Anti-Cyberviolence Policy

Steps to Developing Policy and Best Practices to Prevent Cyberviolence

Bibliothèque et centre d'informatique Atwater
Library and Computer Centre

Status of Women Canada
Condition féminine Canada

Table of Contents

Draft Anti-Cyberviolence Policy

This document was designed as a draft policy that can be modified and used within any organization. The term 'Organization' referred to within this document could be replaced with the name of your organization. This document was designed to be used with the accompanying *How to Develop Policy and Best Practices to Prevent Cyberviolence*. Another useful resource is the *Cyberviolence Prevention Policy and Practices: Cost-Benefit Analysis,* which you can find at (website link).

Organization Value Statement:

Respect and inclusivity are core values of our Organization, and therefore, Cyberviolence will not be tolerated. If you are a target of cyberviolence while working or participating in Organization initiatives, it is essential that you bring this to the attention of your supervisor or other trusted staff member, so that the Organization can assist and support you to the best of our ability.

We acknowledge that online spaces are inextricably interwoven into our offline lives, and what happens online can have profound impacts to our offline realities. Therefore, the Organization does not tolerate harassment in any of our learning or work environments, whether online or offline, and whether it originates at work or at home, and includes cyberviolence resulting from relationships that are established through our initiatives (e.g. collaborations with staff members of another organization).

The Atwater Library and Computer Centre's Preventing Cyberviolence Project's Definition of Cyberviolence:

Cyberviolence refers to online or technology facilitated behavior that constitutes or leads to harm against the psychological and/or emotional, financial, and physical state of an individual or group. Although cyberviolence occurs online, it can begin offline and/or have serious offline consequences. Gender-based cyberviolence, specifically, refers to the cultural and social norms, behaviors, and standards that allow women, girls, LGBTQQI2S,[1] and gender non-conforming people to be targets of violence, inequality, and misogyny, in both online and offline worlds.

Reach of this policy:

The Organization is concerned with all acts of cyberviolence that threaten its members' wellbeing, the safety of its environment, and its general functioning regardless of whether the electronic device used to enact the violence is owned by the organization or is located off its premises. Therefore, the Organization will intervene and provide support whenever appropriate.

*The Organization is committed to act in your best interest, prioritizing your safety, and acting on your behalf only with your explicit informed consent, unless there exists a risk to the safety or wellbeing of other members of the Organization. In such cases, we will keep

[1] Lesbian, Gay, Bisexual, Trans, Queer, Questioning, Intersex, and Two-Spirit

individuals who are targets of cyberviolence involved in on-going conversations regarding the best responses and approaches to take to address the issue.

Prohibitions:

The Organization will not tolerate any electronic communication deemed violent or criminal in nature. This includes, but is not limited to, prejudicial and damaging communication that targets a person's actual or perceived race, colour, religion, national origin, ancestry or ethnicity, culture, sexual orientation, gender, gender identity and expression, and ability, or other distinguishing personal characteristics. Prejudicial and damaging communication that targets a person's perceived association with any of the identities and groups mentioned above is also strictly prohibited. Violent, prejudicial and damaging electronic communication comprises of any electronic communication that intends to:

1. Physically, emotionally, and/or mentally harm an individual or damage the individual's property.

2. Substantially interfere with a student's educational opportunities; or a person's employment opportunities.

3. Create an intimidating or threatening Organizational environment.

4. Substantially disrupt the orderly operation of the Organization.

In this Section, "electronic communication" means any communication through an electronic device, including but not limited to, a mobile phone, tablet, pager or computer, with communication transferred in the form of an email, instant message, text message, blog, phone call, page, online game, web site among many other forms of electronic communication.

The Organization will not tolerate any acts of cyberviolence that are committed on their property, including the Organization's email and social media accounts, through the use of the Organization's equipment (i.e. computers or company provided mobile phones), at Organization-related activities, or in any other circumstance that has the potential to negatively affect the Organization and those who work within it.

For examples, see the Anti-Defamation League's *Cyber Safety Action Guide* https://www.adl.org/cyber-safety-action-guide

Communicating our Cyberviolence Policy

Cyberviolence prevention will be promoted by all members of our Organization and communities.

