

thriv·ol·o·gy

Managing Your Personal Information Online

A Starter Guide for Sex Educators

A workbook with practical steps to take control of your personal information online—**no tech skills needed!**

Healthy Teen Network



Johns Hopkins
Center for Adolescent Health

**By Charlie Blue Brahm, JB Rodriguez-Anello, Mary Foyder,
Randa L. Dean, and Milagros Garrido**

About Thrivology

This workbook is one of many innovative resources developed through the Thrivology project. Thrivology is a U.S. Health and Human Services Office of Population Affairs-funded research-to-practice center. Thrivology creates evidence-backed resources that enable youth-supporting professionals to integrate best practices of trauma-informed, healing-centered, and inclusive practices in adolescent sexual and reproductive health programming and care.

Learn more at [thrivology.com](https://www.thrivology.com)

Suggested Citation

Brahm, C. B., Rodriguez-Anello, J. B., Foyder, M., Dean, R. L., & Garrido, M. (2025). *Managing your personal information online: A starter guide for sex educators*. [workbook]. Healthy Teen Network. <https://www.HealthyTeenNetwork.org/Thrivology/Resources/managing-personal-information-online>

License

© 2025 Healthy Teen Network.

[HealthyTeenNetwork.org](https://www.HealthyTeenNetwork.org)

This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/). Under this license, you are free to:

- Share — copy and redistribute the material in any medium or format.
- Adapt — remix, transform, and build upon the material.

Under the following terms:

- Attribution. You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
- NonCommercial. You may not use the material for commercial purposes.
- No additional restrictions. You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

Welcome

As a sex educator, you're doing essential work to make sure all young people have the knowledge and support they need to thrive. You deserve to feel safe in your work—not just physically and emotionally, but also digitally.

As conversations about sex ed become more visible,¹ so do the people leading them. That visibility can sometimes bring unwanted attention online. Taking steps to stay safe online can support your overall well-being.²

You don't need to be a tech expert to get started. Even small steps can make a big difference. And if you've already experienced online harassment, know this: You are not to blame, and you are not alone. It's up to all of us to advocate for better protections for educators' safety.

As we all work to improve organizational and systemic supports, sex educators deserve accessible, concrete tools to protect themselves now.

We recognize that as an educator who balances many competing priorities, setting up perfect online defenses is likely not an attainable or appropriate goal. Instead, this guide tries to provide you with an understanding of key online safety risks and concrete steps to take control of your personal information online.

Even if you only complete a portion of this guide, taking some steps can still help you guard your sensitive information and feel more secure.



Let's get started!

This guide includes key background information and three concrete steps to manage your digital footprint.

0

Gain Context and Set Intentions

PAGE 5

Learn relevant terms and how managing your information online can help prevent digital safety threats, then clarify your goals and create a plan for how you'll do the workbook.

ABOUT
10 – 20
minutes

1

Manage What You Share

PAGE 10

Reflect on how public you want your personal and professional accounts to be. Then choose your 1-3 most important accounts and update their privacy settings. Repeat as needed.

ABOUT
45 – 60
minutes

2

Manage What Others Share

PAGE 17

Pick your priorities for addressing information shared by your workplace and third parties about you, and then search yourself online. Take action to address anything concerning you find.

ABOUT
45+
minutes

3

Maintain Your Privacy Practices

PAGE 23

Create a plan to check in on your digital footprint regularly. Plus, check out tips for building privacy-supporting habits.

ABOUT
20
minutes

Short on time?

Start by making just one change. Focus on completing Step 1 for your most used social media account. If you have a relatively small digital presence, that might be enough for you to feel more in control of your personal information online! Otherwise, making updates to one account is a solid starting point; you can always come back to this workbook and complete the other steps when you have time.

STEP 0

Gain Context and Set Intentions

Set yourself up for success by reading useful background information and reflecting on why and how you'll go through this workbook.

SUB-STEPS:

Step 0.1 / **Understand key terms.**

Step 0.2 / **Learn about doxing.**

Step 0.3 / **Set intentions for using this workbook.**

STEP 0.1

Understand key terms.

What is a digital footprint?

Online, your personal information is represented in what's commonly called a "digital footprint." A digital footprint contains a unique trail of data about you and your online behavior.

Because privacy isn't the default on the internet, most people's digital footprint contains some amount of Personally Identifiable Information (PII).

What is Personally Identifiable Information (PII)?

