Statement about Authentication

To protect students from identity theft, and to ensure student authentication, the following password protection guidelines should be followed:

1. Passwords are not to be shared except in emergency circumstances or when there is an overriding operational necessity.

2. Passwords should be changed immediately after sharing.

3. Passwords should not be kept in a location accessible to others or secured in a location for which protection is less than that required for information that the password protects.

4. Passwords or any other sensitive information are not to be sent via email.

5. Stolen or compromised passwords should be changed immediately.

6. Passwords are not to be written down and posted in an unsecured area such as a computer’s monitor.