PERSONAL ONLINE ACCOUNT PRIVACY PROTECTION ACT

R.S. 51:1951-1955

WHITE PAPER

INTRODUCTION

This White Paper discusses the Personal Online Account Privacy Protection Act, R.S. 51:1951-1955, which provides for the privacy of online personal accounts belonging to employees and students. The Act prohibits employers and educational institutions from requesting or requiring an employee or applicant for employment, or a student or prospective student, to disclose any username, password, or other authentication information that allows access to the individual's personal online account. The Act further provides notable exceptions to the prohibitions, that is, what employers and educational institutions are allowed to do. These exceptions are more far reaching than the prohibitions in that they allow the employer or school to access these accounts under certain conditions.

Personal Online Account Privacy Protection Act ***Enacts R.S. 51:1951 - 1955***

General

Definitions

Employer Prohibitions

Educational Institution Prohibitions

No Duty to Monitor; Liability

Penalties

Similar Legislation - Confidential Student PII

Personal Online Account Privacy Protection Act

General

The Personal Online Account Privacy Protection Act, R.S. 51:1951 through 1955, was enacted by Act 165 of the 2014 Regular Session. The Act prohibits employers and educational institutions from requesting or requiring current employees, potential employees, students or potential students, to disclose information that allows access to, or observation of, personal online accounts. Further, the Act prohibits employers and educational institutions from taking certain actions for failure to disclose information that allows access to personal online accounts. Additionally, the Act provides for certain individuals to self-disclose information that allows access to or observation of personal online accounts and limits liability for failure to search or monitor the activity of an individual's personal online account. The Act also provides for exceptions that allow the employer or educational institution to demand such disclosure under certain circumstances.

Definitions – R.S. 51:1952

The Act defines in R.S. 51:1952 the following terms:

- **"Educational institution"** means a public or private educational institution or a separate school or department of a public or private educational institution and includes but is not limited to the following:
    - A university, college, or junior college.
    - An academy.
    - An elementary or secondary school.
    - An extension course.
    - A kindergarten.
    - A nursery school.
    - A school system, school district, or intermediate school district.
    - A business, nursing, professional, secretarial, technical, or vocational school.
    - A public or private educational testing service or test administrator.
    - An agent of an educational institution.

- **"Employer"** means a person, including a unit of state or local government, engaged in a business, industry, profession, trade, or other enterprise in this state and includes an agent, representative, or designee of the employer.

- **"Personal online account"** means an online account that the employee, applicant for employment, student, or prospective student uses exclusively for personal communications unrelated to any business purpose of the employer or educational institution. A personal online account does not extend to any account or profile created, serviced, maintained, used, or accessed by a current employee, applicant for employment,

student, or prospective student for either business purposes of the employer or educational institution or to engage in business-related communications.

- **"Electronic communications device"** means any device that uses electronic signals to create, transmit, and receive information, including a computer, telephone, personal digital assistant, or other similar device.

Employer Prohibitions - R.S. 51:1953(A)

An employer is prohibited in R.S. 51:1953 from doing any of the following:

1. Request or require an employee or applicant for employment to disclose any username, password, or other authentication information that allows access to the employee's or applicant's personal online account.

2. Discharge, discipline, fail to hire, or otherwise penalize or threaten to penalize an employee or applicant for employment for failure to disclose.

Exceptions - R.S. 51:1953(B)

An employer is **NOT** prohibited from doing any of the following:

1. Requesting or requiring a current employee or applicant for employment to disclose any username, password, or other authentication information to the employer to gain access to or operate any of the following:

    a. An electronic communications device paid for or supplied in whole or in part by the employer. *(This is not defined. It is not clear what is meant by in whole or in part. If the employer pays a monthly stipend to the employee to keep office email on his or her personal phone, is that covered here?)*

    b. An account or service provided by the employer, obtained by virtue of the employee's or applicant's relationship with the employer, or used for the employer's business purposes.

2. Disciplining or discharging an employee for transferring the employer's proprietary or confidential information or financial data to an employee's personal online account without the employer's authorization.

3. Conducting an investigation or requiring an employee or applicant to cooperate in an investigation in any of the following circumstances:

    a. If there is specific information about activity on the employee's personal online account, for the purpose of ensuring compliance with applicable laws, regulatory requirements, or prohibitions against work-related employee misconduct. *(Specific information in this context is not defined. Does this mean alleged criminal activity? Unflattering statements about co-workers or supervisors? It is not clear.)*

b. If the employer has specific information about an unauthorized transfer of the employer's proprietary information, confidential information, or financial data to an employee's or applicant's personal online account.