PII is just what it sounds like: information that can be used to trace your individual identity, either on its own or in combination with other information that's linked to you.

PII includes...³

1. Basic demographics (e.g., birth date, marital status, race, and gender)
2. Personal preferences (e.g., online screen names and political affiliation)
3. Contact information (e.g., personal and work phone numbers)
4. Community interaction (e.g., social network profiles, law enforcement files, and face pictures)
5. Financial information (e.g., credit card number, credit score, and handwriting sample)
6. Secure identifiers (e.g., home address, biometric data, and government identification)

PII is often categorized as either sensitive or non-sensitive. But the reality is that everyone has different comfort levels with their information being shared publicly. If you belong to a community that experiences more online harassment and violence, it's understandable if you feel protective of your PII overall.



STEP 0.2

Learn about doxing.

Limiting how much sensitive PII is available about you online can help defend against this digital safety threat.

What is doxing?

Doxing (sometimes spelled “doxxing”) is short for “dropping documents.” It’s a type of online attack in which attackers publish their target’s PII online without consent and direct people to use that information to harm them.⁴

That harm can include harassment, intimidation, stalking, and identity theft.⁵ Another possible type of harm is “swatting,” in which attackers illegally report that the doxing target did a made-up crime in the hopes that armed officers will raid a target’s house unexpectedly.⁶

Doxing that targets a professional because of their work—including sexual and reproductive health education—is a type of workplace violence.⁷ Managers have a responsibility to take this threat seriously and work to protect their staff.

How big of a threat is doxing?

Overall, around 11 million Americans have been victims of doxing attacks. Many of these people were targeted because of their work, beliefs, or identity as a way to try and scare them into silence.⁸ People who have been targets of doxing report feeling a loss of control, fearing for their safety, and even withdrawing socially.^{9,10}

Educators are increasingly dealing with the problem of their personal information being shared online without their consent.¹¹ While there isn’t much research on sex educators’ experiences with doxing, they may be targeted specifically because they are visible figures at the center of heated public debates over sex education.

While these facts may feel concerning, keep in mind that only a small fraction of controversies that call out individual educators escalate into doxing.¹² Still, it’s worth taking steps to shape your digital footprint because doxing can cause a lot of harm, and feeling protected can help you resist the pressure to stay silent.

What if someone writes a negative article about me?

Getting called out online isn’t doxing unless it includes personally identifiable information, but it is highly upsetting!

Recently, critics have been more heavily scrutinizing individual educators’ social media and using it to target them.¹³ In rare cases, this negative visibility can escalate into doxing if it’s picked up by malicious sex ed opponents and accounts like Libs of TikTok.^{14,15}

In Step 2.1, you’ll think through whether you want to keep more of your work anonymous to limit the chance of being directly called out.

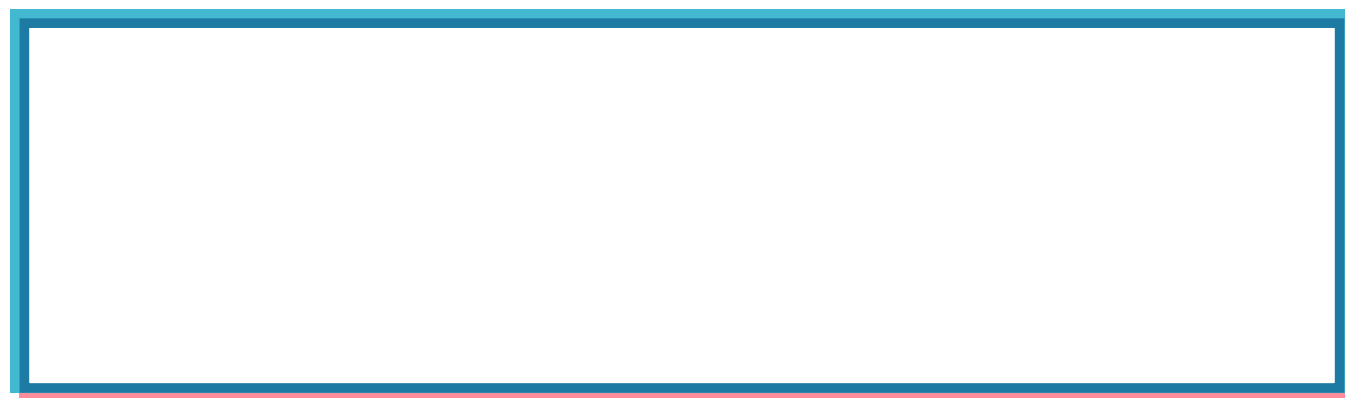
STEP 0.3

Set intentions for using this workbook.

