Administrative Procedure 800

INFORMATION TECHNOLOGY SECURITY

Background

The Chief Financial Officer (CFO) is directed to ensure that information technology security is maintained in order to protect the confidentiality, integrity and effective use of data maintained on staff, students and other individuals or organizations.

Procedures

1. To this end the CFO shall ensure:
   - 1.1 A Disaster Recovery Plan is in place and reviewed on an annual basis to ensure operation integrity and business continuity.
   - 1.2 An Information Technology (IT) Operational Manual is in place and reviewed on an annual basis to document infrastructure systems and IT operations.
   - 1.3 Staff and students receive training resulting in them becoming educated, knowledgeable, and responsible technology users.
   - 1.4 Staff and students are aware of technology policies and the consequences of non-compliance.
   - 1.5 Information technology staff is adequately trained to meet the changing technical issues with respect to technology and security.
   - 1.6 The information technology system is automated to ensure that software patches, virus updates and authentication are maintained in an efficient manner.
   - 1.7 Data retention is secured through the use of effective backups and offsite storage of backup media.
   - 1.8 Information technology networks, related hardware, system users and security are monitored on as required basis to maintain a secure environment.
   - 1.9 All software operated on information technology networks or standalone workstations are properly licensed.
   - 1.10 There is compliance with the information technology security provisions in this AP.

2. All employees of the Division shall be informed of these procedures, and shall comply with, them at all times. All staff currently employed or newly hired staff shall be made aware of this AP.

3. Ensuring Compliance
   - 3.1 The CFO and information technology staff are responsible for ensuring the appropriate use and security of all information. They are responsible for taking all reasonable steps to ensure compliance with this administrative procedure.
   - 3.2 Failure to comply with this policy will result in disciplinary measures.
   - 3.3 The information technology staff are responsible for:
     - 3.3.1 Ensuring that the facilities in their charge are operated according to these APs.
     - 3.3.2 Taking all reasonable measures to ensure the proper operation of the information technology services.
     - 3.3.3 Ensuring the security and integrity of data storage and networks.
     - 3.3.4 Reporting Information Technology Security Policy violations they discover to the Director. Please see the *Reporting and Investigation of Security Policy Violations*.

4. Authorization to Access School Division Information Technology Systems
   4.1 All parties accessing the SRPSD internal network must be authorized by information technology services. The authorized user must exercise due diligence to ensure the security and privacy of their authentication to prevent misuse by third parties. User accounts may not be shared. Users shall access only facilities and information for which authorization has been provided, for the purpose of conducting official business, and other approved functions. Authorization will be terminated immediately upon transfer or dismissal of employees; or change of status of other users.
   4.2 With prior approval of the Director on a per case basis, IT staff may temporarily or permanently withdraw computing access privileges for cause while making allowances for academic penalty.

5. Principles
   5.1 Only SRPSD owned equipment and software may be used or attached to the SRPSD Wide Area Network (WAN).
   5.2 The Division wireless guest networks shall allow access with personal devices.

6. Electronic Security Measures
   6.1 Electronic security (e.g., firewalls, data, computer system or wireless encryption) is required to reduce unauthorized access to information.

7. Physical Security Measures
   7.1 Appropriate physical security (e.g., locked cabinets for routers, card fob swipe, office doors with locks), shall be provided to reduce unauthorized access to critical information technology network hardware.

8. Incidental and Prohibited Use
   8.1 Information technology information and equipment (i.e., databases, laptops, and personal devices) are the property of the Division and shall be used for the purposes for which authorization was granted. The information technology systems shall not be used for commercial, illicit, threatening, discriminatory, harassing or obscene purposes.
   8.2 Confidential information shall not be used for personal or other non-official use nor disclosed to third parties.
   8.3 Individuals using school division computer equipment off premises are subject to the terms and conditions of this policy.

9. Disposal of Hardware and Printed Documents
   9.1 The disposition of information technology equipment must be done in an approved manner. Confidential data on any medium must be securely stored prior to disposal defined in the disposal procedure.

10. Monitoring School Division Information Technology Systems and Information Use
    10.1 Reasonable procedures shall be put in place to monitor the use and access of the information technology systems and information as a means of ensuring compliance with this policy. Users of the information technology systems waive any right to privacy. As appropriate, the results of monitoring will be used in the investigation of violations of this Policy. Please refer to monitoring procedure.

11. Reporting and Investigation of Security Policy Violations
    11.1 Suspected violations of this policy must be immediately reported to the Director. A record should be kept of all reported violations and their disposition. Investigation of the violation may include monitoring and inspection hardware, peripheral devices, files and e-mail of

specific users by authorized internal or external investigating parties at the discretion of the Director. Where reasonable, individuals suspected of being in violation will be invited to cooperate with the investigation process.

11.2 Information available to selected information technology staff by virtue of their authority or privilege shall be held in confidence, except where a violation of the policy is suspected. In such cases, the information technology staff has the duty to report the matter to the Director.

11.3 No individual will disclose confidential data to any external agency without the approval of the Director. *The Local Authority Freedom of Information and Protection of Privacy Act* LAFOIP will guide the disclosure of confidential data.

12. Users have a right to fair and equitable treatment throughout any investigation into violations of Information Technology security policies. Where appropriate, a user being investigated for violations shall be kept informed and shall be invited to cooperate with the investigation.

13. Where a violation has been identified, the Director may apply appropriate sanctions, up to and including dismissal or recommendation for dismissal.

14. Where a violation occurs that might involve possible criminal or legal action, it will be referred to the police for further investigation.

Reference: Section 85, 87, 108, 109, 175, *The Education Act, 1995*

Approved: May 12, 2014