The Organization's definition of cyberviolence, as well as their policies, and procedures on cyberviolence prevention and intervention, including responses and support resources, will be communicated to all people, organizations and communities who are connected to the Organization in some capacity. All definitions policies and procedures related to cyberviolence will be communicated=through the Organization's website, support materials, human relations and employment contracts, anti-harassment and discrimination policies, electronic communication policies, client and/or employee handbooks, conduct codes, and on bulletin boards and wall postings at computer labs and classrooms.

*We strongly recommend that Organizations develop a one page summary of their anti-cyberviolence policy and post it in a widely accessible designated area such as a staff common area, the back of a bathroom door or any other area that is frequented by the Organization's members. We are available to help with this step and will provide plastic holders to conveniently post your short summary policy. A template to support you in developing this summary is provided in Appendix D.

If you are experiencing cyberviolence, here are the steps we encourage you to follow:

1. If you feel you are in immediate danger, please call 911*.

2. If you encounter cyberviolence, whether working with the Organization on their property, participating in any of the Organizations activities or projects, and in any of their spaces, online and offline, please inform your director, supervisor, trusted coworker or other suitable person or department (e.g. human resources) immediately. From here, the Organization will support you with whatever processes and procedures are deemed necessary to address your situation (e.g. reporting process with the police). The Organization will consider notifying law enforcement. This will depend on the unique circumstances of your case, and will be done *only with your explicit consent* or in consultation with you.

3. If possible, keep a record of all communications between you and the person who has been targeting you with cyberviolence (e.g. messages, pictures, etc.).

4. Either with someone from the Organization or with someone you trust, consider exploring resources outside of the legal system that can support you in negotiating your situation in ways that feel meaningful, relevant, and safer for you.

Organizational Responses to Cyberviolence

If a case of cyberviolence is brought to the Organization's attention, some of the ways in which we will potentially respond to cyberviolence, as determined by our mission, policies, and procedures, in consideration of federal and provincial legislation, and based upon the unique circumstances of the specific incident, include:

1. Contacting law enforcement.

2. Revoking the accused person's membership in the organization (e.g. expulsion or termination of employment).

3. Immediate removal of the person accused from the premises.

4. Banning the person accused from participating in future activities with the Organization.

5. Temporary suspension of the person accused from the Organization until further notice.

6. Initiating a mediation or reconciliation process to resolve the incident. This response **will only be considered if the survivor explicitly consents** to such a process AND if the Organization believes that the process will not bring more harm to the survivor.

Tips on Making Meaningful and Effective Responses

1. It is imperative to believe the person reporting an experience of cyberviolence, and to not act in ways that will expose the person to additional harm and trauma. This involves:

   Understanding that it is crucial to not act in any way that has the potential to create additional barriers to the survivor[2] accessing support, beyond the trauma they are already experiencing. Disclosing an experience of cyberviolence, and any violence for that matter, is complex, extremely difficult, and puts the survivor in an especially vulnerable position. It is vital to ensure the person and space that the survivor is seeking to access support through are as safe, welcoming, understanding and validating as possible.

   Refraining from questioning and scrutinizing the survivor, their experience and feelings. For instance, do not ask dismissive and invalidating questions such as: "Are you sure this happened?", "Are you sure you did not just misunderstand what happened?", "Are you sure? Terry seems to be such a nice person. I do not think they are capable of doing what you are saying they did to you."

2. Engaging in rigorous forms of self-reflection with the aim of enhancing your empathy towards, and understanding of, the survivor, their experience, and the challenges that come with reporting an incident of cyberviolence. It is fundamental to develop a strong sense of sensitivity to the survivor's vulnerability if you are to support the survivor in ways that are validating, relevant, and meaningful. Ask yourself: "How would I feel in this situation?", "How would my partner, my child, or another loved one feel in this situation?", "What would I want and need the most if I were reporting a traumatic experience?", "What qualities would I want in the person who I am disclosing to?"

3. In a similar vein, it is equally important to reflect on how the survivor may experience cyberviolence in complex ways given their unique identities and realities. Significantly, people who experience the intersection of multiple marginal identities may contend with additional barriers to reporting their experience and in accessing support. For instance, a transwoman of colour may encounter more challenges accessing support because transphobic and racist attitudes, whether they be overt or covert. For this reason, it is important for the Organization and its members to critically reflect on and consider how identities and experiences along the lines of culture, religion, race, citizenship status, gender identity and expression, ability, sexual orientation, and age, among many other identities and experiences, interact in ways that complicate the experience of cyberviolence and the reporting process for

[2]Terms used to describe the person who has experienced cyberviolence are highly debated. Ultimately, it should be up to the person to define themselves and use terms that they feel most comfortable with (e.g. survivor, victim, target, person experiencing violence, etc.). For the purposes of this document, we are using the term "survivor".

many different people. Neglecting to engage in such reflective processes may lead to actions that expose the survivor to more harm, trauma, and violence.

