ALGONQUIN COLLEGE | Cyber Security Unit

ADOBE SIGN

Security and Privacy Guidelines

Version 1.0

PREAMBLE

This document provides the recommended privacy and security settings for Adobe Sign.

Adobe Sign is a cloud-based platform that allows users to electronically sign, send, track, and manage electronic signature processes and store signed documents in the cloud.

Adobe Sign is not part of Adobe Creative Cloud or Adobe Acrobat Reader. *The Fill & Sign* tool within Adobe Acrobat Reader does not support the same features as Adobe Sign. You can request Adobe Sign from Information Technology Services (ITS).

Adobe Sign has two types of user accounts: 1) *Users*; 2) *Group Administrators*. While Group Administrators are responsible for implementing the recommended settings for their groups that use Adobe Sign, Users are also integral to ensuring that information security and privacy practices are implemented within day-to-day operations.

Section 1.0 of these Guidelines applies to Users. Section 2.0 applies to Group Administrators.

Before reading these Security and Privacy Guidelines please make sure that you familiarize yourself with the Adobe Sign functionality available to you as a user (https://helpx.adobe.com/sign/using/get-started-guide.html).
.

1.0 SETTINGS FOR USERS

1. Prohibited content – Personal Health Information

As per the College's current contract with Adobe, Users must not collect, use or store any document containing personal health information (PHI) within Adobe Sign.

The prohibited content includes information that relates to:

- the past, present, or future physical or mental health or condition of an individual;
- the provision of health care to an individual; and
- the past, present, or future payment for the provision of health care to an individual.

2. Mandatory fields

□ The following fields must be included at a minimum on the signature page:

  - *Print name*
  - *Signature*
  - *Date*

3. Identity authentication for sensitive documents

For sensitive documents that require a higher assurance of the identity of the recipients, consider setting a password.

When you set a password, recipients won’t be able to see or sign a document unless they enter that password.

- □ Navigate to *Send Tab* → Insert recipient email address → click envelope drop-down icon beside email address → select *Password*

If you use a *password* as an identity authentication method, please follow these rules:

- Set a different password for every document;
- Store your password in a password manager or write it down and store in a secure place (the password is not stored in clear text anywhere in the application. If the password is lost, it cannot be recovered or reset. The agreement will need to be cancelled and resent); and
- Communicate the password out-of-band such as by phone, a text message or use a separate email.

4. Provide recipients with a Privacy Notice

The College has to provide individuals with information about how data will be processed in the context of Adobe Sign.

Make sure to include the following text within the body of your email to the recipient:

Privacy Notice

Algonquin College collects, uses, discloses and retains personal information in compliance with the Freedom of Information and Protection of Privacy Act (FIPPA). Your personal information is being processed under the authority of the Ontario Colleges of Applied Arts and Technology Act S.O. 2002, c. 8, Sched. F. and will be used to enable documents to be signed electronically via Adobe Sign.

Adobe Inc. is an American company. An agreement is in place between Adobe and Algonquin College by which Adobe undertakes to provide its services in compliance with the applicable data protection laws and implement reasonable steps to protect the personal information processed for the provision of the services from unauthorized access and disclosure.

Types of personal information processed in the context of Adobe Sign include first name, surname, email address and signature. To ensure the reliability of electronic records, the system also collects information regarding the signing process including information such as the date and time of the event, and the IP address and other information about the browser or device used to send, sign, delegate, approve or take other actions with respect to the document. All of this information is recorded as part of the audit trail that is linked to the electronically signed document.

By default, you will receive a copy of the electronically signed document. When you receive a copy of the electronic record, you can also open it online to review its activity history which includes a summary of the event milestones associated with the record and the time/date stamp of such events.

If you have any questions or require assistance with Adobe Sign, please contact the sender of this email. If you have any questions or concerns specifically about the processing of your personal information by Algonquin College, please contact the Freedom of Information Coordinator by e-mail (FOIcoordinator@algonquincollege.com) or phone (613-727-4723 ext. 6407).

