OHIO VICTIM WITNESS ASSOCIATION
OVWA

Cybersafety Guide for Advocates and Allied Professionals

March 2021

Contents

Contents

Preface & Purpose

SPECIAL THANKS

OVWA wishes to extend a special thanks to our content expert, Bill Wagg, Client Care Specialist with thinkCSC. For central Ohio businesses, government, and education communities, thinkCSC is an IT services firm that invests in their clients' success for over 25 years. To learn how thinkCSC can help your business, please visit their website at www.thinkcsc.com.

As we become more and more connected, we become more vulnerable to cyberattacks. From smart refrigerators, connected thermostats, and IP video cameras, everything can be breached. And every day, there is a new breach. Cybersecurity should be on everyone's mind, but Bill Wagg lives and breathes it, maintaining a singular focus on keeping organizations safe and encouraging everyone to be more proactive about keeping data safe.

Bill's unique blend of coach, teacher and evangelist of all things cybersecurity fuels his passions. Helping organizations maintain data security while protecting the privacy of their clients and end users drives Bill. He spends much of his time educating organizations on how to adhere to both security regulations and best practices around cybersecurity and provides countless trainings to organizations to help them be more cybersecure.

For the last seven years, Bill has worked with thinkCSC clients and vendors to improve their cybersecurity knowledge and believes that every person has a part to play in improving data security. Every business needs a policy and a plan in place to protect them not just from today's threats but tomorrow's threats, too. With 53 different security certifications, Bill is in an excellent position to help ensure every organization has access to cutting edge cybersecurity solutions

ACCESSIBILITY STATEMENT

The authors and partners of this publication believe in accessibility for all individuals. This document is available in alternative formats upon request to OVWA. Contact information for OVWA can be found on the last page of this guide. Please allow for sufficient time to arrange such accommodations.

ELECTRONIC ACCESS

This guide can be downloaded from OVWA's website at www.ovwa.org/best, under OVWA Publications.

DISCLAIMER

This guide includes information about technology that is current at the time this guide was developed. Please know that due to the ever-changing world of technology, some aspects of this guide may change.

The views and opinions expressed in this publication are those of the authors and do not necessarily reflect the policies or position of any agency. Examples provided in this publication are simply examples. Assumptions made are not

reflective of any agency or victim rights organization. The following information has been collected from extensive research, learned experiences, and expert opinion.

This guide was supported by grant number 2021-VOCA-134145796 awarded by the Office for Victims of Crime, Office of Justice Programs, U.S. Department of Justice through the Ohio Attorney General's Office. Victims of federal crimes will be served.

A WORD ON LANGUAGE

For simplicity, you will see that the terms "victim" and "survivor" are used interchangeably throughout this guide. The word "victim" is used by members of law enforcement, advocates, and the courts within the context of the criminal justice system, but for many organizations, "survivor" speaks to the empowerment advocates and allied professionals encourage in the people served. Ultimately, it is imperative to follow the lead of the person seeking support since the journey from victim to survivor varies. To that end, many are beginning to use the term Victim/Survivor to represent this continuum[1]. For more generalized discussions throughout this document the term "client" may also be used in reference to victims/survivors.

[1] Women Against Abuse, www.womenagainstabuse.org/education-resources/the-language-we-use

Introduction

Technological capabilities change frequently and thus it can be difficult to remain vigilant against the many possible ways information may not be secure. Managing victim/survivor information now requires understanding the manners in which information needs to be kept secure.

Though advocates may have a cursory understanding of cybersafety for their clients, chances are they may not know enough to advocate in the best possible manner for not only the client but within the office in which they provide services. The internet today is far more intricate than ever imagined, and this guide aims to make cybersafety and security easier to understand and more importantly, easier to manage for service providers.

This guide is meant to be a companion piece to the recently released **Cybersafety for Victims of Crime** which details the manner in which a survivor may be monitored or tracked, how to preserve evidence, and how to identify an individual's online presence to promote changes that will allow survivors to safely access technology, the internet, and social media.

While a victim/survivor is not all but guaranteed to hear, "Why don't you change your number? Block them? Stay off social media? Shut down Facebook?", advocates know that this is not only unfair and complex but can in fact increase the level of danger if the offender escalates after losing that means of monitoring and/or harassment.

Increasing advocate knowledge so to maintain a safer online presence allows for effective victim/survivor safety planning around technology. To start, we feel it important to provide some definitions that will provide a foundation to successful learning as you read and reference this guidebook. The following information will be useful as you continue to work with victims/survivors towards cybersafety.

This guide will provide advocates and allied professionals with the following:

- A basic education on the parts of the internet and how those parts may impact advocate and survivor safety
- Technology and evidence collection
- Confidentiality and consent
- Best practices in maintaining secure office technology
- Resources for designing and implementing program policies
- Virtual advocacy guidelines
- Social media ethics for advocates

The Internet

The internet is a massive web of networking infrastructure. It connects millions of computers together globally, forming a network in which computers can "talk" to one another as long as both are connected to the internet.

Information that travels over the internet does so via a variety of languages known as protocols.[2] The internet is used every day. It is where every indexed site lives. An indexed site is a site that has been crawled, indexed, and identified by major search engines such as Google, Yahoo, and Microsoft. A web crawler, also known as a "web spider" or "web robot", is a program that browses the World Wide Web in a methodical, automated manner. This process is called web crawling or spidering.[3]

Many legitimate sites use spidering as a means of providing up-to-date data. Search engine companies use bots to visit websites on the internet and track their data. This process allows Google to know where to direct you when you're searching for something.

WHAT IS THE WORLD WIDE WEB?

The World Wide Web, or simply "web", is a way of accessing information over the medium of the internet. It is an information-sharing model that is built on top of the internet. The web uses the HTTP protocol, one of the computer languages spoken over the internet, to transmit data. Web services, which use HTTP protocol to allow applications to communicate in order to exchange business logic, use the web to share information. The web also utilizes browsers, such as Internet Explorer or Firefox, to access web documents called webpages that are linked to each other via hyperlinks. Web documents may also contain graphics, sounds, text, and video.

WHAT IS THE DEEP WEB?

The **deep web** is a subset of the internet that is **not indexed** by the major search engines. Not indexed means that there are websites that need to be visited directly instead of searching for them on a search engine. These non-indexed websites don't include directions on how to find them however, if you know the direct web address, then you can access them.

Here are a few examples of what is on the deep web:

- The content of your personal email accounts
- The content of your social media accounts
- The content of your online bank accounts
- Data that companies store on their private databases
- Content contained within scientific and academic databases
- Medical records
- Legal documents

[2] www.webopedia.com/DidYouKnow/Internet/Web_vs_Internet.asp
[3] www.sciencedaily.com/terms/web_crawler.htm

Many companies use the deep web for things like remote connectivity, large data sets, security, and anonymity. There is only so much information that data search engines can crawl and index making the deep web a perfect place for these websites to live.