4. Not engaging in victim blaming and to ensure that others in the organization are held accountable if they victim blame the survivor. Never ask the person reporting an experience of cyberviolence questions such as: “What did you do for this to have happened to you?”, “What do you expect? Did you not choose to go on that site?”, etc.

5. Acknowledge that online information, communication, interactions, and relationships are REAL**,** and their impacts can be even more profound than offline interactions: it can be much more difficult to get away from online violence given that we are always connected, in some capacity, to our online realities through our phones, tablets, pagers, and computers.

6. Ensure that all parties involved receive appropriate support and guidance.

7. Ensure that any actions taken upholds the rights of all parties involved, including the survivor and person(s) accused. This includes:

    Ensuring that the reporting, legal, and any other processes are transparent to all parties involved.

    Informing all parties of their rights and responsibilities in relation to all processes.

    Providing regular updates on the case and the progression of all relevant processes to all parties.

    Explaining all decisions made and/or outcomes arrived at throughout all processes.

Steps to Developing Policy and Best Practices to Prevent Cyberviolence

(Please do not share without permission – this is a document in progress – direct feedback and suggestions to shanlydixon@atwaterlibrary.ca).

This document is designed to assist your organization in developing a working policy that both prevents and responds to incidences of cyberviolence in your workshop. To better understand the benefits of creating a policy and the potential costs of not doing so, please refer to the Atwater Library and Computer Centre's Preventing Cyberviolence Project's - *Cyberviolence Prevention Policy and Best Practices; Cost benefit Analysis* which can be found at *http://cyberviolence.atwaterlibrary.ca/wp-content/uploads/2017/03/Cyberviolence-Prevention-Policy-and-Best-Practices-Cost-Benefit-Analysis-.pdf*.

It has been our experience that stakeholders are often reluctant to develop and adopt policy, because they are concerned that it may limit their discretion and flexibility in how they respond to individual cases of cyberviolence in their organization. We acknowledge that our stakeholder's communities and needs are diverse, and therefore policy and responses may need to be broad to the forefront to allow for flexibility in drafting policies that ensure safe spaces in your Organization, depending upon the context of the cyberviolence in question that your employees may experience. Therefore, using this guide to develop policy will provide an opportunity for your Organization to both de-normalize cyberviolence within your organization, and send a clear message that acts of cyberviolence will not be tolerated. Additionally, using this guide will help you to envision how cyberviolence might be manifested within your organization, and help you think through possible organizational responses that you may take, so that you aren't blind-sided when faced with such incidents.

Policy is flexible and should be regularly reviewed and adapted according to changing needs, evolving technology, and varied circumstances of your Organization. Getting started on developing policy is crucial, but it doesn't have to be perfect. Perfection is the enemy of very, very good. Therefore, below, we have outlined a series of steps, with examples of possible wording, that your Organization can follow in developing your own individualized Cyberviolence Prevention Policy, and we encourage and support you in refining and continuously developing your policy over time through the following steps:

Step 1: Develop a definition of cyberviolence

Example, The Atwater Library and Computer Centre's Preventing Cyberviolence Projects Definition of Cyberviolence:

Cyberviolence refers to online or technology facilitated behavior that constitutes or leads to harm against the psychological and/or emotional, financial, physical state of an individual or group. Although cyberviolence occurs online, it can begin offline and/or have serious offline consequences. Gender-based cyberviolence, specifically, refers to the cultural and social norms, behaviors and standards that allow women, girls, LGBTQQI2S[3] and gender non-conforming people to be targets of violence, inequality

[3] Lesbian, Gay, Bisexual, Trans, Queer, Questioning, Intersex, and Two-Spirit

and misogyny in both online and offline worlds.

Step 2: Create a statement that prohibits cyberviolence within your Organization

Example: Respect and inclusivity are core values of our Organization, and therefore Cyberviolence will not be tolerated.

