Privacy and Access
in Saskatchewan
Schools

LAFOIP Policy and Procedures Checklist for School Divisions

Delegation of Authority for Privacy Issues

1. Is there an appointed privacy officer within the organization? Yes□ No□
2. Has the board or the head appropriately delegated authority under LAFOIPP to the administrator responsible for LAFOIPP? Yes□ No□

Development of Policy

3. Are board members:
    a. involved in development of privacy measures Yes□ No□
    b. involved in implementation of privacy measures Yes□ No□
    c. informed on privacy compliance issues Yes□ No□
4. Are central office administration:
    a. involved in development of privacy measures Yes□ No□
    b. involved in Implementation of privacy measures Yes□ No□
    c. informed on privacy compliance issues Yes□ No□
5. Are school-based administrators:
    a. involved in development of privacy measures Yes□ No□
    b. involved in implementation of privacy measures Yes□ No□
    c. informed on privacy compliance issues Yes□ No□

Consultation

6. Have key stakeholders been involved in the privacy protection aspects of the procedure and provided an opportunity for comment on any implications? Yes□ No□

Training

7. Is training related to protection of personal information provided to:
    a. board members Yes□ No□
    b. all levels of management Yes□ No□
    c. all employees Yes□ No□
    d. contractors with access to personal information Yes□ No□

Privacy Impact Assessments

8. Are privacy impact assessments required as part of the protocol for the implementation of new procedure, program or projects? Yes□ No□

Collection of Personal Information

9. Is personal information collected for a program, activity, or service that will be of benefit to the subject individual? Yes□ No□
10. Are individuals informed as to the anticipated uses and/or disclosures of their personal information? Yes□ No□
11. Is personal information required to be used only for its originally stated purpose or for uses an individual would reasonably consider consistent with those purposes? Yes□ No□
12. If not, must consent be obtained to use the information in a different manner than originally intended? Yes□ No□

Access to Personal Information

13. Are policies and procedures in place to ensure secure access on a need to know basis only? Yes□ No□
14. Is access to personal information documented? Yes□ No□
15. Is individual consent to release of information obtained whenever possible? Yes□ No□
16. Is information about the collection of personal information readily available to the individuals about whom the personal information is collected? Yes□ No□
17. Are there policies and procedures in place, when appropriate, to deny an individual request for access to personal information? Yes□ No□
18. Are there procedures in place to correct an individual's personal information, when requested? Yes□ No□
19. Are there policies and procedures in place to ensure that personal information is as accurate and complete as possible? Yes□ No□
20. Are there policies and procedures in place regarding disclosure of personal information belonging to a person that is deceased? Yes□ No□

Security and Storage of Information

21. Are records management policies and procedures in place? Yes□ No□
22. Are physical access and security controls in place (locked offices and filing cabinets, clean desk policy, padlocked laptop computers, etc.)? Yes□ No□
23. Are Information Technology access and security controls in place including technological tools and system design techniques considered to enhance privacy and security (encryption, digital signatures, secure passwords, etc.) Yes□ No□

24. Are arrangements in place for an audit of the procedure, including access to personal information, compliance with policies and procedures, enforcement and reporting? Yes□ No□

Breach

25. Are there policies and procedures in place regarding breaches of privacy, security and confidentiality? Yes□ No□

26. Are administration and staff trained on how to avoid breaches and to mitigate/manage in the event of a breach of personal privacy? Yes□ No□

School Level Policy/Procedures

27. Do all school have a school-wide plan in place to address issues of privacy protection? Yes□ No□

28. Has each school in the division developed a privacy policy, guidelines and/or procedures? Yes□ No□

29. Do all schools have processes in place to inform parents about privacy and access to information? Yes□ No□

30. Do all schools have processes in place to educate students about privacy and access to information? Yes□ No□

Organizational Governance

31. Is there an organizational strategic plan or business plan that clearly addresses privacy protection? Yes□ No□

32. Does a written privacy charter or policy exist? Yes□ No□

33. Have privacy guidelines been developed for various aspects of the board's operations? Yes□ No□

34. Does a management reporting process exist to ensure that management is informed of any privacy compliance issues? Yes□ No□

35. Is senior management actively involved in the development, implementation and/or promotion of privacy measures within the organization? Yes□ No□

36. Is it understood in the organization that the Head is accountable for compliance with access and privacy legislation, and that any delegation of powers and duties should be formally recorded? Yes□ No□

37. Are there written organizational policies and procedures that define the responsibility for protecting personal information? Yes□ No□

Human Resource Practices

38. Do employees with access to personal information receive training related to privacy legislation as well as organizational privacy policies and practices? Yes□ No□

39. Is an employee within the organization formally designated responsibility for the daily administration of privacy compliance? Yes□ No□

40. Is the identity of the individual known throughout the organization? Yes□ No□

41. Is there a list of the staff positions or categories that use this personal information? Yes□ No□

42. Do staff receive ongoing training about security policies and procedures, and are they made aware of the importance of security and confidentiality on an ongoing basis? Yes□ No□

43. Can individuals within the organization obtain information about privacy policies and procedures with reasonable ease? Yes□ No□

Privacy Controls and Security

44. Have security procedures for the collection, transmission, storage, and disposal of personal information, and access to it, been documented? Yes□ No□

45. Is there an audit trail maintained to document when and by whom a file or record was created, updated, or viewed? Yes□ No□

46. Does staff maintain a disclosure log or audit trail of:

    a. what information has been disclosed Yes□ No□

    b. the recipient Yes□ No□

    c. purpose and authority for the disclosure Yes□ No□

47. Are access logs and audit trails reviewed on a regular basis? Yes□ No□

48. Are there written information security policies including a definition of roles and responsibilities and sanctions for breaches of policy? Yes□ No□

49. Are there security measures in place for personal information regardless of media format? Yes□ No□

50. Is access to personal information regularly monitored and audited? Yes□ No□

51. Are users assigned unique user identifications and passwords for access to personal information and are passwords changed regularly? Yes□ No□

52. Are access privileges revoked promptly when required (e.g. when an employee leaves or moves)? Yes□ No□

53. Are external providers of information management or technology services covered by written agreements dealing with risks including unauthorized access, use, disclosure, retention, and destruction or alteration as a best practice? Yes□ No□