December 8, 2016

Office of General Counsel

Crisis Management

Gary Cunningham
General Counsel

Noelle Hawton
Chief Marketing and Communications Officer

CRISIS MANAGEMENT

College and universities are the subjects of public attention on a daily basis. Crisis management is comprised of two main concerns:

- The problem or incident giving rise to the crisis must be addressed and resolved. This, of course, depends upon the problem.
- The campus must address the ensuing public, stakeholder and media attention because of its responsibility to the public and because of possible harm to reputation.

RECOGNIZING AND ANTICIPATING THE EXISTENCE OF A CRISIS

- Ideally, campus response to a crisis begins before there is media attention. College and university administrators and key communicators have the responsibility to recognize the emergence of a potential crisis.
- You all know the types of problems on college campuses that currently trigger public attention and scrutiny: campus violence including sexual assault, and especially gun violence; student protests; racial and other discrimination incidents; and data breaches involving campus administration.

COMMUNICATE

It is important that persons who learn of a potential crisis communicate with those campus employees who are responsible for the particular type of problem.

In addition, campus officials must communicate with appropriate contacts at the system office such as the General Counsel's Office and Marketing and Development.

RESPOND TO THE INCIDENT

Of course response to an incident depends upon the subject matter. Because the character of crises are predictable, response teams featuring campus experts should be created so that response can be immediate.

CAMPUS VIOLENCE/ACTIVE SHOOTER SCENARIO

- Safety of students and employees is paramount. Every campus should have an Emergency Operations Plan dealing with the active shooter scenario involving training of students and staff, exercises and responding to emergencies.
- Participation of local law enforcement.
  - Local law enforcement must be alerted
- Mass communication strategy should be in place – text, email, other messaging.

SEXUAL ASSAULT

The federal Office of Civil Rights requires that every campus have procedures in place for the reporting and for addressing sexual assault including an agreement with law enforcement.

- Take all allegations seriously and follow Board Policy 1B.3 and System Procedure 1B.3.1.
- Faculty, Staff and Students should know where to file a complaint and the identity of the Title IX Officer.
- Keep investigations moving (OCR 60-day presumption).
- Consider/Offer services to complainants in all cases even if no investigation or discipline.
- Form a relationship with local law enforcement.

STUDENT PROTESTS

- Identify and analyze state and local laws and ordinances including local safety restrictions, such as Fire Marshal's limits on occupancy
- Consult constitutional policies on protests
- Time, place and manner restrictions
  - Protestors must leave by close of business day
  - Some buildings should be off limits because of no public access, threat of injury
- Free speech zones
- Written permit requirements
- Student Code of Conduct
- Follow existing policies and procedures
- Advice from General Counsel's Office on First Amendment issues

RACIAL OR DISCRIMINATION INCIDENTS

- Racial or discrimination incidents can involve student on student, employee on student or unaffiliated member of the public on student.
- Student on student problems are addressed through the IB1 procedures and the student Code of Conduct.
- Employee on student is addressed in the 1B1 procedures. An investigation should be started as soon as possible.
- The third scenario is much more difficult since the perpetrator is not subject to campus remedial processes. Several possible remedies exist:
    - Involve local law enforcement
    - No trespass notice
    - Student education – reaching out to students

ADMINISTRATIVE CONTROVERSY

- Transparency is good, head in the sand is bad.
- Address problems when they are small, before they grow up.

IN THE EVENT OF A DATA BREACH

- Security Breach Data Notification Guideline 5.23.1.13
  - All System employees must immediately report known or suspected breaches of security to his or her supervisor or the designated System individual or office (Local Campus Authority “LCA”).
  - If suspected breach involves a potential computer virus or other malware, disconnect affected equipment from the internet and turn it off until System office IT has been contacted.
- LCA must complete a Breach of Security Incident Response Summary

IN THE EVENT OF A DATA BREACH

- OGC, with consultation of other system office personnel, will determine if a data breach has occurred.
- The MGDPA (Minn. Stat. § 13.055) requires notice to affected individuals of a breach of security (unauthorized access) for any private or confidential data (not just SSN or financial information) in any medium (not just computerized).
- If notice is required, OGC will assist in determining whether notice is required, how it must be done and other details.
- If notice is required, Internal Audit will notify the Legislative Auditor as required by Minn. Stat. § 3.971.