If you are a target of cyberviolence while working or participating in Organization initiatives, it is essential that you bring this to the attention of the project coordinator, so that the Organization can assist and support you to the best of our ability.

Step 3: Establish the boundaries and spaces where your definition will apply

Example: We acknowledge that online is inextricably interwoven into our offline lives, and consequences of what happens online can have profound impacts offline. Therefore, the Organization does not tolerate harassment in any of our learning or work environments, whether they occur or affect your on- or offline space; this includes cyberviolence resulting from relationships that are established through our initiatives.

Even if the electronic device used to engage in the cyberviolence is located off premises or is not owned by the Organization, but nevertheless disrupts the Organization's environment, functioning, or wellbeing of participants or members of the Organization, acts of cyberviolence will be considered a concern of the Organization. Therefore, the Organization will attempt to provide support, responses, and/or interventions, when appropriate.

Step 4: Clearly articulate in which circumstances the organization will intervene

Will the organization intervene only with informed consent on the part of the person experiencing the cyberviolence or are there situations in which the organization would be obligated to intervene without the consent or participation of the target?

Example:

*The Organization is committed to act in your best interests, prioritizing your safety and acting on your behalf with your informed consent, *unless* there exists a risk to the safety or wellbeing of other members of the Organization. We will keep individuals who are targets of cyberviolence involved in conversations regarding best responses as we address the issue.

Step 5: Clearly articulate which types of cyberviolence behavior are prohibited

Example: The Organization will not tolerate any harmful electronic communication that is shown to be motivated by an individual's actual or perceived race, color, religion, national origin, ancestry or ethnicity, sexual orientation, physical, mental, emotional, or learning disability, gender, gender identity and expression, or other distinguishing personal characteristic, or based on association with any person identified above, when the electronic communication is intended to:

(i) Physically harm an individual or damage the individual's property.

(ii) Substantially interfere with a student's educational opportunities, or a person's employment opportunities.

(iii) Create an intimidating or threatening Organizational environment.

(iv) Substantially disrupt the orderly operation of the Organization.

The Organization will not tolerate any acts of cyberviolence committed on their property (including email and social media accounts related to the Organization), using the Organization's equipment (i.e. computers, company-provided mobile phones), at Organization-related activities, or in any other circumstances where engaging in cyberviolence will have a negative impact on the Organizational environment.

As used in this Section, "electronic communication" means any communication through an electronic device, including, but is not limited to, a mobile phone, pager or computer, where communication includes, but is not limited to, e-mail, instant messaging, text messages, blogs, mobile phones, pagers, online games, and web sites.

Step 6: Clearly articulate how you will communicate your policy, procedures, responses, and support responses

Example: Cyberviolence prevention will be promoted by all members of our Organization and communities.

The Organization's definition of cyberviolence, their policies and procedures on cyberviolence prevention and intervention, responses and support resources, will be communicated to the Organization's participants, employees, facilitators, clients, collaborators, and broader community. These will spaces include communication through the website, support materials, human relations and employment contracts, anti-harassment and discrimination policies, electronic communication policies, client and/or employee handbooks, conduct codes, and on bulletin boards and wall posts in computer labs and classrooms.

Step 7: Explain what the Organization's community should do if they are experiencing cyberviolence

Example: If you are experiencing cyberviolence, here are steps we encourage you to follow:

1. If you feel you are in immediate danger, please call 911.

2. If you encounter cyberviolence, either working within the Organization on their property, or participating in any of the Organizations projects or activities in any of their spaces, immediately inform your on-site facilitator. Your facilitator will notify the appropriate coordinator and the information technology technician.

3. The Organization will consider notifying law enforcement, depending upon the circumstances and only with your consent.

4. To explore other potential strategies and responses, we also suggest that, either with someone from the Organization or with someone you trust, you take advantage of the following additional resources: (http://www.crashoverridenetwork.com/resources.html and http://www.crashoverridenetwork.com/coach.html).

Step 8: Create a list of potential responses to incidences of cyberviolence

A good way to do this is to think of all the potential ways in which cyberviolence might be experienced by individuals or groups working within your organization. You can consult the list of manifestations in the appendix of the *Cyberviolence Prevention Policy and Best Practices;* and, *Cost benefit Analysis*, which can be found at:

http://cyberviolence.atwaterlibrary.ca/wp-content/uploads/2017/03/Cyberviolence-Prevention-Policy-and-Best-Practices-Cost-Benefit-Analysis-.pdf

Now is an especially important time to be mindful of the gender-based and racialized component of the way cyberviolence happens. To ensure your workspace is inclusive for people of all genders, sexual orientations, and so forth, you could consult members of your organizational community to learn the many ways in which others view cyberviolence and how acts of cyberviolence can be manifested within your Organization. Once you have listed all possible scenarios, you can think through best responses to each of them.

Here are some of the ways we will potentially respond to cyberviolence, as determined by our standing anti-harassment committee, and in consideration with federal and provincial legislation, based upon the specific incidents involved:

1. Contact law enforcement.

2. Revoke perpetrator's membership in the organization (expulsion or employment termination).

3. Remove perpetrators from premises.

4. Ban participants from future activities.

Additional steps your organization can take to help prevent and eliminate cyberviolence

Provide organization's community with education and training about ethical digital citizenship and how to address incidents of cyberviolence* For information about training please contact Eric.

For more information regarding how to create your own policy, for advanced policy guidelines, and for the references used to construct these guidelines, please visit the accompanying appendices below.

Appendix A: Basic Checklist for Creating Your Own Policy

- ❒ Do you have a clear definition and prohibition of cyberviolence?
- ❒ Does your definition promote gender-inclusive language?
- ❒ Does your policy promote safer spaces for women and girls, LGBTQQI2S, and gender non-conforming people, boys, men, and the community at large?
- ❒ If yes, were policies and practices developed through an inclusive and participatory process, with relevant input provided by community members and stakeholders?
- ❒ Does the policy address cyberviolence regarding on-campus/off-campus interactions between students or colleagues and/or the at-work/after-work interactions between colleagues?
- ❒ Does your policy include information on your organization's approach, complaint procedures, and methods for conducting investigations?
- ❒ Does your policy take into consideration comprehensive and effective responses that considers everyone involved? For example, does it provide specific support for the individual or group who has been targeted; intervention for the individual who engaged in the act of committing cyberviolence; and strategies for responding to the larger community of bystanders?
- ❒ Have you developed a clearly articulated list of consequences and appropriate remedial actions that affects a person who commits an act of cyberviolence?
- ❒ Have you developed clearly articulated consequences and appropriate remedial actions for an individual found to have falsely accused another individual of cyberviolence?
- ❒ Are your policies, practices, and protection mechanisms written from a human rights and survivor centered perspective? Are these designed to minimize fear of reprisals through, for example, anonymous reporting?

Appendix B: Advanced Policy Checklist

- ❒ Does your policy explain and articulate the varying national and provincial laws?
- ❒ Have you developed a strategy for providing counseling or referral to appropriate services, including guidance, academic intervention, and protection to individuals implicated, both targets and perpetrators, and appropriate bystanders affected by harassment, intimidation, bullying, or cyberbullying, as necessary?
- ❒ Does your policy share a list of potential manifestations of cyberviolence, for instance, examples of cyberviolence specific to your organization or community?
- ❒ Are complaints taken seriously and acted upon promptly? Is there a comprehensive intervention strategy that addresses incidents of cyberviolence in a timely and appropriate manner? If not, what are the barriers and how could they be changed?
- ❒ Does the policy clearly define the role and responsibilities of the investigator? Is the investigator independent, neutral, objective, and knowledgeable of the law, policies, and practices? Do possibilities of conflict of interest or abuse of power exist?[i]
- ❒ Who are the findings of the investigation reported to, and do they have sufficient authority to enforce actions?
- ❒ Are there assurances that findings will be presented in a timely and fair manner?[ii]
- ❒ Are there guidelines for the reporting process? Do they specify that the report must summarize allegations, steps taken during the investigation, evidence gathered?[iii]
- ❒ Do the parties in the investigation have the right to representation from such persons as a union steward, student union, ombudsperson, or legal counsel?
- ❒ Is confidentiality protected throughout the entire process? What mechanisms are present to ensure that information is only shared on a need-to-know basis, and only with interested parties?
- ❒ Do you have a protocol developed outlining how you will provide support and resources to the victims of cyberviolence after investigations have concluded?
- ❒ Do you have information and resources available for victims of cyberviolence?
- ❒ Does your policy provide guidelines, funding, and measurable results/outputs for improving on future prevention activities?
- ❒ Does your policy effectively refer to and make connections with existing policies in place, such as an anti-harassment policy, safer spaces policy, or codes of conduct?

- ❒ Does your policy provide guidelines on how to include anti-cyberviolence messaging in promotion material? (E.g. handbooks, websites, support materials for counselling and development or human resource departments, bulletin boards, posters, etc.)
- ❒ Does your policy assign responsibility to a human resource contact person for the monitoring and evaluation of the effective implementation of the policy? Are adequate resources available to this person?

Appendix C: Resources That Yay be Helpful to your Organization

Crash Override Network – Crisis helpline, advocacy group, and resource center for people experiencing online abuse:
http://www.crashoverridenetwork.com/resources.html and
http://www.crashoverridenetwork.com/coach.html
YWCA's Project Shift - Creating a Safer Digital World for Young Women:
Website: http://ywcacanada.ca/en/pages/cyber/about
Needs Assessment: http://ywcacanada.ca/data/documents/00000460.pdf

Head & Hands – Non-profit organization servicing youth aged 12 to 25 years in Montreal
Website: http://headandhands.ca/
Legal Services: http://headandhands.ca/programs-services/legal-services/

Media Smarts – Canadian not-for-profit charitable organization for digital and media literacy providing resources to youth, parents and teachers.
Website: http://mediasmarts.ca/

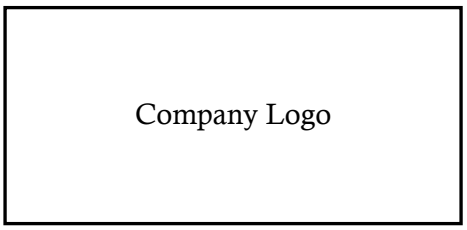
Canadian Women's Foundation - Organization that empowers women and girls in Canada to move out of violence, out of poverty, and into confidence and leadership.
Website: http://www.canadianwomen.org/

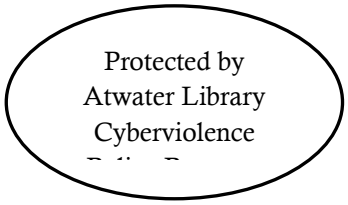
Project 10 – Non-profit organization that works to promote the personal, social, sexual and mental wellbeing of lesbian, gay, bisexual, transgender, transsexual, two-spirit, intersexed and questioning youth and adults 14-25 in Montreal.
Website: http://p10.qc.ca/

ASTT(E)Q – ASTT(e)Q is a non-profit organization that aims to promote the health and wellbeing of trans people through peer support and advocacy, education and outreach, and community empowerment and mobilization.
Website: http://www.astteq.org/

*Where the police are currently at in terms of responses to cyberviolence. If possible, ask someone you trust to accompany you when reporting your experience to the police, and throughout whatever ensuing processes.

Appendix D: Organizational Cyberviolence Template





Cyber Violence policy in our Origination consists of…

1
2
3
4
5

Here are the steps to take if you encounter cyberviolence

1
2
3
4
5

Contact Persons:

Singed and endorsed by Organization Cyberviolence Officer:
name.name@organization.com 514-xxx-xxxx, ext: xxxx

Singed and endorsed by Organization President:
name.name@organization.com 514-xxx-xxxx, ext: xxxx

Appendix E: References Used to Create this Document

Toronto District School Board:
tdsb.on.ca/Portals/0/Elementary/docs/SupportingYou/1800.pdf

Additional Footnotes throughout the document:

---

[i] Lauren M. Bernardi, 2011-05, Investigating Harassment Complaints: Ten Costly Employer Mistakes. Retrieved from https://www.hrpa.ca/Documents/PD/PD%202016/tencostymistakes.pdf

[ii] Ibid. Lauren M. Bernardi, 2011-05, Retrieved from https://www.hrpa.ca/Documents/PD/PD%202016/tencostymistakes.pdf

[iii] Ibid. Lauren M. Bernardi, 2011-05, Retrieved from https://www.hrpa.ca/Documents/PD/PD%202016/tencostymistakes.pdf

Buchwald, E., Fletcher, P. R., & Roth, M. (Eds.). (2005). *Transforming a rape culture* (p. XI). Minneapolis, MN: Milkweed Editions.