# SECURE TECHNOLOGY USE - HOSTED SERVICE OR WEB 2.0 TOOLS

## Background

All staff members are who are accessing and using Information, whether that access is through a Division owned device or a personal device, are responsible for the management and safekeeping of information under their control by ensuring that there is adequate security to prevent unauthorized access, collection, use, disclosure or disposal of information.

## Definitions

*Hosted Services* are technology services where data captured, generated, exchanged or manipulated is stored on servers that belong to organizations other than the Division.

*Web 2.0 Services* are applications delivered through a web browser. These applications may facilitate the capture, generation, exchange or manipulation of data provided.

*Data* in this context refers to information stored or provided to a service or application to enable it to perform its function. This data could, depending upon the application, involve Student/Parent Personal Data, Employee Personal Data or School/Division Operational Data. Some or all of this data may be subject to the Freedom of Information and Protection of Privacy (FOIP) Act.

*Privacy Impact Assessments* are formal reviews of a specific service, consisting of a detailed explanation of the potential benefits of the software and a formal risk assessment by a team which would need to include the FOIP officer and at least one member of Tech Services.

*End User License Agreement (EULA)* is a license agreement associated with a service that indicates the rights and responsibilities of the user and the provider of the service.

*Privacy Policy* is another document often provided by services which identifies and deals with some or all of the data that is gathered by the service.

*HTTP Secure (https)* refers to a website that is protected by a security certificate, meaning that information sent to and received from that website is encrypted while in transit. A website that has https:// in the URL has this protection in place.

It is the responsibility of any staff member storing or using Data within any third party tool to ensure that the tool matches the requirements outlined in this Administrative Procedure.

## Procedures

### 1. Information Capture and Use

1.1 Anyone considering using a third party application must determine whether or not it captures any information covered by the Freedom of Information and Protection of Privacy Act.

1.2 If the application captures and organizes information which is covered under the FOIP Act it is considered a "Personal Information Bank" and details about the usage of that tool must be provided to Technology Services and the FOIP Officer. For more information view the "Guide to Identifying Personal Information Banks" located at the Service Alberta website.

1.3 If the application is complex enough that there are multiple roles and levels of access (e.g. an external Moodle where students can log in to obtain one level of access and teachers log in under a different level of access) Technology Services must be involved in the creation of an ongoing plan for maintenance of the utility.

1.4 If the application does capture information which is covered under the FOIP act there must be some way of finding and extracting the relevant information.

### 2. Privacy Standards

2.1 Any Web 2.0 application will have some type of Terms of Service and/or a Privacy Policy. Any staff member wishing to utilize a third party or Web 2.0 application is required to review these and determine whether the answers to the following questions are acceptable:

2.1.1 Who owns data that is provided to the application and the output or end product of the application? (e.g. if a student uploads a photograph to Instagram, does that student retain ownership of the photograph?);

2.1.2 Does the application use or provide any privileged information to third parties for the purposes of tracking behaviour/serving advertisements?

Any application or service that does not meet acceptable standards must undergo a Privacy Impact Assessment before it can be used.

### 3. Security Standards

3.1 Any external application accessed through a web browser that involves any private data must use a secure certificate (i.e. contain https in the URL).

3.2 Any private data provided to external applications or hosting partners must be exchanged in a secure manner, typically through:

3.2.1 An upload/download page protected by https

3.2.2 An SFTP (Secure FTP) or other secure file transfer program

3.2.3 An encrypted file sent via email

Examples of exchange methods known to be unsecure which are to be avoided:

- Emailing unencrypted files
- "normal" FTP (i.e. FTP not specifically listed as Secure FTP or SSH)

## 4. Higher Level of Responsibility

4.1 Any staff member wishing to utilize a third party or Web 2.0 application is required to agree to a higher level of responsibility, including the following:

4.1.1 You signify that you have read the Privacy Policy associated with the application.

4.1.2 You will conform to the End User License Agreement associated with the application and with any client software or app it requires be installed.

4.1.3 You have verified that the End User License Agreement and any Privacy Policy associated with the application will not violate FOIP or attempt to claim ownership of FOIPable Information.

4.1.4 If the application meets the criteria for a Personal Information Bank you will notify the FOIP Officer.

4.1.5 You will perform due diligence in researching the program or application in question from a security standpoint, verifying (when applicable) that it uses a secure method to transfer private data.

4.2 Additionally, in the cases where the application requires a client software or "app" to be installed, the staff member must review the "Secure Technology Use - End User Security Procedures" Administrative Procedure and confirm that the software or app adheres to those guidelines.

Appendix A contains a flowchart representing the key responsibilities assumed by any individual who chooses to install a piece of software.

Reference: Section 60, 61, 113 School Act
Administrative Procedure 140 - Computer Access Acceptable Use
Administrative Procedure 141 - Portable Technology Security
Administrative Procedure 142 – Secure Technology Use - End User Security Procedures
Administrative Procedure 145 - Use of Personal Communication Devices (PCD's)
Administrative Procedure 146 - Social Media
Administrative Procedure 180 - Freedom of Information and Protection of Privacy
Administrative Procedure 185 - Records Management

Created May 2014