CIR: Online Abuse Policy, Support Mechanisms, and Guidance

1. **Objective and Scope**

   This policy sets out CIR's mechanisms for supporting staff undergoing online abuse as a result of, or associated with, their work for CIR. It defines these phenomena and details the steps CIR associates (i.e., employees, consultants, and volunteers) should take if they are experiencing online abuse, so that CIR can provide the best support. It also gives advice on engagement with adversarial accounts online, as well as resources for support and guidance outside of CIR.

2. **Definitions**
   a. **Online abuse (incl. harassment, trolling, flaming, etc.):** "pervasive or severe targeting of an individual or group online through harmful behaviour."[1]
      i. *Why does severity matter?* CIR recognises that "even a single incident of online abuse, such as a death threat or the publishing of a home address, can have serious consequences."
      ii. *Why does pervasiveness matter?* We recognise that "while some individual incidents...such as insults or spam, may not rise to the level of abuse, a steady drumbeat of incidents, or a coordinated onslaught, does."
   b. **Doxxing:** the public release of personally identifiable information (PII), including addresses and phone numbers.

3. **Escalation:** CIR will do its utmost to assist you if you are facing an episode of intense and/or sustained online harassment, especially related to doxxing and violent threats. In order to do this, we must be notified as soon as possible that you are experiencing these harms. If you are experiencing:

   a. **One-off abusive messages:** keep a log of one-off abusive messages, replies, or other content you receive for future reference. Screenshots are an easy way to do this. Mute or block the sender, depending on your preferences.
   b. **Sustained abuse:** If you are experiencing sustained harassment, trolling, or abuse online, or feeling unsafe as a result of online interactions, inform your line manager/project director immediately.
   c. **Violent Threats or Doxxing:** If you receive a violent threat, no matter the forum or platform (email, social media, mail), or are doxxed, inform your line manager/project director immediately.

[1] PEN America, "Defining Online Abuse: A Glossary of Terms."
https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/

d. **When in doubt**: inform your line manager/project director to discuss the best course of action. In all cases, report the violative behaviour to the platform at hand via their on-platform reporting mechanisms.

All reports will be treated in strict confidence. If you would prefer, you may also report harms to the internal safeguarding email. This includes raising concerns if you think a colleague may be exposed to abuse and harassment online.

4. **CIR Management Responsibilities:** Below are support mechanisms available to staff, consultants, and volunteers.

   a. As a precautionary measure, an employee or consultant working over 40 hours per month who is concerned for their physical safety can request to be subscribed to a corporate DeleteMe account, which provides ongoing scanning and removal of personal information from online and offline sources;
   b. In addition to ongoing institutional online security checkups, CIR will conduct twice-yearly voluntary personal online security and digital self-care refresher trainings where CIR affiliates can ensure their personal devices, social media accounts, etc., are safe and secure, as well as discuss instances of online harassment they have experienced and tactics for withstanding them;
      i. Consider using “Privacy Party” Chrome extension to update your privacy posture on your social media profiles;
   c. Assign someone to temporarily take over your social media and/or email accounts to remove abusive content and/or report violative material;
   d. If you have been doxxed and/or received violent threats, CIR may provide you and the members of your immediate family with safe lodging – e.g. a hotel room or Airbnb, for a default period of two weeks, and longer if necessary, subject to security advice;
      i. Depending on the situation, CIR may also provide you with a Post Office box for mail forwarding;
   e. Assist you in working with local law enforcement should you want to raise a complaint;
   f. Raise complaints to social media platforms through offline channels;
   g. Assist you with heightened/continued online threat monitoring and/or crisis PR support for an initial period of one month after the incident;
   h. Employees can access personal legal advice and support through CIR’s Employee Assistance Programme.

5. **CIR Affiliate Expectations:** As detailed in CIR’s Social Media Policy, remember that any information you make public could affect how people perceive both CIR, our work and yourself. As such, remember that engaging with trolls or harassers online may escalate the situation and cause others to perceive you in a disadvantageous light.

We encourage you to mute or block abusive accounts rather than engage with them, and remind you that we do not tolerate any form of online hatred, bigotry, prejudice, harassment, discrimination, intimidation, exploitation, or abuse, just as we do not tolerate it offline. Nor do we tolerate posts which could, or could be seen to, promote violence, hatred, or discrimination against any individuals or groups. Finally, we do not tolerate doxxing.

6. **Resources:** Below are trusted resources for those undergoing online abuse. Through CIR's Employee Assistance Program, employees are also able to access a 24/7 counselling and advice line; 24/7 health and wellbeing advice and support; and face to face counselling, as well as medical referrals as needed.
    a. Bloom by Chayn: for survivors of gender based violence (online or offline) bloom.chayn.co
    b. The Online Violence Response Hub: onlineviolenceresponsehub.org
    c. Crash Override Network: crashoverridenetwork.com
    d. Right to Be: righttobe.org/guides/responding-to-online-harassment and social media safety guides
    e. Glitch UK: glitchcharity.co.uk
    f. PEN America Online Harassment Field Manual: onlineharassmentfieldmanual.pen.org