

## Guideline: How to review a privacy policy

Reading a privacy policy is essential for understanding how an organization collects, uses and protects your personal information.

Review this general guidance on how to read a privacy policy to help the university make informed decisions before using services or tools that collect personal information.

If you are reviewing a tool for collecting/processing personal information of others at the University, please [contact the privacy office](#). The University is subject to *the Freedom of Information and Protection of Privacy Act* (FIPPA) and this guidance is not meant to solely assess compliance with privacy regulations.

### Start with the introduction

Look for an introduction or overview section that summarizes the purpose of the privacy policy and how it applies to you as a user. Sometimes people make mistakes. You could be presented with the wrong policy. **Double check!**

### Understand the scope

Identify the scope of the privacy policy. Determine the specific services, websites or applications it covers. Some policies are global and apply to all vendor offerings, and some policies are specific to an individual service or tool. Some protections in policies are only relevant to citizens of certain

#### Scope Questions:

- Is your use of the service included in the privacy policy?
- Is this policy written to cover all vendor products/services or is specific to one product?
- Are you relying on privacy protections that are only applicable to certain geographical regions?

geographical regions; an example of this is General Data Protection Regulation (GDPR) protections that apply only to EU citizens.

### What information is collected?

Check what types of personal information the organization collects. Remember, if the policy covers a vendor's entire portfolio of products rather than a specific product, it may include information collection practices that do not necessarily apply to your use of a particular product.

## How is information being collected?

Vendors may collect data about individuals in various ways. This may include data individuals provide directly and information collected indirectly or automatically through use (i.e., analytics) or data obtained from third parties. The distinction between direct and indirect collection of personal information lies in how the information is obtained.

### Collection Questions:

- Does the policy contain a statement about not collecting more than is needed to provide the service?
- Are there collections listed that you feel aren't relevant to your use of a product?

**Direct collection:** Information is gathered directly from the individual. The individual is usually aware of the collection since they are actively involved in the process and normally have consented to provide the information. Examples of direct collection include filling out a form online or in person, providing details over the phone or in a survey, or submitting personal information via email or an application.

**Indirect collection:** Information is gathered from other sources or through other means, without direct input from the individual. The individual may not be aware that their information is being collected or how it is being used. Examples of indirect collection include data mining from social media profiles or websites, collecting information through cookies and tracking technologies on websites, or obtaining data from third parties or public records.

### Key differences in direct vs. indirect collection:

1. **Awareness:** Direct collection involves explicit consent and awareness from the individual, while indirect collection may not.
2. **Control:** Individuals have more control over the information they provide directly, but less over what is collected indirectly.
3. **Source:** Direct collection is from the individual, whereas indirect collection involves third-party sources or technologies that gather data passively.

### Further Collection Questions:

- What information is collected directly from you and what is collected indirectly?
- If you have questions, reach out to the vendor's privacy contact (usually listed in the policy for more information).
- If contacting vendors, be prepared for lengthy response times in many cases.

## Purposes of collection

Understand the reasons why your information is being collected.

### Reasonableness Questions:

- Is the collection reasonable in relation to the service provided? The policy may refer to primary and secondary uses. For example, ordinarily a fitness app should not be asking for health insurance information.
- Is information collection and use limited to only what is necessary for providing the service?
- Pay close attention to the language used to describe purposes. Is it restrictive in nature or is it open-ended? Open-ended language can be vague and open up your information to secondary processing.
- Do they indicate a control or opt-out processes with regards to uses of information?

## Use, retention and disclosure

Look for explicit explanations of how the vendor intends to use the collected data. Purposes often include mention of additional reasons like, “Your data may be used for training purposes.” This is common practice for services that have AI components or capabilities as user inputs are used to train the AI data set. Vendors may provide a user with the ability to opt-out of having their information used in such ways. Privacy policies may not include information about the retention and disclosure of information. These may be found in the terms of use or service statements. We do want to see that these are addressed by the vendor, to ensure that the vendor does not assume ownership or permanent retention of personal information, and that the information will be securely destroyed once the service is no longer required.