5. Adobe Sign and Cookies

Adobe Sign requires the use of cookies to record information from both senders and recipients. This is necessary to form the integrity of the audit trail that is linked to the electronically signed document.

If you want to make sure that Adobe’s website does not place cookies that are not strictly required for the use of Adobe Sign, you can opt-out of using these cookies by using the following links:

- https://www.adobe.com/ca/privacy/opt-out.html#websites
- http://amcglobal.sc.omtrdc.net/optout.html

2.0 SETTINGS FOR GROUP ADMINISTRATORS

1. **Make sure that a PDF copy of the signed document is sent to recipients**
   - □ Navigate to: *My User Group tab* → *Group Setting* → Enable *Attach a PDF copy of the signed document in emails sent to all recipients*

2. **Make sure that the audit report is attached to the signed document**
   - □ Navigate to: *My User Group tab* → *Group Setting* → Enable *Always attach audit report to documents*

3. **Collect explicit consent and allow recipients to opt-out**

In accordance with provincial legislation, the College must provide notice to recipients that they can refuse to use electronic signatures, at any time. Where a recipient refuses to use an electronic signature, the College must provide them with the opportunity to use a "wet" signature or an alternative form of approval.

To respect the choices of recipients, the following controls must be enabled:

- □ Navigate to *My User Group* tab → *Signature Preferences* → *Terms of Use and Consumer Disclosure* →Enable *click terms, review and agree before viewing the agreement* (recipients won't be able to sign the document unless they review and consent to the terms contained in this document)
- □ Navigate to *My User Group* tab → *Signature Preferences* → Enable *Allow recipients to decline*

4. Disable Account Sharing

Account Sharing allows one user or group to share their content with any other user or group.

The default nature of Adobe Sign is to secure a user's content from all other users not explicitly invited to view or interact with that content. However, there might be circumstances that require oversight of transactions.

Group administrators should disable this feature and allow *Account Sharing* only as needed and for a limited period.

- □ Navigate to *My User Group* tab → *Security Settings* → Select *Do not allow Account Sharing*

5. Disable Delegation for Recipients

- □ Navigate to *Group tab* → *Group settings* → *Allow external recipients to delegate their signature* → Disable *external recipients can delegate their participation to others*

6. Enable Identity Verification for sensitive documents

In order for Users in your Group to use a password as an identity authentication method for sensitive documents, make sure that the following settings are enabled:

- □ Navigate to *Group tab* → *Send Settings* → *Enable the following identity authentication methods for recipients* → Choose *Password*

7. Define password authentication rules

Navigate to *My User Group* tab → *Security Settings* → Go to *Apply a password policy when protecting document signing or viewing* and select*:*

- *Restrict number of attempts* → *Allow signer **3** attempts to enter the agreement password before cancelling the agreement*
- *Document Password Strength* → *Select Strong*

8. Allow users in your group to attach documents only from trusted sources
Adobe Sign offers several options for attaching files, including Users' computers, Adobe Sign shared libraries and several cloud storage platforms.

Users that want to attach documents stored on the cloud should be reminded that Microsoft OneDrive is the only College's official cloud-based information storage solution. In order to access OneDrive use your College network id and password to log in directly at onedrive.live.com.

Group Administrator must restrict Users from uploading documents from other cloud storage platforms:

- Navigate to *My User Group* tab → *Send Settings* → *Attaching documents* → Enable all except Google Drive, Dropbox, Box.com.

For additional Adobe Sign information or assistance, *including security and privacy-related concerns*, please contact the ITS Service Desk via phone (613-727-4723 ext. 5555), email (5555@algonquincollege.com) or web form.

If you have any questions or concerns specifically about the processing of your personal information by Algonquin College, please contact the Freedom of Information (FOI) Coordinator by email (FOIcoordinator@algonquincollege.com). Please note: This is for FOI related questions or concerns only. For all other concerns, please contact the ITS Service Desk.