Administrative Procedure 124 RESPONSIBLE SECURITY OF DISTRICT INFORMATION

All records created in the service of East Central Alberta Catholic Schools, regardless of form or creator, are the property of East Central Alberta Catholic Schools. Records are an asset and support the District's work in providing a quality education to each student to reach their maximum potential.

Procedure

Employee Responsibility

1. It is the responsibility of each employee to be informed and fully understand their role regarding the proper handling and protection of information in their custody and control.

Supervisory Role

2. Supervisors are responsible for the establishment and communication of expectations and procedures, which conform to this procedure and provide for the security of information within their environment/service unit.

Information Security

3. All information received, created, managed and maintained by East Central Alberta Catholic schools is the property of ECACS and subject to this procedure.

4. Only authorized persons may have access to information.

5. All authorized ECACS staff that create, use, manage, distribute, dispose of or preserve records/information have a responsibility to protect those records/information to prevent unauthorized access, unauthorized modifications or loss.

6. All information must be securely maintained in confidence throughout the entire time it is in ECACS custody including from creation to usage to disposition and/or preservation.

7. Personal information may only be disclosed if authorized by regulation or law including, but not limited to, the Alberta *School Act*, the Alberta *Freedom of Information and Protection of Privacy Act*, the Alberta *Child, Youth and Family Enhancement Act* and the *Canada Income Tax Act*.

Access

8. Access to information is restricted to those whose duties require such access and have received the appropriate authorization for each level of access.

Security Measures

All employees who use personal/confidential/sensitive information in the execution of their duties shall:

9. Use secure remote connections to access personal/confidential information whenever possible;

10. Refrain from storing anyone's personal information on non-ECACS owned portable devices;

11. Ensure that all information stored on portable or personal devices is encrypted and password protected;

12. Copy, download, print or transport only the information that is required for specific tasks;

13. Keep paper records and portable or personal devices physically secure;

14. Maintain an inventory or copy of the information temporarily stored at home or on portable or personal devices under their control;

15. Ensure that the master copy of information is stored on a centralized ECACS system;

16. Destroy or remove transitory paper, digital or electronic records information when it is no longer required to carry out their duties;

17. Not leave electronic devices or portable storage in non-secured areas;

18. Ensure precautions are taken which are consistent with sensitivity of the data under their custody.

Storage of Information

19. Information must be stored in a secure manner with access restricted to those authorized.

20. The use of ECACS owned or managed devices, storage and sites is highly recommended.

Use of Information

21. Use of information is limited to the specific purpose for which it was collected.

22. All information which is collected will be for a stated purpose which is clearly communicated upon collection.

Disposal of Information

23. The disposal of information must be in accordance with the retention schedule as outlined by ECACS Records Management.

24. Paper documents must be disposed of by secure shredding.

25. Digital documents must be disposed by permanent deletion.

Retention of Information

26. The retention of information must be in accordance with the retention schedule as outlined by Records Management.

27. Only information that is required must be retained.

Distribution of Information

28. Information shall only be shared or distributed to those whose duties require such information and have the appropriate level of authorization to access.

29. Personal/confidential information regarding self or others should not be disclosed, in any form, to unauthorized persons.

Reporting Loss of Information

30. If ECACS information is lost or stolen, the employee must inform their supervisor immediately upon discovery, and make the following contacts:

    a. For ECACS owned devices, contact the Principal

    b. For personal devices that contain ECACS information, contact the FOIP Coordinator (Secretary-Treasurer)

Created: August 2015