SOCIAL MEDIA

- Types of Problems
  - Threats of Violence and Harassment/Discriminatory comments.
  - Impersonation of campus officials, departments, or student groups.
  - Copyright/Trademark infringement.
- Discovering a Problem
  - Monitoring: If you have specific information about a threat, it is appropriate in order to facilitate campus safety.
  - From a Communications standpoint, monitoring is essential.
  - Mention is available to all campuses to monitor social media.
  - Reports from the community.

SOCIAL MEDIA

- Ways to respond?
  - Distinguish between System-owned accounts (e.g., @MnSCU or a college's official Facebook page) and non-System owned accounts
- For System-owned accounts
  - Rely on the Acceptable Use Policy (5.22) & Procedure (5.22.1)
    - Users may not engage in harassment, threats to or defamation of others, stalking, and/or illegal discrimination
    - An institution may limit who creates official pages and uses campus logos and trademarks
    - Users may not forge the identification of the person using system information technology
  - Consider disabling comments entirely (blogs, Facebook)
  - Place careful limitations on the forum
  - Fight speech with more speech

CRISIS COMMUNICATION CONCERNS

- Consider whether and what type of information should be sent to interested groups
  - Stakeholders
  - Employees
  - Students
  - Alumni
  - Local Community
- Identify a spokesperson for the issue. It is of vital importance that the college or university speak with one voice.

CRISIS COMMUNICATION CONCERNS

- Media
  - Plan for communication in advance, may develop templates based upon past occurrences.
  - Opt to be as transparent as possible and as responsive as possible.
- Social Media
  - Planning should take into account social media channels, monitoring and protocol regarding how and if to respond.

WHAT STANDARDS APPLY?

- Minnesota Government Data Practices Act
  - All government data
- Family Educational Rights and Privacy Act (FERPA)
  - Student records
- Other laws, standards depending on content
- Sanctions for violations – to institution, individuals

YOU ARE A STEWARD

- You are authorized to access/use private data to the extent you need it to do your work.
- You are ONLY authorized to access/use private data for assigned work purposes.
- You are responsible to protect non-public data from improper disclosure.

FERPA EDUCATION RECORDS DEFINED

- Personally identifiable information (PII) collected/maintained by college/university about students.
- Enrolled students (including online) or applicants
  - in any (tangible) format
  - in any location
- Including information from which student's identity could be ascertained, either by itself or in combination with other available information.

EDUCATION RECORDS CLASSIFIED

- Mostly “private” = accessible to:
  - Subject
  - “School officials” with a “legitimate educational interest” and
  - Third parties with subject’s written consent or as permitted or required by law
- “Directory data” is public
  - Designated by each college/university
  - **Annual notice** to students required
  - Students have right to “opt-out” or suppress

CONSENT REQUIREMENTS

- If student consent required to release private data, must be **signed** (including electronic "signature" that provides appropriate ID and authentication of the student and approval of content), **dated** and:
  - Specify the records to be disclosed
  - State purpose of disclosure
  - Identify party or class of parties to whom disclosure is authorized

DE-IDENTIFIED EDUCATION RECORDS

- No consent required to release if all PII removed, and reasonable determination is made that a student's identity is not ascertainable, whether through single or multiple releases, and taking into account other reasonably available information.

HEALTH OR SAFETY EMERGENCY DISCLOSURES

- If school determines there is “articulable and significant threat” information needed to protect health/safety may be released:
  - To (any) appropriate party
- Take into account the totality of circumstances pertaining to a threat; so long as rational basis, Department of Education won’t second-guess.
- Maintain a record of basis and disclosure.

HI, CAN YOU JUST TELL ME . . .

Another recent FERPA amendment prohibits disclosing *or confirming directory data* without consent if

- Student's SSN *or other non-directory information*
- Either alone or in combination with other data

is used to identify the student or the student's records.

MINNESOTA GOVERNMENT DATA PRACTICES ACT MINNESOTA STATUTES CHAPTER 13

- Applies to all government data, wherever located
- Presumes data are public – available on request
  - But most personnel and educational data are *private* – subjects generally have right to access to data about themselves and otherwise control access as permitted by law
- Government entities must keep data secure and maintain with appropriate privacy protections
  - Administrative
  - Physical
  - Technical

GOVERNMENT DATA – WHAT IS IT?

