CLOUD APPLICATION OR STORAGE RISK ASSESSMENT

Background

The Division recognizes that cloud based applications and storage hold a lot of potential for use in our schools. Not only are we able to realize cost savings by not having to maintain our own servers for applications, many cloud tools enable new levels of sharing and collaboration, which can transform how students learn.

The purpose of this risk assessment is to ensure appropriate consideration is given in regards to the use of personal information when using cloud applications and storage.

Definitions

Cloud-based applications are applications hosted outside of the Division's internal network facilities.

Cloud-based data storage facilities are data storage services that provide data storage on servers that are outside the Division's internal network facilities.

Digital Citizenship is defined as the generally-accepted behavior of responsible citizenship carried over to online environments and can be said to include, but not limited to, the following:

- Treating others with dignity and respect;
- Respecting the privacy of others;
- Respect others by refraining from sharing information about them without their knowledge or consent;
- Respect others by refraining from using profane or abusive language;
- Respect others by refraining from posting or storing and content that contains sexual, racial, religious, or ethnic slurs, any other form of abuse, or that contain threatening or otherwise offensive language or pictures;
- Protecting your own personal information from unknown or non-understood online environments, agencies or individuals;
- Only engaging in online financial transactions with known agencies, and only then via secure means;
- Respect others by refraining from actions that are malicious or harmful to them;
- Respecting copyright;
- Respecting and abiding by Canadian law, whether Federal, Provincial, Municipal or other statute;

- Respecting the laws or rules of any other state, international agency or organization with whom you interact;
- Ensuring you are authorized to access resources either inside or outside of the Divisions network prior to accessing them;
- Refraining from sending files or messages designed to disrupt other computer systems or networks.

Portable storage device is deemed to be any mobile device that can store or process or transmit information digitally. This Includes, but not limited to; laptops, tablets, smartphones, thumb/portable drives, CD/DVD.

Personal Information under the FOIP Act, means recorded information about an identifiable individual, including:

- Name, home or business address, or home or business telephone number;
- Race, national or ethnic origin, colour or religious or political beliefs or associations;
- Age, sex, marital status or family status;
- An identifying number, symbol or other particular assigned to the individual;
- Fingerprints, other biometric information, blood type, genetic information or inheritable characteristics, and photo likeness;
- Information about the individual's health and health care history, including information about a learning, physical or mental disability;
- Information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given;
- Another's opinion about the individual; and
- The individual's personal views or opinions, except if they are about someone else.

Procedures

1. Risk Assessment Completion

    1.1 For cloud based applications or storage where an agreement is entered into by the classroom teacher the Cloud Application and Storage Risk Assessment (Form 141-1) will be completed by the teacher in consultation with all stakeholders.

    1.2 For cloud based applications or storage where an agreement is entered into by the Principal (Form 141-1) will be completed by the Principal in consultation with all stakeholders.

    1.3 For cloud based applications or storage where an agreement is entered into by the Division (Form 141-1) will be completed by the Director of Technology Services in consultation with all stakeholders.

    1.4 Upon submission of a completed risk assessment to the Director of Technology Services approval is granted for the use of cloud application or storage.

1.5 The Director of Technology Services in consultation with other stakeholders will audit a portion of submitted assessments to ensure compliance. The stakeholders may include the Learning and Technology Advisory Committee, School Administration, and Executive Staff. If the information is not correct or incomplete approval to use the service may be withdrawn.

1.6 All submitted assessments will be published and made available as a reference for Division staff.

1.7 This Appendix will be updated as new information regarding best practices for risk assessment of cloud application and storage become available.

Adopted/Revised: JUN 2016/NOV 2019/JUN 2023

Reference: Section 11, 18, 31, 33, 52, 53, 67, 196, 197, 222 Education Act
Freedom of Information and Protection of Privacy Act
Canadian Charter of Rights and Freedoms
Canadian Criminal Code
Copyright Act
I.T.I.L. Standards, Alberta Education