Here are some general things to keep in mind before investing in software applications for your organization.

When you're researching vendors, consider the following:

- ❏ Have there been past security issues with or criticisms of the tool?
    - ❏ If so, how quickly have they responded to criticisms about their tool? How quickly have they patched or made updates to fix vulnerabilities? Generally companies should provide updates to vulnerable software as quickly as possible, but sometimes actually getting the updated software can be difficult.
        - ❏ Note that criticisms and vulnerabilities are not necessarily a bad sign for the company, as even the most carefully-built software can have vulnerabilities. What's more important is that the company takes security concerns seriously, and fixes them as quickly as possible.
    - ❏ Of course, companies selling products and enthusiasts advertising their latest software can be misled, be misleading, or even outright lie. A product that was originally secure might have terrible flaws in the future.
- ❏ Do you have a plan to stay well-informed on the latest news about the tools that you use?
    - ❏ Setting up a Google alert for "*[example product]* data breach flaw vulnerability" is one way to find out about problems with a product that you use, though it probably won't catch every problem.
    - ❏ You can also follow tech news websites or social media to keep up with information security news. You can check the "Security News" section of the Security Education Companion, which curates EFF Deeplinks posts relevant to software vulnerabilities, as well as other considerations for people teaching digital security to others.
- ❏ Is this vendor honest about the limitations of their product?
    - ❏ If a vendor makes claims like "NSA-Proof" or "Military Grade Encryption" without stating what the security limitations of the product are, this can be a sign that the vendor is overconfident in the security of

their product. A vendor should be able to clearly state the situations that their security model doesn't defend against.

- ❏ Does the company provide a guarantee about the availability of your data?
    - ❏ This is sometimes called a "Service Level Agreement" (SLA).
    - ❏ How likely is it that this company is going to stick around? Does it seem like they have sustainable business practices?
    - ❏ If the service disappears, is there a way to access your data and move it to another service provider or app? Or will it be gone forever?
    - ❏ Is there any chance that they will ban you from using their app or service, and thus also lock you out from accessing your data? Think about if there are any limits to how the service can be used.

Questions to ask the vendor:

Note that you may not be able to hit all of the following points—however, asking these questions will give you a better sense of what to expect from the service.

- ❏ Does the vendor have a privacy policy on their website? Do they share or sell data to any third parties?
    - ❏ If you have the means to chat with a lawyer while reviewing the privacy policy, you can ask about:
        - ❏ Notification: do they promise to notify us of any legal demand *before* handing over any of our data, or data about us (with no exceptions)?
        - ❏ Viewing: Do they promise not to look at our data themselves, except when they absolutely need to?
        - ❏ Sharing: Do they require anyone who they share the data with to abide by the same privacy policy and notification terms?
        - ❏ Restriction: Are they only using the data for the purpose of which they provided?
- ❏ Will the vendor disclose any client data to their partners or other third parties in the normal course of business? If so, are those conditions clearly stated? What are the privacy practices of those other entities?

- ❏ Does the vendor follow current best practices in responding to government requests in your jurisdiction?
    - ❏ Do they require a warrant before handing over user content?
    - ❏ Do they publish regular transparency reports?
    - ❏ Do they publish law enforcement guides?
- ❏ Do they have a dedicated security team? If so, what is their incident response plan? Do they have any specifics about responding to breaches of data security?
- ❏ Have they had a recent security audit? If there were any security issues found, how quickly were they fixed?
- ❏ How often do they get security audits? Will they share the results, or at least share an executive summary?
- ❏ What measures do they take to secure private data from theft or misuse?
- ❏ Have they had a data breach? (This is not necessarily a bad thing, especially if they have a plan for how to prevent them in the future. This is really about *what* was breached— for example, was it a contact list from a webform, or their health information files?)
    - ❏ If they had a data breach in the past, what measures have they taken to prevent a data breach in the future?
- ❏ How does the company notify customers about data breaches?
- ❏ Does the vendor give advance notice when it changes its data practices?
- ❏ Does the vendor encrypt data in transit? Do they default to secure connections? (For example, does a website redirect an unencrypted HTTP website to an encrypted HTTPS site?) What is the vendor's disaster recovery plan and backup scheme?
- ❏ What internal controls exist for vendor's staff accessing logs, client data and other sensitive information?
- ❏ Does this service allow 2-factor authentication on login?
    - ❏ If not, why not? How soon do they plan to implement it?
- ❏ Do they push regular software updates?

While many companies don't yet do this, it is still good to ask:

- ❏ Do they encrypt stored data? (This is also called "encrypted at rest." For example, when it's "in the cloud"/on their computers, is it encrypted?)

- ❏ Do they have a bug bounty program? If they do not have a bug bounty program in place, how do they respond to vulnerability reports? (If they are hostile to security researchers, this is a bad sign.)

If the service is free...

It is often said that "if the software is free, then you are the product"—this is true of any company that has targeted advertising as a business model. This is even true of the free products that nonprofits use. For this reason, free services and apps should be treated with extra caution. If you are pursuing a free service, in addition to asking the questions above, you will want to consider the following additional points.

- ❏ How does the vendor make money? Do they make money by selling access to—or products based on—your private data?

- ❏ Will they respond to customer service requests?

- ❏ How likely are they to invest in security infrastructure?

If your organization has legally-mandated requirements for protecting data...

- ❏ If your organization has a unique legal circumstance (e.g. needing to abide by attorney-client privilege, HIPAA requirements for those in the medical profession, COPPA and FERPA for working with K-12 students), ask:

    - ❏ Is the client data being stored and transmitted in accordance with the legally mandated standards of your field?

    - ❏ How often do they re-audit that they are in compliance with these standards?

    - ❏ Are the audit results publicly available?

- ❏ If you use education technology or if you work with youth under 18 years old, consider following up with this series of questions for K-12 software vendors: check out EFF's white paper on student privacy and recommendations for school stakeholders.

These questions do not on their own guarantee that the vendor or product will be perfectly private or secure, but that's not a promise any vendor or software can make (and if they did, it would be a red flag). However, the answers to these questions should at least give you some idea of whether the vendor takes security and privacy seriously or not, and can therefore help you make an informed decision about whether use their product.

For more information about considerations for smaller organizations evaluating tools, check out Information Ecology's Security Questions for Providers.