NNEDV

Choosing a Vendor for Digital Services

Digital services are increasingly looked at as option for survivors to connect to advocacy and support services. In choosing a digital services platform, the first step is to think about which type of tool is best suited to the services you want to offer. Once you have decided on a digital services platform, there may be more than one vendor to choose from. There are some key considerations when choosing a vendor: (1) cost, (2) features, (3) data security and privacy, (4) customer service, and (5) service downtime.

Cost

When assessing vendors, bear in mind that higher cost doesn't necessarily equal a more suitable product. Depending on the type of digital service you want to offer, some platforms may be free. For example, if a program wanted to use video calls to occasionally supplement their in-person services, some platforms offer free versions of their software. When evaluating vendors that offer free products or services, check whether they restrict the length of calls or set a low number of allowable calls per month.

Vendors that do charge a service fee can have additional costs, including the costs of initial startup, add-on features, ongoing fees and maintenance. Other costs could include upgrading hardware (computer, server, memory) and even the cost of training staff to learn how to use the platform. Review "Total Cost of Ownership" in Assessing Readiness for Digital Services for an overview of all the costs that might be involved in offering digital services.

Features & Customizability

Many free digital platforms (messaging services, video chats, online forums) are designed to be used by individuals. They are often not robust enough to be used by an organization that requires more than one staff person or device to be connected at the same time. Choose a platform that can support your staffing

resources and capacity with features that can help you appropriately deliver the service you want to provide. Vendors with upgradable features and customizations can make the platform work better for your program.

Consider what features will be most helpful and appropriate for your services. For example, some texting platforms may offer an automated, artificial-intelligence-based service (called chatbots) that will communicate pre-determined responses based on what the survivor texts. While this option may appear helpful in lightening the workload of staff, a non-human, computer-generated response to someone who is in crisis or trauma is not appropriate.

See the Best Practices resources for more information on platform-specific features that may be helpful, as well as the ones to avoid or disable.

Data Security & Privacy

Digital platforms can capture a lot of information about users as part of their standard functionality. This can include "incidental" data, such as phone number, IP address, user name, etc.; information about the communication (date, time, duration, account information); and sometimes the content of the conversations. In many cases, this information is available to the platform provider and may be stored on the devices after the communication ends.

Digital platforms designed to be used by for-profit sales companies or other industries collect even more data, with the intention of helping their customer (your program) collect, retain, and synthesize as much data as possible about those you engage with.

This excessive data collection can be problematic for survivors' privacy and your program's confidentiality obligations. Most domestic violence and sexual assault programs are legally and ethically obligated by confidentiality laws and regulations to ensure that the program does not disclose client information to external parties, such as a platform vendor. Select a vendor that allows you to

collect only the information you actually need and allows you to control what your program discloses to the vendor. You should also review the company's privacy policies to learn about how they share data they collect from their users. For more information, read our FAQs on Record Retention & Deletion.

When talking with a potential technology vendor, ask what information they collect, store, and can access (in addition to reviewing their privacy policy). This includes during their regular course of business, but also in response to legal requests for information of their users. Ask what identifying information the technology itself incidentally collects, such as users' IP address, browser history, date and time of conversations, etc. For a full list of questions when choosing a vendor, use our Choosing A Vendor Checklist to help guide your decision-making process. If you have questions about specific platforms, you can reach out to us for assistance.

Customer Service

A final factor to consider is customer service. Depending on the platform you choose, the customer service will vary. Some platforms have a support form that is set up to receive concerns, ranging from reporting abusive content to forgotten passwords. Other platforms have a dedicated business support team that will respond more quickly, while others have no customer service at all. Some companies may charge a fee for more in-depth customer service. Do your research and read reviews or speak with others who have used the platform to learn if they are responsive and helpful to their customers.

Consider whether your staff and the survivors who reach out to you would be able to easily troubleshoot any technical issues that arise. Or perhaps you might have IT staff or consultants who can troubleshoot technical issues. If you don't have the ability to troubleshoot technical concerns, and the vendor doesn't have a dedicated or quick customer service response, this might result in your service being down longer than you want.

Service Downtime and Cancellation

Some vendors may take their services offline for a variety of reasons, including unplanned outages, upgrades and maintenances, or they shut down. Ask your vendors how they handle unplanned outages. Do they notify customers when an unplanned outage occurs? If so, when and how? Ask your vendor if they take the service offline to perform upgrades and maintenances. If they take the service offline, how often and how long does that take? Will users be required to re-download the software or app after the upgrade? And finally, what is their notification plan with their customers if they shut down or sell their service?

Next Steps

Cost, features, data security and privacy, customer service, and service downtime need to be considered as a whole, since they impact each other. A platform that is relatively low in cost might not provide the features you need or the data security you require. Some platforms may have features that could be a privacy risk for survivors or put you at risk of violating confidentiality. To assist with this, review NNEDV's various guides, including:

- Choosing a Vendor Checklist
- Digital Services Best Practice Principles

© 2019 National Network to End Domestic Violence, Safety Net Project. This resource is funded through a grant from the Office for Victims of Crime, Office of Justice Programs, U.S. Department of Justice. Neither the U.S. Department of Justice nor any of its components operate, control, are responsible for, or necessarily endorse, this resource (including, without limitation, its content, technical infrastructure, and policies, and any services or tools provided)

We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.