4. Conducting an investigation or requiring an employee or applicant to cooperate in an investigation as specified in the Act, including requiring the employee or applicant to share the content that has been reported in order to make a factual determination, without obtaining the username and password to the employee's or applicant's personal online account.

5. Restricting or prohibiting an employee's or applicant's access to certain websites while using an electronic communications device paid for or supplied in whole or in part by the employer or while using an employer's network or resources, in accordance with state and federal law. *(As noted above, does this include the stipend situation?)*

6. If through the use of an electronic device or program that monitors an employer's network or the use of an employer-provided device, an employer inadvertently receives an employee's or applicant's username, password, or other authentication information, the employer shall not be liable for having the information, but shall not use the information to access the employee's or applicant's personal online account. *(There are no apparent penalties for violating this provision. One must presume any violations of this Act would lie in civil court.)*

7. An employer shall not be prohibited or restricted from complying with a duty to screen employees or applicants prior to hiring or to monitor or retain employee communications that are established pursuant to state or federal law, rules or regulations, case law, or rules of self-regulatory organizations.

8. An employer shall not be prohibited or restricted from viewing, accessing, or utilizing information about an employee or applicant that can be obtained without a username, password, or other authentication or that is available in the public domain.

9. An employer shall not be prohibited or restricted from requiring an employee to provide a personal e-mail address in order to facilitate communication with the employee in the event the employer's e-mail system fails.

Nothing in the Act shall be construed to prohibit or restrict an employee or applicant for employment from self-disclosing any username, password, or other authentication information to the employer that allows access to the employee's or applicant's personal online account. *(This addition would appear to open the door to subtle pressure on the employee to disclose.)*

Educational Institution Prohibitions - R.S. 51:1954

An educational institution is prohibited from doing any of the following:

1. Request or require a current student or prospective student to disclose any username, password, or other authentication information that allows access to the student's or prospective student's personal online account.

2. Expel, discipline, fail to admit, or otherwise penalize or threaten to penalize a student or prospective student for failure to disclose this information.

Exceptions - R.S. 51:1954(B)

An educational institution is **NOT** prohibited from requesting or requiring a student or prospective student to disclose any username, password, or other authentication information to the educational institution to gain access to or operate any of the following:

1. An electronic communications device paid for or supplied in whole or in part by the educational institution, except where the device has been provided to the student or prospective student with the intent to permanently transfer ownership of the device to the student or prospective student. *(The same questions under the employer section exist here. What does in whole or in part mean?)*

2. An account or service provided by the educational institution that is either obtained by virtue of the student's or prospective student's admission to the educational institution or used by the student or prospective student for educational purposes. *(This appears to mean any school owned or school provided account a student is required to possess and use is completely accessible by the school.)*

An educational institution is **NOT** prohibited from doing any of the following:

1. Viewing, accessing, or utilizing information about a student or prospective student that can be obtained without a username, password, or other authentication information or that is available in the public domain.

2. Restricting or prohibiting a student's or prospective student's access to certain websites while using an electronic communications device paid for or supplied in whole or in part by the educational institution or while using an educational institution's network or resources, in accordance with state and federal law, except where the device has been provided to the student or prospective student with the intent to permanently transfer the ownership of the device to the student or prospective student.

Nothing in the Act shall be construed to prohibit or restrict a student or prospective student from self-disclosing any username, password, or other authentication information to the educational institution that allows access to the student's or prospective student's personal online account.

No Duty to Monitor; Liability - R.S. 51:1955

There is no duty imposed by this Act for an employer or educational institution to search or monitor the activity of an individual's personal online account.

No employer or educational institution shall be liable for failure to request or require an employee, a student, an applicant for employment, or a prospective student to disclose information that allows access to the employee's, student's, applicant's, or prospective student's personal online account**.**

Penalties

There are no civil or criminal penalties imposed by the Act for violations of its provisions. However, it is assumed that a violation may result in a civil court action by the employee, potential employee, student or potential student against the employer or educational institution.

Similar Legislation - Confidential Student PII- R.S. 17:3913 and R.S. 17:3914

R.S. 17:3913 and R.S. 17:3914 provides similar protections for student personally identifiable information (PII). These laws provide that any information that personally identifies a public school student, or could be used to personally identify such a student, may not be made public without parental consent. Additionally, these laws impose criminal penalties for violation of a student's personally identifiable information. These laws apply to charter schools pursuant to R.S. 17:3996(B)(38). It further appears that these laws apply to public elementary and high school students only.