### Use and retention Considerations:

- Is information use and disclosure limited to what is reasonable and necessary to provide the service and support? Will the vendor disclose information to additional third-parties as sub-contractors? The university must be aware of all third-parties who may have access to the information
- If the product or service uses components of AI, are customer inputs (i.e., content submissions) used to train AI models? Is there an option to turn off model training?  
**McMaster is prohibited from allowing personal information to be used for training AI models.**

## Consent and permission

Pay attention to sections regarding consent. Understand how the organization confirms permission to collect, use and share information if outside of or different than the purposes for which it was originally collected.

### Consent Considerations:

- Is the university responsible for collecting consent? Or, will the vendor integrate this into the service?
- How does the vendor notify users of changes to policy? Do they provide direct notice – emails directly to users notifying them of the intended change – or do they simply post revision dates online?
- Will the vendor seek direct consent from users if changes to use occur?
- Will the vendor notify users if there has been a disclosure outside of the normal course of expected activities?

**The university must ensure that notification protocols are in place for compelled disclosure.**

## Third-party sharing

Check for details about information-sharing with third parties.

- Identify the third parties involved and the purposes for sharing data with them.
- Look for language that ensures any third parties are bound by the terms outlined in the privacy policy.
- Be aware of phrases like, “We may share your data with our vendor partners for marketing purposes.” It is not uncommon for vendors to outsource their marketing to third parties, who will then have access to your data. For example, a company might use an email delivery provider such as Mailchimp to send out their marketing emails.

## Security measures

A good privacy policy should explain how the organization safeguards user information, including details about third-party involvement, or direct users to relevant pages for more information.

## Cookies and tracking technologies

Understand how the vendor uses cookies, pixel tags and other tracking technologies. Check for information about user abilities to manage or disable these technologies. Cookie tracking involves storing small pieces of data on users’ devices to track their online behavior and preferences. While this can enhance user experience by personalizing content and remembering login details, it also

raises several privacy concerns. Cookies can track users across multiple sites, creating a comprehensive picture of their online behaviour. This can be intrusive and users may not always be aware of who is collecting and sharing their data.

#### Security Notes:

- Users may configure their browser privacy settings to limit or block cookies.
- Users should periodically delete cookies from their browser to reduce the amount of data collected and stored. Most browsers have settings that allow users to clear cookies manually.
- Avoid granting unnecessary permissions or sharing personal information on websites that are not fully trust.

#### Legal jurisdiction and compliance

Look for sections outlining where user data is stored geographically and what laws the vendor is required to comply with. This could affect user data if government agencies request access to the information. This is called a **compelled disclosure**. The vendor may also be required to comply with certain privacy laws as part of providing the service. Check if there are legislated requirements that could affect how user data is managed and what rights users have under these acts. Some privacy policies may link to other documents such as cookie policies, Data Protection Addendums (DPAs) or other security documentation. Review these documents to get a better understanding of their data protection and security controls.

The University is subject to FIPPA legislation. All activities at the University must use information in a manner that is compliant with this legislation. If you are reviewing a tool or service for use at the University, please [contact the privacy office](#) prior to signing an agreement or contract and implementation.

#### User rights and choices

Look for sections outlining your rights, such as the right to access, correct or delete user data. Understand how users can exercise these rights and make choices about their data. A good privacy policy should provide individuals with details of how they can exercise their rights, specifically related to data deletion and opt-out options. Identify circumstances where the university can restrict access, use and disclosure through terms of an agreement.

#### User Rights:

- Check the policy to ensure there are detailed instructions for the access, correction and deletion of user data.

## Policy updates

Most policies will have a last updated date at the beginning of the policy. This is important to understand whether the policy is relevant and current. If you come across a privacy policy which is more than a few years old, you should check with the vendor on the relevance of the policy and any plans to revise the policy.

### Policy management:

- Check how the organization will notify users of changes to the privacy policy.
- Ideally, they will directly inform you of material changes. However, it is still common (though not ideal) for organizations to ask users to regularly review the policy and check the modification date.

## Look for contact information

Find contact details for the organization's privacy representative or data protection officer. Knowing who to contact for privacy-related inquiries is important.

Remember, if you have questions or concerns after reading the privacy policy, don't hesitate to contact the privacy office, or the vendor for clarification. Privacy policies are meant to empower users by providing transparency about how their information is handled.

## Implementation – Vendor policy transparency

Consider making a link to the vendor's policies available to university community members whose information will be collected, used, retained and disclosed through the vendor's services.