users with DSU email accounts understand that DSU has the right to:
  - Monitor the email system electronically and determine how to best operate the system, specifically as it relates to management of bandwidth, upgrades to the system, etc.
  - Protect itself or its users.
- Disclose any information as necessary to satisfy any law, regulation or other governmental request.

### **Request Email Monitoring:**

- If DSU needs to monitor a DSU employee or student email account:
  - The appropriate VP or the President will provide authorization to Computing Services to monitor a DSU employee or student email account.
  - The request must be detailed and include account information, scope, and time frame.
  - Upon approval from the appropriate VP/President, DSU Computing Services will gather the requested information, provided it is available and accessible on the system.

### **Backup:**

- Backups of the servers hosting DSU email accounts will be maintained on a "best effort" basis. These backups contain copies of the information contained in user mailboxes.
- These backups are maintained for disaster recovery purposes only. They will not be used to recover missing messages from individual mailboxes.

---

## **Additional Policies Related to DSU Email**

### **Security:**

- DSU users shall use their best efforts to prevent unauthorized use of their accounts. They shall promptly report any suspected unauthorized use or any other suspected breach of security to DSU Computing Services.
- DSU users will be held responsible for knowingly sharing their credentials or unknowingly sharing their credentials with others through negligent or careless behavior.
- DSU users may not knowingly share their passwords with others. This includes, but is not limited to, the following restrictions:
  - DSU users may not share their passwords with other DSU employees or students.
  - DSU users may not share their passwords with friends, family members, or significant others.
  - DSU users may not knowingly use their DSU email address and password, nor their DSU username and password, as the credentials to access third-party online services (e.g. Facebook, Google, Twitter, or any other third-party website or service).
- DSU users may not share their passwords with others through negligent or careless behavior. This includes, but is not limited to, the following restrictions:
  - DSU users may not send their passwords by e-mail.
  - DSU users may not post their passwords in any public area, or any area that is easily accessible by others (e.g. a Post-It note stuck to the monitor, the bottom of the keyboard, in an unlocked desk drawer, etc.)
    - DSU will immediately disable and reset the password for any DSU user whose password has been shared with others, or reasonable evidence exists that it may have been shared. Also, DSU will notify the supervisor of the employee of the password violation.

### **Right to Restrict Access:**

- DSU may disable access to a DSU user's account if evidence exists that, in its sole discretion, indicates the user's account may have been compromised.
- DSU may deny access to all or part of the system without notice if a DSU user engages in any conduct or activity that, in its sole discretion, DSU believes is in violation of any of the terms and conditions of DSU or BOR policy.
- DSU reserves the right, in its sole discretion, to stop any services they feel are in violation of DSU or BOR policies. Upon stopping a service for this reason, attempts will be made to contact the individual or their supervisor to remedy the violation.

### **Retiring Faculty or Staff:**

- DSU faculty or staff retiring from the university may request to keep their DSU email address. (See also the "Email Archiving" section of this policy.)