- Information that is collected, created, received, maintained or disseminated by government entity
  - In any tangible form
  - Wherever located
  - About individuals – or not
  - Very broad

PUBLIC DATA

- The general “default rule” under MGDPA
- Available to anyone upon request – but orderly procedures are appropriate
  - May not require identification or reason (except credit card marketers for undergraduates)
  - Immediately (if possible) or within “reasonable time”
  - Access (viewing) at reasonable time, location; free
  - May charge costs for copies (per policy)
    - $.25 per page for standard B & W copy

“PRIVATE” DATA

- Default rule for employee & student data
- “Private” means:
  - Accessible to subject upon request (10 work days);
  - Accessible to school officials/agents *for job-related needs (legitimate educational interest in education records);*
  - Accessible to third parties with:
    - Subject’s written consent (MGDPA/FERPA required elements) or
    - Appropriate legal authority
- Always private: SSN (even partial), ethnicity, immigration status, national origin, etc.
- Collect only what is *needed*.

DATA ON EMPLOYEES

- Government data on employees are private except:
- Name; employee identification number, which must not be the employee's Social Security number; actual gross salary; salary range; terms and conditions of employment relationship; contract fees; actual gross pension; the value and nature of employer paid fringe benefits; and the basis for and the amount of any added remuneration, including expense reimbursement, in addition to salary; job title and bargaining unit; job description; education and training background; previous work experience; date of first and last employment; work location; a work telephone number; badge number; work-related continuing education; honors and awards received; payroll time sheets or other comparable data that are only used to account for employee's work time for payroll purposes, except to the extent that release of time sheet data would reveal the employee's reasons for the use of sick or other medical leave or other not public data.

EXISTENCE AND STATUS OF A COMPLAINT AGAINST AN EMPLOYEE IS PUBLIC

- Status is open, pending, under investigation, closed.
- Existence does not include nature of complaint or identity of complainant.

FINAL DISPOSITION OF A DISCIPLINARY ACTION IS PUBLIC AND THE REASONS FOR DISCIPLINE ARE PUBLIC

- Discipline is final only if arbitration is complete or time limit has passed.
- Discipline for administrators is complete upon imposition of discipline.
- If no discipline is imposed, data is not public (unless subject is public official).

INVESTIGATION DATA ON PUBLIC OFFICIAL IS PUBLIC

- Investigation data on public official is public even if official resigns or is terminated before discipline is imposed.

PUBLIC OFFICIAL DEFINED

- The head of a state agency and deputy and assistant state agency heads.
- Members of boards or commissions required by law to be appointed by the governor or other elected officers.
- Executive or administrative heads of departments, bureaus, divisions, or institutions within state government.

THE STATE MAY NOT ENTER INTO AGREEMENTS LIMITING DISCLOSURE OR DISCUSSION OF PERSONNEL DATA

- A government entity may not enter into an agreement settling a dispute arising out of the employment relationship with the purpose or effect of limiting access to or disclosure of personnel data or limiting the discussion of information or opinions related to personnel data. An agreement or portion of an agreement that violates this paragraph is void and unenforceable.

PERSONNEL DATA MAY BE PROVIDED TO LAW ENFORCEMENT

- Private personnel data, or data on employees that are confidential data under section 13.39, may be disseminated to a law enforcement agency for the purpose of reporting a crime or alleged crime committed by an employee, or for the purpose of assisting law enforcement in the investigation of a crime committee or allegedly committed by an employee.

CIVIL INVESTIGATORY DATA

- Data collected as part of an investigation in connection with pending civil legal action is confidential.
- Pending civil legal action determined by chief attorney.
- May be disclosed to promote public health or safety or to dispel widespread rumor or unrest.

DEFAMATION

- An intentionally published false communication about a particular person that damages the person's reputation.
- Libel – printed statement
- Slander – oral statement

HANDLING A MEDIA INQUIRY

- Capture the question accurately
- Tell them you will have to get back to them
- Ask for their deadline
- Respond within their deadline whenever possible, even if it is to tell them you don’t yet have the information or can’t obtain the information because it isn’t public
- In a crisis (and as a part of crisis planning) instruct non-spokespeople how to handle a surprise media interaction

MINNESOTA STATE CONTACT INFORMATION

Gary R. Cunningham
General Counsel
gary.cunningham@so.mnscu.edu
651-201-1818

Noelle Hawton
Chief Marketing and Communications Officer
noelle.hawton@so.mnscu.edu
651-201-1801

Office of General Counsel
www.ogc.mnscu.edu

Please take a few minutes to complete our poll!

MINNESOTA STATE