If you're not yet sure of your goals and process, look through the rest of the workbook and then come back to these questions.

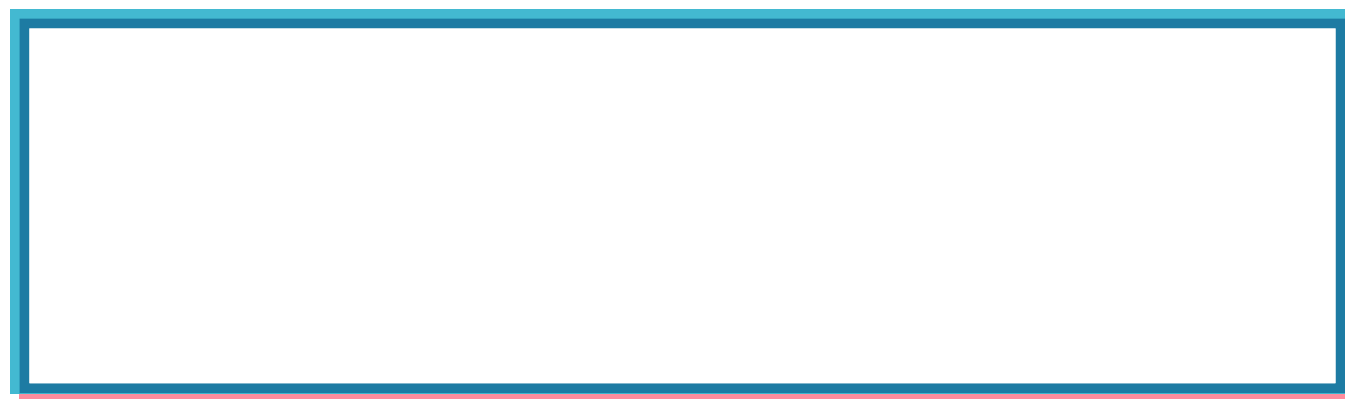
How do you feel about your digital footprint?

Do you have a pretty good sense of what information is out there about you, or are you unsure? How relaxed or concerned do you feel about your publicly available information?

**What are your main goals in taking steps to shape your digital footprint?**

Try listing your 1-3 top goals so that you can prioritize your effort. For example, you might prioritize understanding what information is already posted about you online, getting clear on privacy options for your accounts, or trying to anonymize controversial content you published through previous workplaces.

Remember, you can always change your goals as you go through the workbook.



STEP 0.3 (CONTINUED)

Set intentions for using this workbook.

What is your plan for completing this workbook?

Start by considering the size of your digital footprint and how thoroughly you want to audit what information is out there. Given that, what supports and structure would help you reach your goals? Trying to complete the workbook alone and all at once may not work for everyone—could you break the workbook up into manageable chunks and do them over time? It could also be helpful to find an accountability buddy and check in regularly to keep each other on track. Check out the example plans below for inspiration.

1. *I don't publish under my own name through my work, and I only use a couple of social media accounts. I've blocked off two hours to try and get through the whole workbook today.*
2. *I am fairly present online, professionally and personally. I will spend 30 minutes on workbook tasks every afternoon this week. Then I'll figure out a plan if I need to do anything more.*
3. *I am very online! Social media is a big part of my work, so this feels important but also overwhelming. I'm going to find an accountability buddy who can get on a biweekly call. We will work through it together until we've both made all the changes we need to feel safer.*



STEP 1

Manage Your Accounts

Your first line of defense in shaping your digital footprint is managing what you share publicly on your own accounts.

SUB-STEPS:

Step 1.1 / **Set privacy goals for your personal accounts.**

Step 1.2 / **Set privacy goals for your professional accounts.**

Step 1.3 / **Identify your top priority accounts.**

Step 1.4 / **Update your privacy settings.**

STEP 1.1

Set privacy goals for your personal accounts.

Written goals can help you make your account settings consistent.

Use these questions to set a baseline. When you're updating your settings later, you can decide that specific accounts need more or less restriction. Since personal accounts generally contain sensitive information, try to restrict them where possible. Note that "1st / 2nd degree connections" means your direct connections plus their connections.

