Handling of Personal Information and Sensitive Data

User’s Responsibilities for Safeguarding University Data

The university generates and manages a considerable amount of confidential and sensitive information and it must be protected.

Confidential information should not be stored on portable media – such as USBs, memory cards, removable or external hard drives and CDs/DVDs, Smartphones, tablets, iPods - unless it is protected from unauthorized access or encrypted.

- DO NOT disclose personal information to unauthorized individuals.
- Remember: Portable storage media is easily lost or stolen.
- All confidential information should be stored on an encrypted secure storage media devices.
- “Encrypted USB thumb drives” are available from CCS Hardware Services at ext. 4063.
- Use network drives to store confidential student data, financial data, health records and research data.
- Printed documents and faxes containing personal and sensitive information must be collected quickly so the information is protected.
- Lock your computer screen when it is left unattended. Close or minimize computer programs if your computer is being viewed by individuals not authorized to see the information.

If you believe there has been a breach of confidential information, please contact the CCS Service Desk immediately at ext. 3700.

- A strong password consists of at least 8 characters, upper/lower case and special numbers.
- Change your password regularly, as per the Password Policy for Information Systems.
- Only use portable storage media to store university information that is not otherwise publicly available.
- Removable media should NOT be left unattended and locked in a secure area.