WHAT IS THE DARK WEB?

The **dark web** is a subset of the deep web. The dark web is not only **not indexed** but also requires special credentials or authorizations to be able to access it and often uses a unique customized communication protocol. The dark web often sits on top of additional sub-networks. A sub-network is a smaller network inside of a larger network like Tor, I2P, or Freenet. Two common types of the dark web are social networks and networks specifically used for maintaining anonymity. Often associated with criminal activity of various degrees, there are some legitimate uses including anonymizing reports of domestic abuse, government oppression, and other criminal reports.

Dark websites look like any other site but there are important differences. One is noticeable in the naming structure of the website URL. Instead of using ".com", dark websites end in ".onion". This allows the dark websites to maintain their anonymity. Dark websites also use a scrambled URL naming structure that makes the websites impossible to remember. However, not everything is illegal on the dark web. There's also material you would quite possibly find on the public web.

Here are a few examples of what is on the dark web:

- The content of your personal email accounts
- The content of your social media accounts
- The content of your online bank accounts
- Data that companies store on their private databases
- Content contained within scientific and academic databases
- Medical records
- Legal documents

Technology and Evidence Collection

When a cybercrime has been committed, investigators may try and gather **metadata** to track and document evidence that the crime has been committed.

Metadata is data about data.

In other words, it is information that is used to describe the data that is contained in something like a web page, document, file, or picture. Another way to think of metadata is as a short explanation or summary of what the data is.

> There are many types of metadata including Descriptive, Rights, Technical, Preservation, and Markup. These different types include the title, subject, copyright status, file type, navigation and interoperability of the data.

Why is this metadata important to advocates and victims of crime? Analyzing the metadata in pictures and messages can show the GPS data, including where, when, and how the pictures or messages were sent. This type of data is considered “EXIF data”.

Another way to find the origination of a message is through the IP address of a computer or phone. IP addresses are the numerical label assigned to each device connected to a network. IP addresses can be tracked and traced back to devices and locations.

IP addresses are the equivalent of a mailing address in the material world. Every computer or device that can connect to the internet is assigned an IP address. When connected to the internet through internet service providers, IP addresses can be connected to a physical address like someone’s house. An internet service provider is an organization that provides services for accessing, using or participating in the internet. Another way to track IP addresses is through metadata. Often metadata collects the device’s IP address and can be tracked.

Both metadata and IP addresses can be used to trace online activity back to a specific user or computer. This process is typically initiated by law enforcement through the use of search warrants and subpoenas. Some of this information can be captured by the victim when documenting and/or sending evidence to law enforcement, and it is important to understand how this can be done in order to best help a victim preserve essential evidence. Metadata is stored directly in the document, image, or video file. It is important to get a copy of the data as quickly as possible so the data cannot be deleted.

Google Location Data vs. Cell Tower Records

Most advocates are aware of a common evidentiary practice by law enforcement in tracing calls, texts, and the location of an offender through cell tower records.

You may have heard the phrase “pinged off a tower” and its relationship to a general location. Cell tower records are only accessible through a subpoena and are connected to a phone, not necessarily the user, therefore it is important to establish that the phone was used primarily by a specific person. Another source of data that has been used in this evidentiary practice is Google location data. If access to the physical phone or Gmail account can be obtained, the device’s location history can be accessed through a simple search.

> The evidentiary benefit of Google location data can be greater than cell tower records because the Google location is more specific and identifiable than a cell tower ping, which only narrows the location to a general vicinity.

Google location data provides coordinates that can place a phone in a very specific location; a business, dwelling, etc. However, this data relies on a person not turning their location settings off. Location tracking must be on to capture the information.

Conversely, while it can be helpful to law enforcement when tracking an offender, this information can be used by an offender to track the victim if they have access to their Gmail account and password. For this reason, the possibility and potential benefits of disabling Google location services is important to explain to a victim/survivor during the process of safety planning. Both Google maps and Apple maps can function as a location service. Location services work by keeping track of your location to provide custom routes, directions, and location-aware services. These location services also provide data to companies like Facebook, Yelp, Fitness Apps, and Twitter.

All of this data is accessible to a user of these apps and websites and could be useful in court cases, however this data is also available to anyone with the login and password. A victim/survivor could unknowingly be giving out their locations to their abusers or other criminals. Disabling location settings may be beneficial if there is a concern that they are being used for tracking. More information on how to do this can be found in the guide, **Cybersafety for Victims of Crime**, or by using a simple internet search.

How to Access Location Data

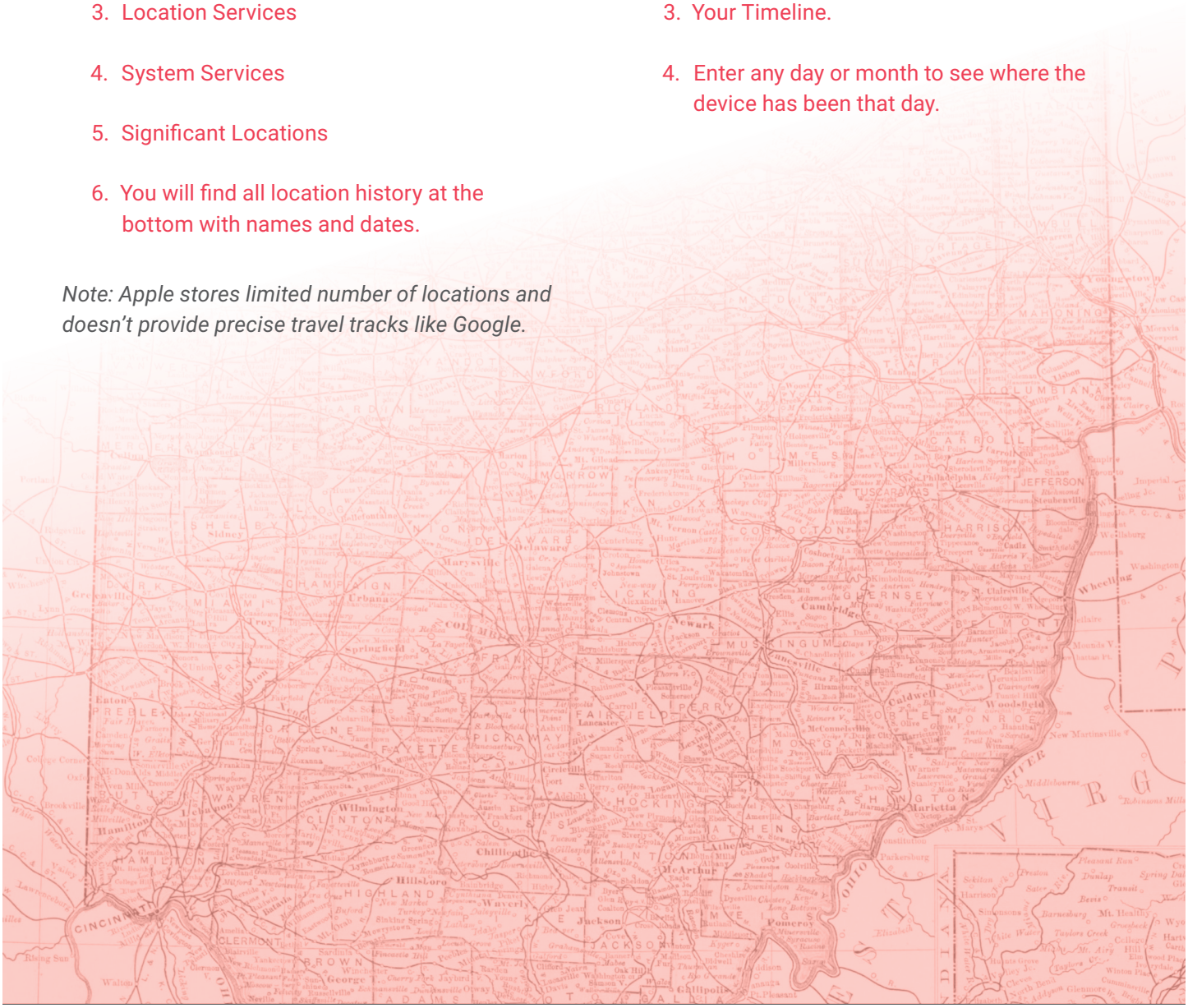
To access Apple Maps location data, click on the following on your device(s) settings:

1. Settings
2. Privacy
3. Location Services
4. System Services
5. Significant Locations
6. You will find all location history at the bottom with names and dates.

Note: Apple stores limited number of locations and doesn't provide precise travel tracks like Google.

To access Google Timeline, click on the following on your device(s):

1. Go to the Google Maps app on the device.
2. Click on the Account Circle.
3. Your Timeline.
4. Enter any day or month to see where the device has been that day.



Obtaining Social Media Records

Social media platforms allow the user the ability to download data and activity and provide law enforcement with more specific instructions to obtain records. Twitter, Facebook, TikTok, Instagram, Reddit, 4chan, 8chan are all common social media platforms. Reddit, 4chan, and 8chan have been found to hold more criminal activity.

Social media apps, like most apps on your phone, collect data about you. The apps track what device is being used when you are connected. If you or a victim/survivor use apps like Facebook, Twitter, or Instagram, your location data and records of every phone call you make are being collected. Individual users have the right to request their data from all of these companies however, they all have different requirements to get that data. Users have the ability to turn off these companies' data collection but many times the apps won't work when they are not collecting data. In addition, these companies have been fined by multiple countries for not turning off data collection on the apps when they said they had. Below are steps on how users can obtain their data from Facebook and how users can manage their activity on Google and Twitter.

Retrieving your Facebook data:

- Open your Facebook app.
- Go to Settings.
- Click on Download My Data.
- You will then make your request and await Facebook to compile your data.
- Facebook will send you a link. The longer you have been on Facebook, the longer the request will take.
- Once the file arrives double click to open the index.htm and it will open in an internet browser.

How to delete your activity on Google by device:

The steps needed to delete activity on Google are extensive and vary by type of device used by the user. We recommend visiting the below website to learn more about deleting Google activity according to the specific device used.

https://support.google.com/websearch/answer/465

Retrieving Your Twitter History and Data:

- Open the Twitter app.
- Click in the upper left corner to open the home screen options.
- Go to Settings and Privacy.
- Click on Account.
- Go to Your Twitter Data.
- Confirm your password to download an archive of your data.

Manage your Twitter location information:

Twitter uses your location to personalize your user experience on their platform. Twitter uses information such as your current location and where you are when you are signing into the app to show the user relevant content. When this setting is enabled, Twitter may also personalize the platform to places you have been in the past. To disable this setting, follow the steps below:

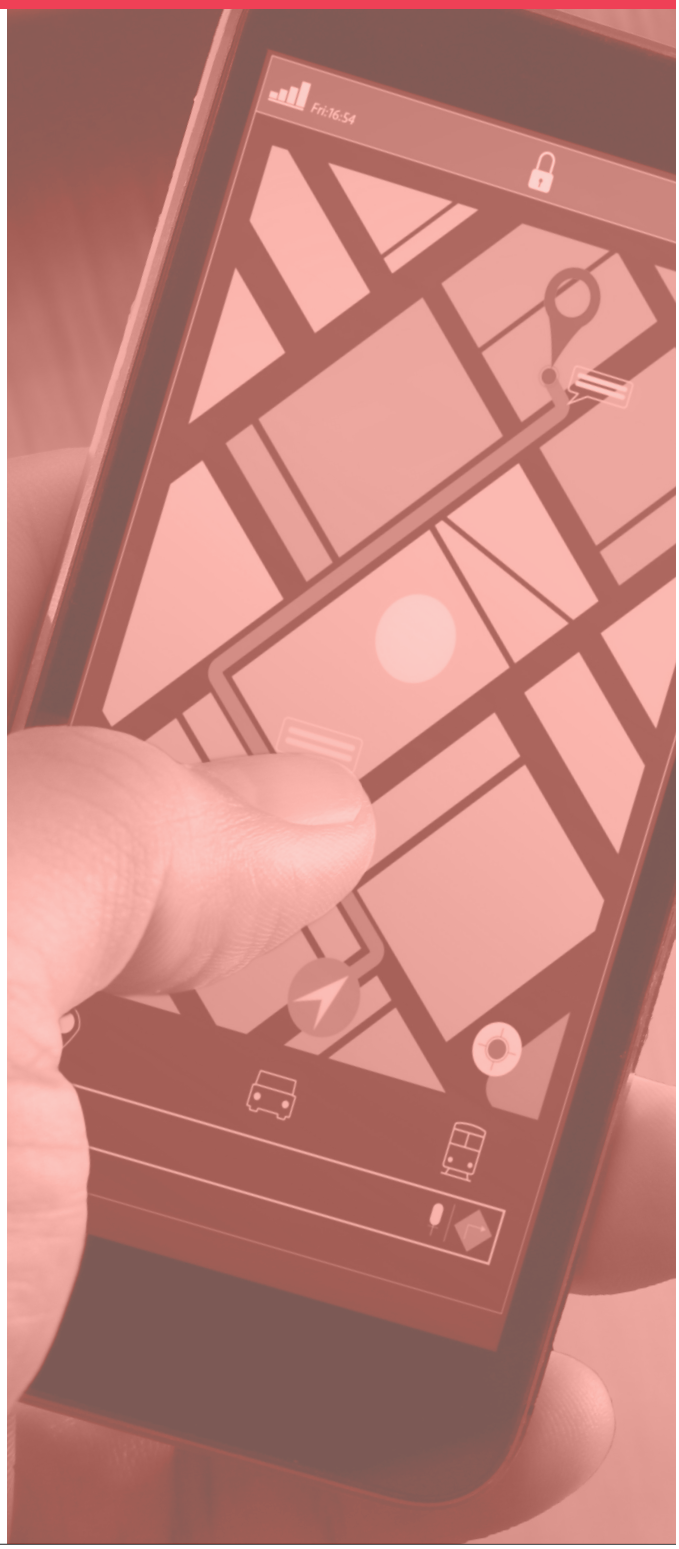
- Open the Twitter app.
- Click in the upper left corner to open the home screen options.
- Go to Settings and Privacy.
- Click on Privacy and Safety.
- Scroll down to find the section titled Location.
- Click on the arrow for "Precise Location" to disable this setting.

GPS Detection

Some people use technology—such as photos, videos, social media, and dating apps—to engage in harassing, unsolicited, or non-consensual interactions.[3] This is a very traumatizing and vulnerable position to be in.

Additional tracking applications can be downloaded and installed on any mobile device. This practice is common for victims of domestic violence when the offender wishes to track their location. Advocates might be approached by their clients telling them that their offender is showing up in their same vicinity or location. This might be a sign to have the victim check their GPS and location services on their devices and apps they frequently use.

GPS tracking applications can be applied to devices when an offender has both access to the device and the password for the app store (e.g. Apple App Store) to download and install them. Sometimes tracking apps can be hidden and hard to detect. If a victim believes that they are being tracked via their mobile device, they should take the device to the police so they can copy the data. Law enforcement routinely removes data from victim/survivor personal devices to prove that crimes have been committed. Copying the data will allow for proof of the tracking. Victims/survivors might share their concerns about their personal devices being reviewed by law enforcement. When these concerns are brought up, it is important they share those concerns with their advocate and/or law enforcement. More information on GPS tracking applications can be found in the OVWA guide, **Cybersafety for Victims of Crime**.



[3] "Using Technology to Hurt Others", Rape, Abuse & Incest National Network (RAINN), www.rainn.org/safe-tech

Confidentiality and Consent

Many victim service programs receive federal and state grant funds to operate.

The Violence Against Women Act (VAWA), the Victims of Crime Act (VOCA), and the Family Violence Prevention and Services Act (FVPSA) contain strong confidentiality provisions that limit the sharing of victims' personally identifying information, including entering information into public records and databases. The National Network to End Domestic Violence (NNEDV), the U.S. Department of Justice, and the Victims of Crime Act (VOCA) Administrators developed online resources to assist federally funded victim service organizations with their confidentiality questions and concerns. While this guide will not elaborate on the federal guidelines, below are three resources focused on confidentiality and other grant provisions to help organizations ensure confidentiality of information.

It is vitally important to remember that a victim's personal information is their information. It belongs to them. An important part of advocacy is supporting a victim on their road to becoming a survivor. This includes providing various levels of support they can feel safe to be open, truthful, and transparent about the personal data that is collected. However building that safe space with victims can be difficult when the advocate is not open, truthful, or transparent about how that personal data may be used.

- **National Network to End Domestic Violence**
  "Confidentiality: VAWA, FVPSA, and VOCA"
  https://www.techsafety.org/confidentiality-in-vawa-fvpsa
- **National Network to End Domestic Violence**
  "Confidentiality Toolkit"
  https://www.techsafety.org/confidentiality
- **U.S. Department of Justice Office for Victims of Crime Victims of Crime Act (VOCA) Administrators**
  "VOCApedia"
  https://ovc.ojp.gov/program/victims-crime-act-voca-administrators/vocapedia

Discussing what information needs to be obtained, how it will be used, and who will see it allows the individual to make an informed decision about what, when and how to share personal information. Incorporating this trauma-informed support into daily advocacy with survivors allows the survivor the choice to share or not share their personal information.

Example: If a release of information needs to be signed by a survivor at any time for any reason, it is essential that the survivor knows the release can be changed or made inactive at any time at their request.

Maintaining Secure Office Technology

When considering the confidentiality of victim/survivor information and how it is managed in the office, taking physical measures to protect this information must be a priority.

Physical measures may include locking filing cabinets, keeping active files in locked desk drawers instead of on desks or workspaces, and closing doors to decrease the probability of others hearing confidential information. In our increasingly technological world, confidentiality in the context of other daily operations can get overlooked. Our daily use of technology also means that we tend to respond automatically to situations without thinking of confidentiality of information when it comes to cell phones, databases, computers, emails, and printers and copiers.

PHYSICAL SPACE MISTAKES

Assessing the physical space in which you meet with survivors is the first step towards fostering a perceived sense of safety. Below are some of the most common ways victim/survivor information is breached in a physical space:

- There is a **lack of private meeting space** that is not separate from other professionals or offices. Not having a private meeting space allows for conversations, both in person and virtually, to be overheard.
- Files containing victim/survivor information is **left open and unsecured** on desks, in courtrooms, in offices or in some cases, removed from the building.
- **Confidential information is shared** between advocates and other personnel in a public area.
- **Computer screens and applications** are left open giving access to survivor information.
- **Fax machines and copiers** are unsecured in a public or non-private location.
- Computers and work phones issued to employees are **removed from the office** and not secured.

Many advocates work in an office that has an IT department or partners with an external agency to ensure that the program's technology and equipment is protected and running smoothly. While your IT service works to keep systems secure, who has the responsibility of securing confidential client information?

Here are some steps you can take to keep their information safe and secure.

- Hold calls with victims/survivors in a **private area** separate from co-workers and other clients
- When leaving your desk, **lock your computer screen** to ensure that when walking by, other co-workers don't see private victim/survivor information. All employer-owned machines should be locked down as much as possible while still allowing employees flexibility to do their jobs. Unless there is a special reason for it, no users should be local administrators to their own machine. This means they do not have the ability to download or upload applications onto the computer without specific permissions.
- **Job-specific data** should be saved on a centralized server or Cloud appliance and then backed up regularly. No personal or outside data should be placed on employer-owned machines.
- If you're forwarding an email, review it to make sure it does not contain any information specific to a victim/survivor. Email is an **inherently unsecure** form of communication. No email communication is encrypted unless you are using specific encryption software. Emails can be intercepted, copied, and forwarded without your knowledge. By encrypting emails, the data within the email will not be able to be seen in the event it is intercepted.
- When you are making copies of documentation that contains victim/survivor information, make sure to **get all copies off of the printer** not leaving any behind.
- Also, consider **deleting the data storage** on shared office printers. These large capacity printers will store data of items copied or printed. To maintain confidentiality, consider deleting this data.
- **Don't talk about confidential information** relating to clients outside of your professional workspace. If you are given permission to share sensitive or confidential information, make sure you and your client are both completely clear about who you have permission to share information with and in what circumstances.
- Make sure all computers, databases, and email accounts require **log-in credentials** for each staff person.
- Is your database used to manage survivor information on a **personal server?** If not, is the server located in the Cloud? Who owns the data and do they have access to the data?
- **Do you own your data** with your database software provider? Owning your data is very important so that if you ever have to change to another database, your organization will retain the data you have already entered. Some software developers will contractually own your data. This means that anything you have entered into the system will no longer belong to your organization and it will be impossible to keep it confidential.

Policy Development

Your agency or program may already have policies and procedures in place for technology, phones, internet, and computer use within a professional setting.

Victim advocacy organizations may consider the development of policies and procedures for cybersafety, both for employees and for survivors served. Developing internal policies and procedures is another layer of protection that programs can take to protect information. These internal policies and procedures also uphold the program's services to a high level for consistent and quality services. However, developing and implementing effective policies and procedures can be a daunting task. Fortunately, other organizations have developed guidelines for the creation of such policies!

THE NATIONAL NETWORK TO END DOMESTIC VIOLENCE

www.techsafety.org/confidentiality-templates

Included with the "Confidentiality Toolkit", the National Network to End Domestic Violence (NNEDV) developed templates for programs working with survivors. The toolkit includes templates focused on:

- Notice of Rights and Confidentiality Forms
- Releases of Information
- Intake Forms
- Documentation Retention Policy
- Visitor Confidentiality Agreement
- Confidentiality, Privacy, and VAWA
- Collaborative Partnerships and Confidentiality
- Memorandums of Understanding
- Co-located Partnerships

THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

www.nist.gov/itl/smallbusinesscyber/planning-guides

The National Institute of Standards and Technology (NIST) compiled comprehensive information for small businesses in planning and developing cybersafety plans.

U.S. DEPARTMENT OF JUSTICE CYBERSECURITY UNIT, COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION

https://www.justice.gov/criminal-ccips/file/1096971/download

The U.S. Department of Justice Cybersecurity Unit, Computer Crime and Intellectual Property Section developed *"Best Practices for Victim Response and Reporting of Cyber Incidents"*.

Serving Survivors Virtually

Under routine circumstances, victim/survivors, of all backgrounds and abilities, face barriers to accessing support and the criminal justice system.

With the onset of the global pandemic in 2020, new barriers became evident that required creative solutions in how advocates and allied professionals responded to the needs of victim/survivors. These changes impacted crime victim safety, public safety, and had the potential to violate crime victims' rights. Advocacy programs had to quickly determine how they were going to continue to serve victims/survivors safely while adhering to state and federal guidelines. This required innovative thinking and partnerships that have defined a year in our field.

More and more programs began to provide services virtually to meet the needs of victims/survivors however, this too created service concerns. Many victims/survivors did not have access to technology for virtual platforms; victims/survivors didn't understand how to use the virtual platforms; potential victim rights violations; and if victims/survivors were not able to participate and exercise their rights at hearings, the courts may have sought reconsideration that requires additional hearings and therefore more involvement within the criminal justice system.

Advocates faced their own set of concerns. Advocacy programs may not have had access or funds available to implement virtual advocacy; researching safe and confidential virtual platforms became a full-time job and outside of their scope; there was a lack of availability of equipment for remote work; accessibility to records and information was limited; and new processes had to be developed to ensure that victims were being notified and able to participate in the criminal justice process. Advocates became experts in teleconferencing while becoming skilled at conveying empathy and support virtually.

Eventually, our programs will return to their traditional ways of providing services however, many have learned that virtual services may be the key to equitable and accessible practices for many victims/survivors. Being able to provide virtual service delivery options expands a program's outreach and reduces the risk of victims/survivors going without services simply because they are not face to face. As programs continue to provide virtual services, here are some guidelines to consider for accessible advocacy.

Virtual Advocacy Considerations

- The criminal justice process can be **confusing and daunting** without these new barriers so it is important to clarify expectations and provide victims/survivors with thorough descriptions of what to expect. Their anxiety about participating in proceedings may be increased given the new formats available so it is important to take a bit more time and explain the process thoroughly in a trauma-responsive manner.
- Now that programs are in a place where **teleconferencing platforms** are being used to provide services, this is an opportunity to look at the confidentiality and accessibility of all services and internal systems.
- There are countless teleconferencing platforms however, in order to maintain confidentiality, finding an **end-to-end encrypted platform** is a priority.
- **Virtual platforms are not a one-size-fits-all.** Do some research and choose the platform that is most easy to use for staff working remotely and for victim/survivors. Choose a platform that is most comfortable for the victim/survivor being served, has the accommodations necessary to meet their needs (e.g. closed captioning) or dual screen options for interpreting, and is equipped to provide the victim/survivor with a full range of participation.
- **Practice the virtual platform** with your colleagues before using it with a victim/survivor. Practice muting the other individual and learn how to instruct someone to turn off their camera or mute themselves. Be conscientious to what the victim/survivor might see from their view while on the virtual platform. Can they see the defendant? Can the defendant see them? Utilize skills that you would in-person to ensure the victim's/survivor's safety and well-being but through the virtual platform.
- Use the virtual platform to take the victim/survivor on a **tour of the courtroom or the program.** Coming into a courtroom or new environment while in the aftermath of a traumatic event can be overwhelming and can be a trigger. Doing a virtual walkthrough can be a safe option for victims/survivors who wish to participate in the criminal justice process or in your services but need some extra support.

Social Media Ethics for Advocates and Their Programs

Introduction

For victim advocates to be effective, establishing a safe and trusting relationship with those they serve is paramount.

To help guide these relationships, professional boundaries define what is appropriate in interactions with victims and colleagues that allow for safe and respectful connections. Boundaries exist to protect both the victim advocate and the person being served. Ultimately, the importance of maintaining ethical standards in advocacy work cannot be overstated.

Using social media can be both an accessible way for programs to provide victims/survivors with connection and support while simultaneously unleashing a whole host of ethical dilemmas for the advocate and their program. There are several ethical codes available to victim advocates and allied professionals. Many of these ethical standards are focused on relationships with victims; relationships with colleagues, other professionals and the public; and for the advocate's overall professional conduct.

While this publication does not cite any one code of ethics as the ultimate authority, it does recognize that there have been great strides in the professionalizing of the advocacy field that has resulted in the development of several progressive ethical codes. Some programs may choose to adopt a code of ethics within their program as a form of internal policies and procedures while some advocates may choose to become professionally credentialed therefore committing to following a code of ethics embedded within their certifications and licensures.

- **National Organization for Victim Assistance (NOVA)**
  Code of Professional Ethics for Victim Assistance Providers
- **U.S. Department of Justice, Office of Justice Programs, Office for Victims of Crime**
  Achieving Excellence: Model Standards for Serving Victims and Survivors of Crime
- **Prosecuting Attorney's Council of Georgia**
  Code of Professional Ethics for Victim Witness Assistance Providers

The following content has been influenced and inspired by the experiences of advocates in the field as well as the following social media ethical guidelines set forth by the American Psychological Association and the National Association of Social Workers. This information is designed to aid advocates, allied professionals, and their programs in navigating the technology-driven communication tools and social media platforms that are so widely used by professionals and clients alike.

- **American Psychological Association.** (2010). Ethical principles of psychologists and code of conduct. Retrieved from www.apa.org/ethics/code/index.aspx
- **National Association of Social Workers.** (2015). Code of ethics of the National Association of Social Workers. Retrieved from www.naswdc.org/pubs/code/code.asp
- **National Association of Social Workers, Association of Social Work Boards, Council on Social Work Education, Clinical Social Work Association.** (2017) *NASW, ASWB, CSWE, & CSWA Standards for Technology in Social Work Practice.* Retrieved from NASWCulturalStandards2003.Q4.11 (www.socialworkers.org)

The following ethical guidelines are divided into four sections: Social Media Ethics for Programs, Social Media Ethics for Advocates, Dual Relationships, and Professionalism and Social Media.

Social Media Ethics for Programs

Social media can be used to connect with others and act as a means to provide information. Advocacy programs usually develop a professional social media page in addition to maintaining a central website. Programs widely use Facebook, Twitter, and Instagram as vehicles to provide information that is both accessible and equitable for victims/survivors. While greatly beneficial, there are several important factors to consider in order to maintain ethical standards, confidentiality, and boundaries while maintaining an effective social media presence.

INFORMATION SHARING & MANAGING COMMENTS

Posts shared on social media can contain powerful messages that can positively affect victims/survivors however, if the same post also contains information or opinions that alienates a group of people then the sharing of that information can do more harm than good. Some examples would be sharing posts and information that seek to disenfranchise victim/survivors of color; posts that invalidate the experiences of sexual assault survivors; or sharing information that uplifts celebrity perpetrators. Such ill-reviewed posts can degrade the program's reputation and decrease victim/survivor trust in the program.

In an effort to be proactive, it is wise to expect that anything you post, share, or retweet from your professional page will be viewed by clients, their family, friends, and/or allied professionals. Additionally, the re-sharing of information requires attention to the comments that may be made in reaction to the information. Having a dedicated staff member who monitors the program's social media presence is invaluable. This staff member can monitor comments and content that may be abusive in nature and manage those comments that may be considered harmful for victims/survivors and program staff.

While many advocacy organizations are open to the dialogue and see it as an educational opportunity, there can become a point where the dialogue becomes harmful and unhelpful.

> Consider developing internal procedures that outline steps to take when such dialogue becomes harmful. Internal procedures provides the program with some measures of accountability and support to the dedicated staff member.

ADVOCACY THROUGH SOCIAL MEDIA

Social media can be used as a tool for communication with victims/survivors to connect safely with support programs. Younger generations may feel more comfortable reaching out via social media than calling in to an office or sending an email. Social media platforms can provide excellent accessibility options to persons with disabilities as well in their efforts to reach out to advocacy programs.

Upon receiving the information from the victim/survivor on social media, programs should provide the victim/survivor with a disclaimer ensuring that they understand the limitations and privacy concerns when using social media sites as the primary form of communication. Programs can include a statement on their social media notifying victims/survivors of the program's preferred method of communication. For example, some victims/survivors might find it appropriate to write their request for help in the comments section of a post from the program. The program would do well to contact that client via private messaging on the platform, if possible, and redirect the conversation to a more private space. The program can then take the steps to delete that victim/survivor's comment so to maintain confidentiality of their request for services.

> Consider developing internal policies and procedures for how services can be provided via social media, diverted from social media, and how records can be retained from social media platforms for documentation within your program.

CLIENT'S CONSENT FOR COMMUNICATION

It is important to be transparent with a victim/survivor regarding your use of social media and technology to communicate. In doing so, it becomes easier for the advocate to assess the preferred and more easily accessible means of technological communication with the victim/survivor; provides the advocate with an opportunity to discuss confidentiality; and provides the opportunity to obtain the victim's/survivor's consent before using technology or social media. Failure to discuss or obtain consent from the victim/survivor constitutes a breach of trust and impedes the effective and transparent advocate and client relationship.

Advocates and their programs can develop statements notifying victims/survivors of the privacy concerns and limitations when communicating via social media and request that the individual provide written consent to continue communications on that platform.

> ### Here is an example of such a statement:
>
> "Thank you for reaching out to (agency name). The information you share on this platform will be kept confidential to the greatest extent allowed by law. Please be aware that (agency name) cannot guarantee the confidentiality and privacy of any information that you should share on this platform. To ensure confidential communication you may also contact us at (agency's preferred contact methods). If you prefer to continue communications via this platform, please provide us with written consent."

> ### A victim's/survivor's written consent could look like this:
>
> "I consent that (agency name) can continue communicating with me via mobile phone, messages, email and online communications, provided that these communications comply with agency policies and privacy regulations."
>
> When in doubt, the victim/survivor, the confidentiality of their information, and their lived experiences always come first. As advocates and allied professionals, it is our responsibility to place respect for the victim/survivor at the center of any ethical decision. By doing so, you can swiftly determine the correct course of action.

FREQUENT MONITORING

Hacking of social media sites is not unusual therefore diligent monitoring is a must for any advocacy program's social media presence. If a victim/survivor should happen to reach out to the program via social media in an emergent situation, they need to be aware of how frequently the page is checked, alternate and/or preferred contact information, and contact information for a 24-hour emergency provider.

Facebook's messaging allows for programs to develop an automatic response that is sent to anyone who contacts the program via social media through private messaging. This is a great space for programs to include the above information so that victim/survivors in immediate need can receive the services they are seeking.

> Consider developing language to include in an away message for your social media messaging platforms as well as internal procedures to ensure that social media accounts are monitored regularly.

TECHNOLOGY EDUCATION

Programs may find the use of social media as an alternative way to educate the public and victims/survivors about safety when using social media and technology. Many victims/survivors continue to experience safety concerns even after their lived experiences because offenders and their cohorts can use technology to locate, harass, threaten, and harm a victim/survivor. Because of the ongoing evolution of technology and its use in our daily lives it is important that advocates stay educated on how technology can be used to victimize others.

> Programs should consider developing internal policies and procedures that also require staff to receive regular training so that they are apprised on the continuously evolving uses of technology and how it can be both harmful and helpful.

DEVELOPING A SOCIAL MEDIA POLICY

To ensure accountability and support ethical services, programs can consider developing internal policies and procedures that outline the expectations of employee use of social media when it comes to what is deemed unacceptable behavior. Policies may include the following:

- **Definition of social media** – You may wish to clearly define what social media is for less ambiguity. Social media can also include blogs, forums, video sharing and other networking apps.
- **Departmental roles and expectations** – Who is responsible for what and how is it done.
- **Response plans** – Occasionally, a quick response to a negative post or misinterpreted information is necessary. Having a response plan identifies who is responsible and what needs to be done when swift action is required.
- **Legal compliance** – This section of the social media policy addresses any legal compliance as directed by the company.
- **Brand identity and reputation** – Provide employees with guidance on the language to use when discussing the company including when and how they should respond to posts or comments about the company.
- **Regulatory awareness** – Identify the difference between public and private information so that employees can be aware of what is allowed to be shared and what is not.
- **General prevention** – Clarify what is and what isn't appropriate for social media can reduce the number of inappropriate actions.
- **Open communication** – Having a social media policy encourages open communication between leadership and employees. It also allows for concerns to be addressed before they become issues.
- **Clear expectations** – When employees know the company's expectations, they'll be less likely to post anything that will negatively impact the program.
- **Personal social media use** – Providing employees with a clear explanation of expectations for employee's personal social media accounts sets clear boundaries for professional behavior online.
- **Responses to outside posts** – Employees may feel compelled to respond to posts about the company from their personal social media accounts and this part of the policy provides them with appropriate ways of doing so.
- **Consequences** – Give a brief overview of the consequences for violation of this policy.

The above information was adapted from the article, *"Crafting Effective Social Media Policies for Employees (with Template and Examples)"* from Indeed.com. Find the article HERE.

> *"Social media policies are becoming ubiquitous in employee handbooks because social media use is often integral to personal and professional life. Establishing a policy for the company is a great way to protect the company's interests while providing clear guidance and support for employee use."* – Indeed.com

Social Media Ethics for Advocates

Social media is everywhere! We use it to keep in touch with friends, family, colleagues and simply for entertainment. However, when used incorrectly it can blur the lines of professional boundaries for both the advocate and the victim/survivor. For example, blurred boundaries can happen when an advocate has a public social media presence where victim/survivors may see personal pictures and information about the advocate's family. By not making their page private, the advocate has unintentionally created boundary issues for the victim/survivor as they now have an inside view of their advocate that is more personal than professional.

It is natural for a victim/survivor to express fondness for their advocate and an interest in maintaining a relationship with anyone in the helping profession that provides much needed validation and support. Unintentionally, and sometimes intentionally, an unhealthy reliance between the advocate and the victim/survivor can develop if healthy boundaries are not maintained. Social media creates an added layer of ethical concerns as the advocate may not be aware of victims/survivors accessing their personal information.

In this section we will be discussing how advocates can continue to use social media while taking steps to maintain boundaries and professionalism. The following ethical guidelines can be summarized into three categories; Confidentiality, Dual Relationships, and Professionalism.

> The phrase, "the appearance of impropriety" is helpful for advocates and allied professionals to remember. Regardless of whether any activity is improper within the professional relationship, if it could give an outsider the appearance of something improper, the situation should be avoided.

CONFIDENTIALITY

The simplest solution to protecting confidentiality of victim/survivor information is to refrain from posting anything about their case on any social media page. This is true for accounts that are public and private.

> The theory of "Six Degrees of Separation" is very important when considering posting anything to your personal social media accounts. This theory is the idea that anyone can be connected to anyone else in just six steps.

You may not know all of the connections and friendships of your social media contacts. They may know people that are close to the victim/survivor and the information can be shared through connections not known to you.

Above all, victims/survivors have the right to privacy. Sharing personal information about the victim/survivor could place them in danger, hurt their case, and inhibit future advocate relationships. Another way to protect victim/survivor information is to turn off your location settings on social media platforms. For example, if an advocate is in court with a victim/survivor and the advocate posts to their social media with their location settings active, their location will appear alongside the post.

A quick way to avoid ethical dilemmas is to make your personal social media accounts private and inaccessible to the general public. Doing so allows you to determine who can view your page and ensures that you are not sharing information publicly that could cause harm to both you and the victim/survivor.

SEEKING INFORMATION ON SOCIAL MEDIA

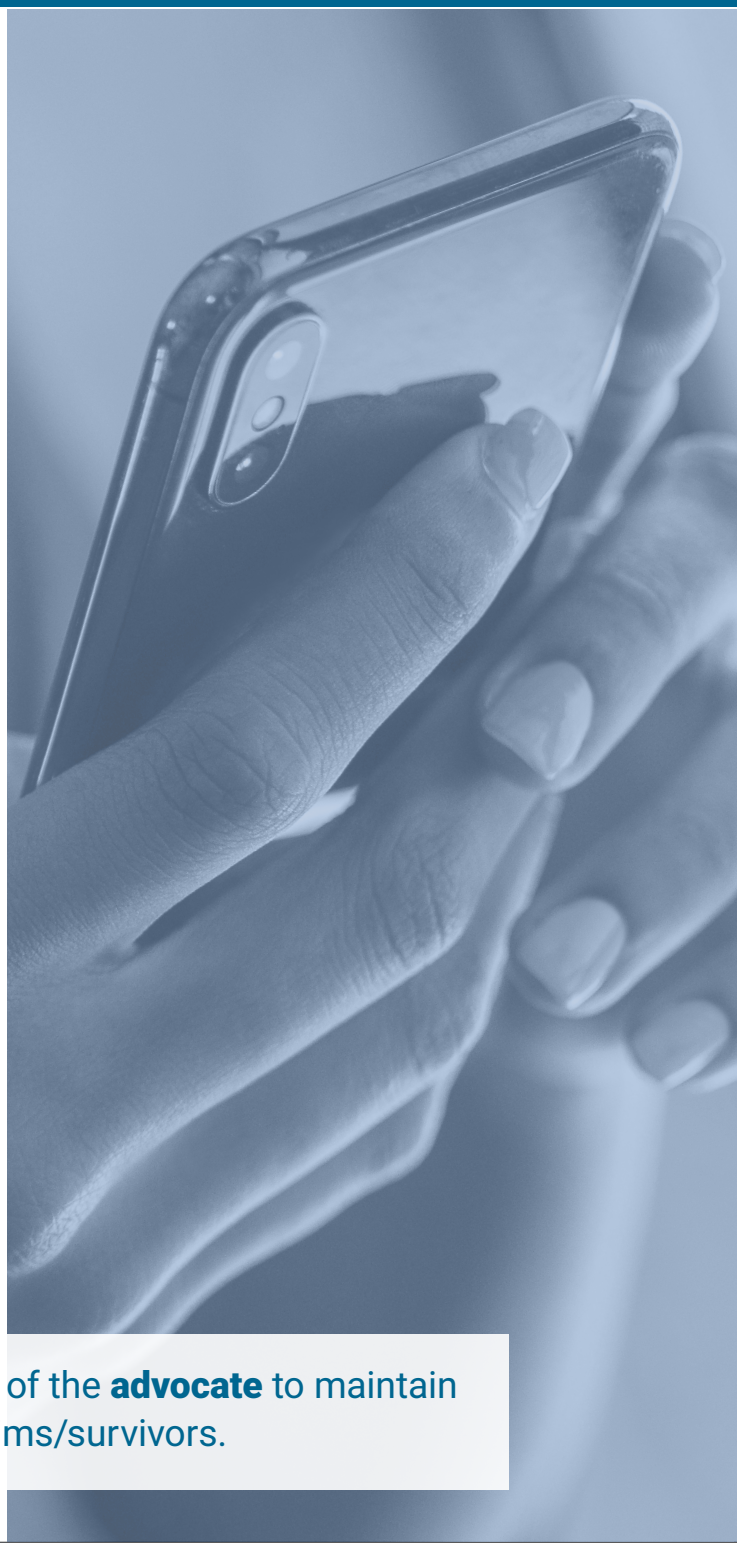
Advocates should obtain a victim's/survivor's consent before conducting an online search for information about the victim/survivor as a way to respect the individual's privacy. Unless there is a safety concern for the individual, seeking additional personal information about a victim/survivor outside of the professional relationship can blur boundaries and create unnecessary judgments on the activities and social lives of victims/survivors. If there is not a safety concern, any information obtained in this manner is a breach of trust between the advocate and the victim/survivor that can only serve to complicate the need for the professional's unbiased advocacy.

Dual Relationships

A dual relationship exists when a victim/survivor and an advocate communicate for the purposes of anything other than that within their professional relationship.

An easy way to avoid this unethical boundary crossing is to not accept friend or follow requests on social media from the victim/survivor. The advocate may believe they will maintain this boundary despite having social media interaction with a victim/survivor but this is not guaranteed. Texts and emails about non-work related matters is another way dual relationships can be formed or maintained therefore maintaining ethical boundaries in all aspects of communication with a victim/witness is essential.

What if a current "Friend" or "Follower" on social media becomes a client? This can and does occur and presents a difficult situation for any advocate. If this should happen, it is preferred to have another advocate handle their case or any case in which the advocate has an outside relationship with the client. Collaborative relationships with other advocacy organizations is really beneficial in these moments. In the event this is impossible, it is imperative that the advocate is clear with the victim/survivor that the advocate is not able to discuss the case on any personal social media accounts, personal email, or texting to personal cellphones. Professional emails, phone calls, and visits are easily traceable and documented while personal communications may not be. This is to ensure that boundaries are maintained and ethical lines are not crossed.



Ultimately, it is **always** the responsibility of the **advocate** to maintain and protect ethical boundaries with victims/survivors.

Professionalism and Social Media

RESPECT FOR OTHERS

What you put on social media is a permanent online record, even if you attempt to delete it later. Once it is online, it is searchable and could harm you professionally with clients, co-workers, current and even future employees. Discussions or references to any professional situation including other organizations, colleagues, co-workers, or clients on social media is an ethical violation. Some believe that discussion without specific names is acceptable but this is a good time to remember that the theory of "Six Degrees of Separation" is applicable.

Many stories are already known despite names not being mentioned. A friend of a friend can easily pass the information to persons that do understand the references. It is important to mention that regardless of any situation, it is likely you do not have all of the information and perspectives regarding that situation. Making assumptions and judgments in any manner can and will harm working relationships and promote toxic work environments.

The job of an advocate can be inherently traumatizing and requires taking individual responsibility to remain professional and supportive of one another. "Venting" on any form of social media about professional concerns is considered unethical and can have profound implications professionally.

CULTURAL EQUITY AND SENSITIVITY

Advocates are helpers to all. When advocates post racist and inequitable views on the internet, it destroys the very meaning and purpose of being an advocate. When we take the mantle of becoming an advocate, we take on the responsibility of uplifting all victims/survivors no matter their background or identity. Advocates should be careful to avoid sharing information on personal social media accounts that is not sensitive or equitable to gender, race, sexuality, culture and ethnicity, sexual orientation, ability, or otherwise insensitive to a particular population. If a victim/survivor sees these comments, posts, links, or articles on your personal social media accounts it can permanently damage the relationship with the victim/survivor and their relationship with your advocacy program.

Conduct a Social Media Audit

Now that you have covered the ethical guidelines for professional and personal social media pages of advocates, it's time to conduct a social media audit! This audit has been adapted from "The 15-Minute Social Media Audit Everyone Can Do" by Kevan Lee retrieved from https://buffer.com/library/social-media-audit.

LOCATE ALL YOUR SOCIAL MEDIA PROFILES

First things first, where are you online? This may seem like the easiest task in the history of social media tasks. Find where you are online? Piece of cake! I'd imagine you could list off your major social profiles with ease.

But what about the uncommon spots, those outside the Big Four of Facebook, Twitter, Instagram, and LinkedIn? Did you create a YouTube page a couple years back on a whim? What new social networks did you try out when they were brand new and have never viewed them again? Take note of them all.

You might want to check these other places:

- Pinterest
- YouTube
- Tumblr
- Quora

As you locate your profiles, **make note of the ones you find and keep track of the following elements:**

- The social media network
- The URL
- Your profile name and/or description
- The number of followers or fans
- The date of your last activity

Now that you have your list of locations, **it's time to prune**. Make sure that your presence at these places is purposeful. You can consider asking some of the following questions to determine the necessity of certain profiles.

- "Why am I using this social account?"
- "Am I using this account for private or professional connections?"
- "Could clients or potential employers find me on this platform?"

If you no longer have a good reason to use the account, don't hesitate to cut ties.

CHECK PROFILES AND SETTINGS

After you have found all your social profiles, the next step is to give them a thorough once-over. If you're using the site professionally, start by checking to see that the profiles have been completely filled out. Social networks offer a lot of customization these days, so it's easy to miss a spot.

To be certain you have everything covered, it might be helpful to **open the customize settings on each social network** and review one-by-one to make sure that all images, text, and options are being used and optimized.

You might find that it is best to have a different feel on different social networks—Twitter might lend itself more toward a laidback personality whereas LinkedIn might require a more professional presence. In this case, consistency doesn't carry quite the same importance as making sure that the tone of the profile is right for the network. Think environment first and consistency second.

If you're using the site personally, make sure the privacy settings are set appropriately. Either way, be careful to check your privacy settings regularly to be sure you know exactly what pieces of information you are sharing with the public. Settings often automatically change when sites are updated, so you'll want to double-check your controls during those times.

OVWA is a private, non-profit organization.
Tax-deductible contributions are appreciated.

Contact us or visit our website at www.ovwa.org
to learn more about our services.

90 Northwoods Blvd., B-6
Columbus, OH 43235

phone 614-787-9000
fax 614-396-8863
info@ovwa.org

www.ovwa.org

This guide was supported by grant number 2021-VOCA-134145796 awarded by the Office for Victims of Crime, Office of Justice Programs, U.S. Department of Justice through the Ohio Attorney General's Office. Victims of federal crimes will be served.