THE UNIVERSITY OF OKLAHOMA
Gaylord College of Journalism and Mass Communication

Policy and Procedure: Information Security Policy Statement of Expectations

---

Policy

The Gaylord College of Journalism and Mass Communication is committed to ensuring the security and privacy of a range of data for students, faculty, and staff, e.g. student contact information, credit card numbers, grades, and other important and otherwise confidential data. Confidential student data (defined below) is not stored on any individual computers or shared drives by the Gaylord College. No credit card information will be stored on a local desktop, network drives, or any form of storage device at any time. The Gaylord College is in compliance with the Payment Card Industry's (PCI) financial and information technology standards. Following the "confidential data defined" section are ways the Gaylord College is fulfilling requirements to protect personal information. Employees who no longer work for the Gaylord College will have all of their information and security access removed by the director of Gaylord College information technology at the end of the last day of their departure. This includes all access to the college's shared folders and files. The director of Gaylord College financial operations will contact the Gaylord College director of information technology and inform him or her of the individual's last day of employment with the Gaylord College. Purchasers, PCard holders, etc. will also need to have that access removed by the director of Gaylord College financial operations.

Confidential Data Defined: Data that are specifically restricted from open disclosure to the public by law are classified as Confidential Data. Confidential Data require a high level of protection against unauthorized disclosure, modification, transmission, destruction, and use. Confidential Data include, but are not limited to:

- Student Data protected by the Family Educational Rights and Privacy Act (FERPA), including personal identification data such as Social Security Number and other Data not classified as directory information under FERPA;
- Medical Data, such as Electronic Protected Health Information and data protected by the Health Insurance Portability and Accountability Act (HIPAA);
- Research (e.g., information related to a forthcoming or pending patent applications, information related to human subjects);
- Information access security, such as login passwords, Personal Identification Numbers (PINS), logs with personally identifiable data, digitized signatures, and encryption keys;
- Primary account numbers, cardholder data, credit card numbers, payment card information, banking information, demand deposit account numbers, savings account numbers, financial transaction device account numbers, account passwords, stock or other security certificate or account numbers (such as Data protected by the Payment Card Industry Data Security Standard);

- Personnel files, including Social Security Numbers;
- Library records (such as covered by the Michigan Library Privacy Act 455); and
- Drivers license numbers, state personal identification card numbers, Social Security Numbers, government passport numbers, and other personal information that is protected from disclosure by state and federal identity theft laws and regulations.

Procedures

1) **Ensure access to credit card information is secure**. Only two authorized Gaylord College staff members may take credit card payments (both individuals are located in the Gaylord College financial services area). Gaylord College staff members working with credit cards comply with the "Gaylord College of Journalism & Mass Communication: Credit Card Security Awareness Policy, the "University of Oklahoma Campus Payment Card Security Standard—Norman Campus", and they comply and follow the "University of Oklahoma Addendum to the Security Incident Response Plan. No other employee should accept or store any credit card data defined as confidential data.
2) **Perform regular software updates as prompted on your computer devices**. Perform all prompted and regular updates to your desktop, laptop, and other devices. This will help to ensure your device is up-to-date on all software and security updates.
3) **Email safety**. Do not open emails, web links, or attachments from unknown senders. Do not respond to any emails requesting personal information or that ask you to "verify your information" or "confirm your user ID and password." Change your password immediately if you have accidentally responded to one of these messages with your personal information and notify the Gaylord College information technology director. Double check spelling when entering website addresses—mistakes can direct you to an infected website and put you at risk of having your information "hacked." If you receive suspicious email, send it to spam@ou.edu. If at any time you experience unusual behavior on your computer please contact the Gaylord College information technology staff members.
4) **Data and information security**. Do not store confidential data (as defined above) on any computer device (desktops, laptops, tablets, telephones, etc.). Grant applications and proposals should be encrypted. Always lock your computer when stepping away from your workstation and log out of your computer at the end of the day. Always lock your screen when you step away from your workstation throughout the day. Do not leave any passwords or sensitive materials visible at any time. Always be mindful of your surroundings. People may observe information on your monitor without your knowledge. All computers must be logged off at the end of each business day.
5) **Use strong passwords and change your passwords frequently on email accounts**. Change your passwords frequently. This is a very important measure to guard against theft and fraud. Your OU 4+4 account can be managed through https://account.ou.edu. Strong passwords lower overall risk of a security breach and are more resistant to attacks. OU IT recommends choosing a strong password with the following attributes:

a. A minimum of 8 characters
b. At least one upper case letter (A-Z)
c. At least one lower case letter (a-z)
d. At least one number (0-9)
e. At least on special character (~!$%^&*()_=,./;"<>{}\|-)
f. A new password every six months
g. Do not reuse passwords
h. A different password for every login you have

6) **Safety while browsing on Internet**. Accidentally clicking on a bogus link and entering your personal information can expose your banking, credit card, or other personal information. Make sure there is an "s" at the end of the "https." For example: https://www.bankofamerica.com/. The "s" stands for secure, meaning the website is employing SSL encryption. This is especially important if you are banking online or have to give any personal information. Never store passwords in web browsers or on your computer. If your computer is compromised the attacker can easily find your password.
7) **Incident response on system failures, loss of services, and breaches**. If you experience system failure or loss of Internet connection, please contact the Gaylord College information technology staff members. They will evaluate the problem and work closely with the OU information technology staff members to resolve the problem, if necessary. If you are unable to login to your email with your 4+4 account or any OU website that may require your 4+4 account, please double check your username and password. If you have tried multiple times and are still unable to login, please call 325-HELP to check if your account has been locked. The OU IT Help Desk technician will be able to help you with all 4+4 account related problems. If you suspect your computer system has been compromised, you need to contact the Gaylord College information technology staff members immediately. They will evaluate the problem to determine if additional precautions are necessary.

This policy is hereby setout, authorized and approved for implementation by:

_____ _____

Dr. Joe Foote, Dean, Gaylord College Date

THE UNIVERSITY OF OKLAHOMA
Gaylord College of Journalism and Mass Communication

EMPLOYEE ACKNOWLEDGEMENT:
Policy and Procedure: Information Security Policy Statement of Expectations

Employee Name: _____

Position Title: _____

Faculty/staff member must read and complete this document, **initial each item** in the space provided, sign and date, and return it to the Gaylord College dean's office. A copy will be placed in the employee's personnel file maintained in Gaylord College. Faculty/staff member is required to update their acknowledgement of these policies by September 1, annually.

1._____ I acknowledge receiving "Information Security Policy Statement of Expectations."

2. _____ I understand that I may have access to confidential and sensitive information. I agree to use reasonable precautions to assure that this information is not disclosed to unauthorized persons or used in an unauthorized manner.

3. _____ I understand that non-compliance with these policies may result in internal discipline, up to and including discharge, in accordance with University of Oklahoma policy, local, state, and federal laws.

4. _____ I understand that any tampering, interference, damage, or unauthorized access to computer data or computer systems may constitute a violation of law or a breech of privacy. I understand I may be held civilly and criminally responsible for such breeches.

SIGNATURE:
In signing this document below, I agree to comply with my responsibilities under all terms of the University of Oklahoma and the Gaylord College of Journalism and Mass Communication Information Security Policy and other related and applicable policies, procedures, and laws governing the security of data.

_____ _____
Signature of employee Date