Finding your accounts	Yes	No
Do you want your accounts to be visible to search engines like Google and DuckDuckGo?	<input type="checkbox"/>	<input type="checkbox"/>
Do you want people to be able to look up your accounts using your email address?	<input type="checkbox"/>	<input type="checkbox"/>
Do you want people to be able to look up your accounts using your phone number?	<input type="checkbox"/>	<input type="checkbox"/>

NOTES/QUESTIONS

Managing your data	Yes	No
Do you want to be able to review posts or photos you're tagged in before they appear publicly?	<input type="checkbox"/>	<input type="checkbox"/>
Do you want apps or third parties to have access to your data?	<input type="checkbox"/>	<input type="checkbox"/>
Do you want the apps you use to have access to your location?	<input type="checkbox"/>	<input type="checkbox"/>

NOTES/QUESTIONS

Connecting with you

	1 st /2 nd degree connections	Anyone
Who do you want to be able to send you friend requests?	<input type="checkbox"/>	<input type="checkbox"/>
Who do you want to be able to follow you?	<input type="checkbox"/>	<input type="checkbox"/>
Who do you want to be able to send you direct messages?	<input type="checkbox"/>	<input type="checkbox"/>

NOTES/QUESTIONS**Information visibility**

	Only direct connections	1 st /2 nd degree connections	Anyone
Who do you want to see your personal information?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Who do you want to see information and photos that you post or share? (Some sites allow you to set a default audience.)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Who do you want to see your other contacts or connections?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

NOTES/QUESTIONS

STEP 1.2

Set privacy goals for your professional accounts.

Professional information you share

	Yes	No
For websites like blogs or portfolios, do you want any of your work to be password protected or guarded in another way?	<input type="checkbox"/>	<input type="checkbox"/>
If you have a publicly visible CV or resume, do you want it to include where you've lived?	<input type="checkbox"/>	<input type="checkbox"/>
If you have a publicly visible CV or resume, do you want it to include an email address and phone number?	<input type="checkbox"/>	<input type="checkbox"/>

NOTES/QUESTIONS

Finding your accounts

	Yes	No
Do you want your accounts to be visible to search engines like Google and DuckDuckGo?	<input type="checkbox"/>	<input type="checkbox"/>
Do you want people to be able to look up your accounts using your email address?	<input type="checkbox"/>	<input type="checkbox"/>
Do you want people to be able to look up your accounts using your phone number?	<input type="checkbox"/>	<input type="checkbox"/>

NOTES/QUESTIONS

Managing your data

	Yes	No
Do you want to be able to review posts or photos you're tagged in before they appear publicly?	<input type="checkbox"/>	<input type="checkbox"/>
Do you want apps or third parties to have access to your data on this account?	<input type="checkbox"/>	<input type="checkbox"/>
Do you want the apps you use to have access to your location?	<input type="checkbox"/>	<input type="checkbox"/>

NOTES/QUESTIONS**Connecting with you**

	1 st /2 nd degree connections	Anyone
Who do you want to be able to send you friend requests?	<input type="checkbox"/>	<input type="checkbox"/>
Who do you want to be able to follow you?	<input type="checkbox"/>	<input type="checkbox"/>
Who do you want to be able to send you direct messages?	<input type="checkbox"/>	<input type="checkbox"/>

NOTES/QUESTIONS**Information visibility**

	Only direct connections	1 st /2 nd degree connections	Anyone
Who do you want to see your personal information?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Who do you want to see information and photos that you post or share? (Some sites allow you to set a default audience.)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Who do you want to see your other contacts or connections?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

NOTES/QUESTIONS

STEP 1.3

Pick your top priority accounts.

Choose 1-3 accounts to manage that you use the most often, share the most personal information on, or have the widest audience on. For each account, start by writing the website and username. Then, under "Current Usage," check the option that best describes the content you share, your audience, and your connections.

If you marked "Both," consider choosing a single usage going forward. Narrowing your audience lets you tailor privacy settings and content to protect your information. If you decide to make a change, check the matching box under "New Usage" and note if you want to create a new account for the other usage. You'll fill in "Action Status" later.

