

The University of Wisconsin System
UPS OPERATIONAL POLICY: GEN 32



SUBJECT: Personal Internet Account Access

Original Issuance Date: July 1, 2015

Last Revision Date:

1. POLICY PURPOSE:

The purpose of this policy is to provide guidance on how to comply with [Wis. Stat. § 995.55](#), a law that places restrictions on access to, and observation of, the personal Internet accounts of current and prospective employees and students. It also identifies the rights applicable to employers and educational institutions.

2. POLICY BACKGROUND:

[Wis. Stat. § 995.55](#), which was created by [2013 Wisconsin Act 208](#), limits employers and educational institutions from accessing and observing personal Internet accounts of current and prospective employees and students.

3. POLICY DEFINITIONS:

Please see UPS Operational Policy [GEN 0: General Terms and Definitions](#) for a list of general terms and definitions.

Definitions specific to this policy:

“Personal Internet account” means an Internet-based account that is created and used by an individual exclusively for purposes of personal communication (e.g., personal email accounts and social media).

“Access information” means a user name and password or any other security information that protects access to a personal Internet account.

4. POLICY:

A. Employer Prohibitions

As Employers, UW System institutions may not:

- (1) Request or require an employee or applicant for employment, as a condition of employment, to disclose access information for the personal Internet account of the employee or applicant or to otherwise grant access to or allow observation of that account;

- (2) Discharge or otherwise discriminate against an employee for:
 - (a) Exercising the right under (1) above to refuse to disclose access information for, grant access to, or allow observation of the employee's personal Internet account;
 - (b) Opposing a practice prohibited under (1) above;
 - (c) Filing a complaint or attempting to enforce any right under (1) above; or
 - (d) Testifying or assisting in any action or proceeding to enforce any right under (1) above; or
- (3) Refuse to hire an applicant for employment because the applicant refused to disclose access information for, grant access to, or allow observation of the applicant's personal Internet account.

B. Employer Freedoms

As employers, UW System institutions are permitted to do the following:

- (1) Request or require an employee to disclose access information to the employer in order for the employer to
 - a) Gain access to or operate an electronic communications device supplied or paid for in whole or in part by the employer or
 - b) Gain access to an account or service provided by the employer, obtained by virtue of the employee's employment relationship with the employer, or used for the employer's business purposes;
- (2) Discipline or discharge employees who transfer confidential or proprietary information to their personal Internet accounts without authorization;
- (3) Require an employee to cooperate in an investigation of employment-related misconduct, violations of law, or violation of established rules if the employer has reasonable cause to believe that the personal Internet account contains information related to the violation or misconduct;
- (4) Restrict or prohibit an employee's access to certain Internet sites while using an electronic communications device supplied or paid for in whole or in part by the employer or while using the employer's network or resources;
- (5) Comply with a duty to screen applicants for employment that is established under state or federal laws, rules, or regulations;
- (6) View, access, or use information that can be obtained without access information or that is available in the public domain; and
- (7) Request or require employees to disclose their personal email addresses.

C. Educational Institution Prohibitions

As educational institutions, UW System institutions may not:

- (1) Request or require a student or prospective student, as a condition of admission or enrollment, to disclose access information for the personal Internet account of the student or to otherwise grant access to or allow observation of that account;
- (2) Expel, suspend, discipline, or otherwise penalize any student for:
 - (a) Exercising the right under (1) to refuse to disclose access information for, grant access to, or allow observation of the student's personal Internet account;
 - (b) Opposing a practice prohibited under (1) above;
 - (c) Filing a complaint or attempting to enforce any right under (1) above; or
 - (d) Testifying or assisting in any action or proceeding to enforce any right under (1) above; or
- (3) Refuse to admit a prospective student because the prospective student refused to disclose access information for, grant access to, or allow observation of the prospective student's personal Internet account.

D. Educational Institution Freedoms

As educational institutions, UW institutions may do the following:

- (1) Request or require a student to disclose access information to the educational institution in order for the institution to gain access to or operate an electronic communications device supplied or paid for in whole or in part by the institution or in order for the educational institution to gain access to an account or service provided by the institution, obtained by virtue of the student's admission to the education institution, or used for educational purposes; and
- (2) View, access, or use information about a student or prospective student that can be obtained without access information or that is available in the public domain.

Questions about accessing personal Internet accounts or electronic devices provided by the institution should be directed to your campus counsel or the UW System Office of General Counsel.

5. RELATED DOCUMENTS:

[2013 Wisconsin Act 208](#)
[Wis. Stat. § 995.55, Internet privacy protection](#)

6. POLICY HISTORY: