# Internet Harassment or Cyberbullying – Fact Sheet

## WHY SHOULD A WORKPLACE LOOK AT INTERNET HARASSMENT?

Many workers do their work using the computer and the Internet. Internet harassment is being identified as a concern at work, as well as at home and school.

### WHAT ARE EXAMPLES OF INTERNET HARASSMENT OR CYBERBULLYING?

Internet harassment, also referred to as “cyberbullying”, is the term used to describe the use of the Internet to bully, harass, threaten, or maliciously embarrass. It can involve behaviours such as:

- Sending unsolicited and/or threatening e-mail.
- Encouraging others to send the victim unsolicited and/or threatening e-mail or to overwhelm the victim with e-mail messages.
- Sending viruses by e-mail (electronic sabotage).
- Spreading rumours.
- Making defamatory comments about the victim online.
- Sending negative messages directly to the victim.
- Impersonating the victim online by sending an inflammatory, controversial or enticing message which causes others to respond negatively to the victim.
- Harassing the victim during a live chat.
- Leaving abusive messages online, including social media sites.
- Sending the victim pornography or other graphic material that is knowingly offensive.
- Creating online content that depicts the victim in negative ways.

### WHAT ARE SOME TIPS TO PREVENT INTERNET HARASSMENT?

While every situation is different, in general, steps to help prevent cyberbullying can include:

In the workplace:

- Use a gender neutral e-mail address if you have a choice.
- Make your e-mail password at least twelve (12) characters long although

longer passwords may be appropriate. Make sure that it is a combination of capital and lower-case letters, numbers, and symbols. The best passwords don't spell anything and don't follow a logical pattern.
- Change your password frequently.
- Review the workplace's policy about the use of e-mail signatures (the block of text that gets added automatically to the end of an outgoing message). It should provide enough information about the person so that they can be identified, but not so much that they are providing e-mail recipients with personal information.
- Use encryption, privacy settings, software, or other technological tools to increase the security provided to e-mails and internet use.
- Follow guidelines from your organization's Internet technology specialist as there will be additional requirements regarding privacy settings, and safety from computer viruses, malicious software, etc.
- Follow any policies or procedures your organization has in place for Internet communication. Discuss Internet privacy and safety with your organization's Internet technology specialist.
- Limit the information you share in your "out of office" message to the dates of your absence and who to contact. Don't broadcast that you are on vacation or on work-related travel.
- Do not leave your computer logged in and unattended.

Other tips:

- Be careful what you post. While you may be able to remove the original post, it is not possible to remove copies that others have made.
- Watch for "red-flags", for example someone asking where you live or where you work.
- Be very cautious about meeting online acquaintances in person. If you choose to meet, do so in a public place and take along a friend or business associate.
- For personal use, consider setting up two e-mail accounts. One used for formal correspondence and one that has another name for use in discussion groups, etc. Change or cancel your secondary account if you start receiving too much unwanted mail.
- If you want to remain anonymous, DO NOT list your e-mail address on any Web pages or give your e-mail address when filling out forms on Web pages unless necessary.
- If possible, use an anonymous browser to browse the Web. Web sites collect information about visitors (e.g., what Web browser you used, "cookies", your Internet Service Provider and potentially your e-mail address). Anonymous browsers offer varying degrees of security, some are free and some are not.
- Discuss your safety and privacy with your Internet Service Provider. Seek their help and advice.
- Make sure your Internet Service Provider, discussion groups and chat networks have an Acceptable Use Policy (no harassment permitted) and that the policy is enforced by the administrator of the site.

DO NOT

- Do not tell anyone your password.
- Do not share personal information in e-mail – even e-mail addressed to a trusted individual.

- Do not share personal information in public forums anywhere online, nor give it to strangers, including in chat rooms.
- Do not attack or insult anyone while participating in discussion groups. If you disagree with the person, state your position objectively and factually.

**HOW SHOULD YOU RESPOND IF SOMEONE IS HARASSING YOU BY E-MAIL?**

If the person is a member of your workplace:

- Report the incident(s) by following your workplace's policy and procedures for workplace bullying , harassment or violence.

If someone is harassing you by e-mail (in general):

- If the harasser is known to you, make it clear that you do not want him or her to contact you again.
- Once you have told a known harasser not to contact you again, or if you are receiving harassing e-mail from someone you do not know, block or filter messages from the harasser. Many e-mail programs have a filter feature that will automatically delete or place e-mails from a particular e-mail address or that contain offensive words into a separate folder.
- DO NOT reply to unsolicited, harassing or offensive e-mail if the harasser is not known to you. By responding, you confirm that your e-mail address is valid and active.
- DO NOT open attachments as they may contain viruses.
- Keep a log of any harassing activity.
- Save all offending communications for evidence, both electronically and in hard copy (print). Do not edit or alter them in any way.
- Using your name, conduct a Web search to find out if any information exists about you, so you are at least aware of what information about yourself is publicly available.
- If the harasser is known to you and harassment continues after you have asked the person to stop, contact the harassers Internet Service Provider (ISP).
    - Most ISP's have clear policies prohibiting the use of their services to abuse another person.
    - Often, an ISP can stop the conduct by direct contact with the harasser or by closing his or her account.
    - The ISP domain name is identified by the information after the @ (e.g. name @ home.com). Most ISPs have an e-mail address such as postmaster @ domain name that can be used for complaints.

**WHAT CAN YOU DO IF SOMEONE IS PUBLICLY HARASSING YOU (IN A DISCUSSION GROUP OR CHAT SITUATION)?**

In a discussion group:

- Keep a log of any harassing activity.
- Save all offending communications for evidence, both electronically and in hard copy (print). DO NOT edit them in any way.
- Contact the group's administrator and provide evidence of the harassment. If they fail to respond, stop participating in the group (i.e., have your e-mail removed from the group's distribution list).

In a live chat situation:

- Log off. If the situation causes you to fear for your safety or that of others, contact your local police or law enforcement agency.
- Keep a record of any harassing activity.
- Save all offending communications for evidence, both electronically and in hard copy (print). DO NOT edit them in any way.
- Contact the group's administrator and provide evidence of the harassment. If they fail to respond, stop participating in the group.

**WHAT SHOULD YOU DO IF SOMEONE IS BULLYING OR HARASSING YOU THROUGH SOCIAL MEDIA SITES?**

Most applications ("apps") and social media sites (such as Facebook, Twitter, YouTube, and Snapchat) have published guidelines that state what is and is not okay to be posted on their sites. You can find these guidelines by looking for pages on "Terms and Conditions", or Community Standards/Guidelines. These sites also have a mechanism for reporting abuse of these guidelines. When making a complaint, use the advice provided above about documenting your situation. Include a screenshot of the comment or a copy of the photograph as evidence when you submit your report. If you feel you are in immediate danger, contact the local police or law enforcement agency.

As a user, you can also opt to take action, such as:

- Always think before you post – are these words or this photo something you would want everyone to see? Could your comments elicit a potentially harmful reaction?
- Use recommended privacy settings provided by the site.
- Unfriend, hide, block, or mute another user from seeing your profile.
- Remove tags as necessary on posts or photos, or adjust your privacy settings so that you can review tags before they are published.
- Keep personal details private, including your address, date of birth, phone number, school, credit card number(s), and passwords. Be aware of the details you're showing in photos, such as address numbers, street names, and work buildings.
- Turn off location settings that may be embedded in your device when taking photographs.
- Log out of your accounts when you are not using them, especially when using a public computer or device.
- Avoid retaliating. Most bullies are looking to get a reaction.

**WHAT SHOULD YOU NOT DO IF BEING HARASSED OR BULLIED BY E-MAIL?**

DO NOT send or reply to e-mail when you are angry or upset. Wait until you are calm and composed; you do not want to become perceived as the harasser.

DO NOT rush into a confrontation. You can risk starting a "flame war" which can rapidly escalate.

DO NOT respond to flaming (provocation online).

DO NOT engage in any question and answer scenarios that make you feel uncomfortable.