1	Account Information	APP/WEBSITE <input type="text"/>	USERNAME <input type="text"/>
	CURRENT USAGE <input type="checkbox"/> Personal <input type="checkbox"/> Professional <input type="checkbox"/> Both	NEW USAGE <input type="checkbox"/> Personal <input type="checkbox"/> Professional <input type="checkbox"/> No change	ACTION STATUS <input type="checkbox"/> Not started <input type="checkbox"/> In progress <input type="checkbox"/> Updated

2	Account Information	APP/WEBSITE <input type="text"/>	USERNAME <input type="text"/>
	CURRENT USAGE <input type="checkbox"/> Personal <input type="checkbox"/> Professional <input type="checkbox"/> Both	NEW USAGE <input type="checkbox"/> Personal <input type="checkbox"/> Professional <input type="checkbox"/> No change	ACTION STATUS <input type="checkbox"/> Not started <input type="checkbox"/> In progress <input type="checkbox"/> Updated

3	Account Information	APP/WEBSITE <input type="text"/>	USERNAME <input type="text"/>
	CURRENT USAGE Personal Professional Both	NEW USAGE <input type="checkbox"/> Personal <input type="checkbox"/> Professional <input type="checkbox"/> No change	ACTION STATUS <input type="checkbox"/> Not started <input type="checkbox"/> In progress <input type="checkbox"/> Updated

STEP 1.4

Update your privacy settings.

Take it one account at a time, and celebrate the progress you make along the way!

Start by finding the privacy centers or privacy settings pages for your top account. Make updates according to the privacy goals you set in Steps 1.1 and 1.2. Make sure to update the "Action Status" checkboxes for your top priority accounts (Step 1.3) as you go. You can use the "Notes" boxes to jot down any open questions, stopping points, or links to the webpage where you can update that site's privacy settings. Repeat this process for each account you listed in Step 1.3.

Plan to spend about 10 minutes per account, and remember you don't have to do it all at once. If you notice yourself getting overwhelmed or tired, that could be a good time to refer back to your plan for completing the workbook.

Want a space to keep track of all your accounts? Use our [Managing Your Personal Information Online spreadsheet template](#) to list everything, prioritize, and keep track as you update privacy settings over time.

STEP 2

Manage What Others Share

In this section, you'll identify priorities for managing your information in online spaces you don't directly control.

SUB-STEPS:

Step 2.1 / **Set privacy goals for your workplace.**

Step 2.2 / **Set privacy goals for other sites.**

Step 2.3 / **Search for your publicly available PII.**

Step 2.4 / **Ask your work to limit information about you.**

Step 2.5 / **Try to get concerning PII removed.**

STEP 2.1


Set privacy goals for your workplace.

How can you protect your personal information while still being recognized for your valuable work?

You may not have direct control of your current and former workplaces' websites, but you can ask them to make changes that protect your digital safety.

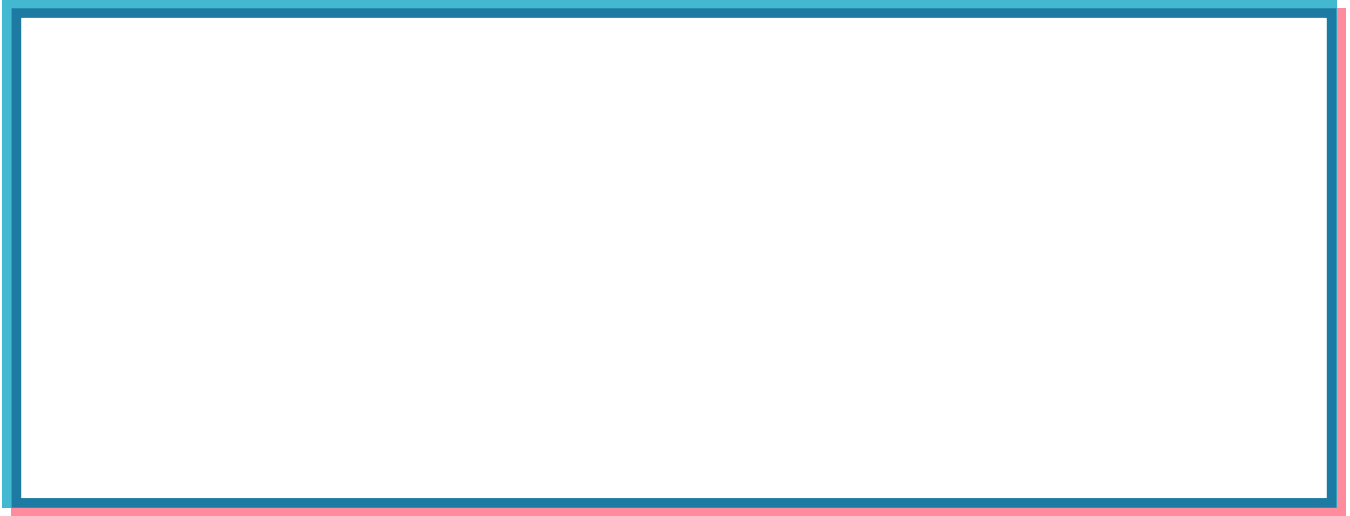
What information do you want on your organization's staff page?

Do you want your full name, just a first name, or a nickname? Do you want to use a headshot or a symbol or avatar instead? Do you want to be fully anonymous?



How do you want your name included in publications and resources?

Are there any controversial topics for which you would rather stay anonymous or use a different name?

**If a publication lists your full name, do you want to require an extra step to access it?**

This extra step might be entering a password or reaching out to your organization directly to see the full resource or authorship information.



STEP 2.2

Set privacy goals for other sites.

Your digital footprint isn't just made up of the things you share personally or through your work. Information about you can end up online without your input, like when third parties collect or share data about you.

Even if your PII is shared on a website you don't have direct control over, there may be a way to get it taken down. Prioritizing your concerns will help guide your actions.

Some of this PII might make you feel unsafe, especially if you have a high-visibility job, are a parent of young children, or belong to demographics that are more likely to experience online harassment.

What kinds of PII would make you feel unsafe to find about yourself online?

As a reminder, PII can include information such as basic demographics, personal preferences, contact information, community interaction, financial information, and secure identifiers. (See page 6 of this workbook.)

How much time and money would you spend to remove and monitor those kinds of PII?

There are a wide range of data monitoring and removal services that vary in cost from free to hundreds of dollars per year. There are also DIY guides to request your information be removed, but doing that across many apps and websites can be time consuming.

STEP 2.3

Search for your publicly available PII.

To get a sense of what information is out there, look up your name on popular search engines and people finder websites.*

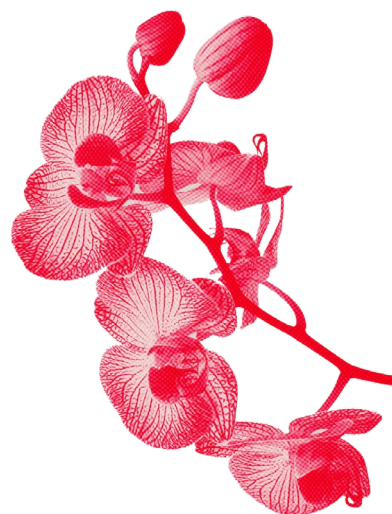
You can also try free or paid services that help you identify your digital footprint, but be sure to review their privacy practices before using them. If this step is feeling overwhelming, try for just 10-15 minutes to start.

If you want a way to structure and document your search process, consider using the [Managing Your Personal Information Online spreadsheet template](#). Filling in a spreadsheet may be especially helpful if you're doing a fairly comprehensive search or if you might take action to get information removed.

If you're using the spreadsheet, follow the steps below to record what you find in your search. You can leave "Course of Action" and "Progress Notes" blank until Step 2.4.

1. In the "My Accounts" sheet, add any accounts of yours that you uncover, which you haven't already listed.
2. In the "Workplace Info" sheet, list any sites you find where your current or past workplaces are sharing more information about you than you feel safe with.
3. In the "Red Flags" sheet, list any websites you find that share concerning PII. This could include people finder sites and data brokers (companies that collect and sell personal information about individuals).
4. In the "Webpages to Monitor" sheet, list any webpages that don't share threatening PII, but which name you or your work in a way that feels useful to track in case they escalate into a digital attack like doxing.

**Examples of people finder sites include Radaris, MyLife, and PeekYou. Digital footprint services like Experian's personal privacy scan and DeleteMe can also help. Since these services' privacy agreements may change over time, always do a careful review before providing personal information.*



STEP 2.4

Ask your job to limit information about you.

During your search, did you find any sites where a past or current workplace is sharing more information about you than you feel safe with?

If so, find out who you can contact to try getting this information removed or restricted. That might be a manager, colleague, or HR representative. If it is helpful, write that person's name and contact information in the "Course of Action" column on your spreadsheet.

Next, set aside time to reach out and request changes. If you're using the spreadsheet, you can track any updates in the "Progress Notes" column.

If you're able to get information removed, ask for help removing past versions of those pages from [the Internet Archive's Wayback Machine](#). This site allows people to see previous versions of the internet; this means that even if information has been removed from a webpage, it might still be visible there.

STEP 2.5

Try to get concerning PII removed.

Removing personal information from third-party websites can be hardest because you don't have direct control. Even so, there are likely still things you can do to get at least some of it removed!

If your PII was shared on data broker sites, you can either pay for a data removal service or submit a request yourself for them to remove it. There are also many personal data removal services available that range in cost and effectiveness.* Consider talking to your employer about covering the cost of these services as a way to support your team's digital safety.

If your info was posted on a specific website and it doesn't seem like it was shared with the goal of causing harm (for example, if a student posted something about you that you're uncomfortable with), try reaching out to the poster or website owner directly.

Even if you can't get site owners to take down the content, you can [ask Google to remove PII or doxing content from its search engine](#) or [try reporting a concern to Bing](#).

*At the time of publishing, popular options for data removal include more accessible services like EasyOptOuts as well as more thorough options like Optery, Incogni, and Privacy Bee. For a DIY route, [Yael Grauer's Data Broker Opt Out List](#) is a great resource.

STEP 3

Maintain Your Privacy Practices

Now that you've made some changes, it's time to think about how to shape your digital footprint going forward.

SUB-STEPS:

Step 3.1 / **Make a plan for monitoring.**

Step 3.2 / **Build privacy-supporting habits.**

STEP 3.1

Make a plan for monitoring.

If it's a priority for you to monitor certain webpages that talk about you, creating a plan can help you follow through on this intention.

How will you keep tabs on webpages where your name or work appears? (These are the websites you may have listed on the "webpages to monitor" column of the spreadsheet.)

How often do you want to check in on these pages? What kind of reminder would be useful?

You can keep tabs on new information that is shared about you online over time by setting up a system like Google Alerts. If you find new concerning pages, make a note or add them to the Managing Your Personal Information Online spreadsheet.

Is there anyone who can support you in keeping an eye on these websites?

Leaning on colleagues or friends to help monitor concerning pages can be helpful, since reading negative content about yourself can take an emotional toll. They can also keep a log of any harassment incidents, which could be useful if you need to take further action later.

STEP 3.2

Build privacy-supporting habits.

Below, check out a few tips to help you build practices that keep your personal information safe online.

- **Revisit the privacy goals you set in Steps 1.1 and 1.2 whenever you create a new account, since your priorities can change over time.** Use these goals to guide privacy settings in your new account. Make sure to update your other accounts as well if your privacy goals have changed.
- **Watch out for unintentionally sharing personal information in photos on publicly visible accounts.** When you are going to post a photo, take a moment to review what's in the background. Is there anything sensitive you don't want people to see online? Additionally, it's useful to think about what might be revealed through EXIF metadata, which contains information about an image like when and where it was taken. Many popular social media platforms remove this metadata when you upload a photo, but you can also look online for guides on how to remove it yourself before posting.
- **Avoid real-time posting.** This practice can help to prevent others from tracking your location or movements.
- **Switch to a privacy-focused browser and search engine.** There are quite a few options, many of which are free to use and very quick to install and set up! Take it a step further by installing a browser extension like Privacy Badger, created by the Electronic Frontier Foundation to limit online tracking by third parties.
- **Consider getting a PO Box for work-related mail.** If it's accessible for you, this can be a great way to keep your home address private and separate from your professional life.



Congrats, you did it!

By taking steps to shape your digital footprint and protect yourself online, you are also safeguarding your ability to continue the important work of showing up for young people.

More Resources

- Student Privacy Compass | [Let Teachers Be: Concerns About the Online Harassment of Teachers and Practical Tips For Self-Protection](#)
- Teach.com | [50 Resources to Support the Mental Health of Teachers and School Staff](#)
- NEA | [Responding to Harassment and Doxxing of Educators](#)
- PEN America | [Managing Your Online Footprint and Protecting from Doxing](#)
- Equality Labs | [Anti-Doxxing Guide for Activists](#)

References

1. Bauer, S. (2021, September 8). *Analysis-Sex education becomes battlefield in U.S. culture war over LGBT+ rights*. Reuters. <https://www.reuters.com/article/world/analysis-sex-education-becomes-battlefield-in-us-culture-war-over-lgbt-rights-idUSKBN2G4ORI/>
2. SchoolSafety.gov. (2023). *Online safety resources for the K-12 community*. https://www.schoolsafety.gov/sites/default/files/2023-06/SchoolSafety.gov%20Online%20Safety%20Resource%20Infographic_June%202023.pdf
3. Milne, G. R., Pettinico, G., Hajjat, F. M., & Markos, E. (2016). Information sensitivity typology: Mapping the degree and type of risk consumers perceive in personal data sharing. *Journal of Consumer Affairs*, 51(1), 133–161. <https://doi.org/10.1111/joca.12111>
4. New York University Tandon School of Engineering. (2017, November 7). *Why they dox: First large-scale study reveals top motivations and targets for this form of cyber bullying*. <https://engineering.nyu.edu/news/why-they-dox-first-large-scale-study-reveals-top-motivations-and-targets-form-cyber-bullying>
5. PEN America. (2025). *Defining “online abuse”: A glossary of terms*. <https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/#doxing>
6. Equality Labs. (2024, December 3). *Anti-doxing guide for activists*. <https://www.equalitylabs.org/wp-content/uploads/2024/12/EQUALITY-LABS-ANTI-DOXING-GUIDE-FOR-ACTIVISTS-3.0.pdf#h.t5mjznsGOnyr>
7. Wilson, R. C., & Zwang, K. (2024). Call to action: Supporting teams when cyberbullying and doxing occurs a new form of workplace violence. *Nurse Leader*, 22(5), 520–525. <https://doi.org/10.1016/j.mnl.2024.06.006>
8. Sheridan, M. (2024, August 8). *Doxing statistics in 2024: 11 million Americans have been victimized*. SafeHome.org. <https://www.safehome.org/family-safety/doxing-online-harassment-research/>
9. Eckert, S., & Metzger-Riftkin, J. (2020). Doxing, privacy and gendered harassment. The shock and normalization of veillance cultures. *Medien & Kommunikationswissenschaft*, 68(3), 273–287. <https://doi.org/10.5771/1615-634x-2020-3-273>
10. Muthusamy, A., Kumar, T., & Minakshi. (2025). Cybersecurity for preserving mental wellness and preventing abuse. In Minakshi, A. Bijalwan, & T. Kumar (Eds.), *Exploiting Machine Learning for Robust Security* (pp. 211–232). IGI Global Scientific Publishing. <https://doi.org/10.4018/979-8-3693-7758-1.ch010>
11. Sparks, S. D. (2024, May 9). *What is doxxing, and how can educators protect their privacy online?* Education Week. <https://www.edweek.org/teaching-learning/what-is-doxing-and-how-can-educators-protect-their-privacy-online/2024/05>
12. Healthy Teen Network. (2025). *Insights from key informant and Thrivology Youth Leader interviews: A human-centered design approach to research-to-practice translation*. [Unpublished raw data].
13. Gilbert, D. (2022, April 13). *“She needs to be executed”: The far-right is doxxing school officials they think are “groomers.”* VICE. <https://www.vice.com/en/article/far-right-groomers-doxing-school-officials/>
14. Tirrell, A., & Gogarty, K. (2023, November 2). *TIMELINE: The impact of Libs of TikTok told through the educators, health care providers, librarians, LGBTQ people, and institutions that have been harassed and violently threatened*. Media Matters for America. <https://www.mediamatters.org/lib-tiktok/timeline-impact-lib-tiktok-told-through-educators-health-care-providers-librarians>

Managing Your Personal Information Online: A Starter Guide for Sex Educators

A workbook developed through the Thrivology project by Charlie Blue Brahm, JB Rodriguez-Anello, Mary Foyder, Randa L. Dean, and Milagros Garrido

Acknowledgments

We are grateful for all the support we received in creating this workbook. Our gratitude goes out to our Research Alliance members Lauren Lapointe, Jaclyn Friedman, and Amber Barcel for sharing insights during interviews and multiple draft reviews that helped make this workbook relevant and usable. Thanks to Arianna de la Mancha for testing an early version of the workbook and pointing out sections that felt confusing.

Thank you to Nicholas Sufrinko and Megan Thomas for your brand and visual design support. Last but certainly not least, we greatly appreciate Mackenzie Piper for being a steady, encouraging presence in managing the resource creation process and helping this workbook come to fruition.

This project is supported by the Office of Population Affairs (OPA) of the U.S. Department of Health and Human Services (HHS) as part of a financial assistance award (1 PHEPA000006-01) totaling \$1,168,985 with 100 percent funded by OPA/OASH/HHS. The contents are those of the author(s) and do not necessarily represent the official views of, nor an endorsement, by OPA/OASH/HHS, or the U.S. Government. For more information, please visit opa.hhs.gov.

thriv·ol·o·gy