Addressing the Cyber-victimisation of disabled people in Northern Ireland:

a human rights issue and a public health priority

Policy Brief

Dr Zhraa Alhaboby
Jolena Flett
Anna Pustelnik

The British Academy

The Open University | PolicyWISE

Executive summary

Cyber-victimisation of disabled people is a human rights issue, a public health concern, and a barrier to safe participation online. Cyber victimisation is a form of digital abuse involving repeated and unwanted behaviours such as harassment, insults, threats, or spread of misinformation. Due to the complexity of the experience, we adopt the term "cyber-victimisation" as an umbrella covering cyberbullying, cyberharassment, cyberstalking, and cyber hate, when the targeted person is disabled. Cyber-victimisation of disabled people has immediate and long-term consequences for health and self-management, raises human rights concerns, and undermines the safety of online participation. For disabled people in Northern Ireland, these acts are not only traumatising but often go unrecognised in policy responses. This brief reports new evidence from a 2024 study of 113 disabled adults in Northern Ireland (NI), which revealed a high prevalence of online targeting. Despite clear harm, few victims received support, and none reported to the Police Service of Northern Ireland (PSNI).

Current responses rarely recognise the health consequences or rights implications. This brief sets out practical steps to protect health and self-management, uphold human rights, and enable safe online participation.

A public health and human rights issue

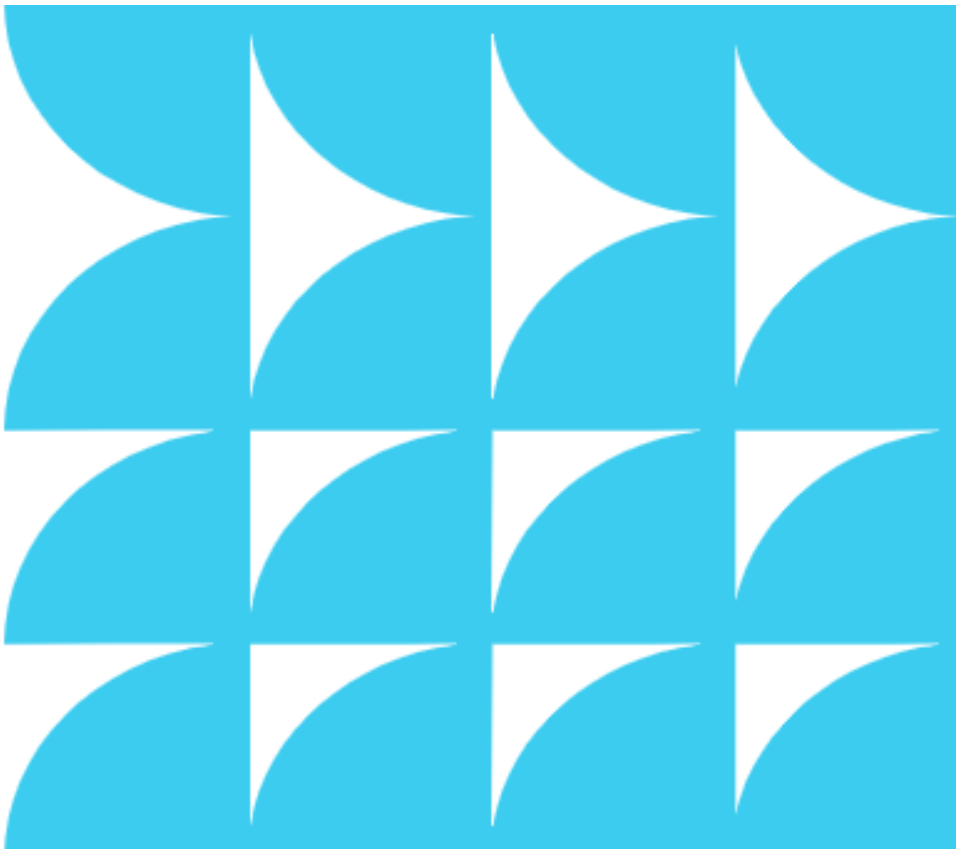
Cyber-victimisation should be recognised as a public health and human rights issue. While much of the research to date has focused on young people, this study is the first of its kind to explore the experiences of disabled adults in Northern Ireland. Of the 113 participants, 30.09% reported experiencing cyber-victimisation, and 23.01% specifically during the COVID-19 pandemic. These incidents included repeated hostility, sharing of private health or political information, coordinated pile-ons and direct messages designed to intimidate or shame.

Cyber-victimisation is a digital determinant of health, many participants highlighted how it had real-world consequences. Participants in Northern Ireland described missed appointments, unintended changes to lifestyle, changes to medications and self-monitoring, impact on mental health and stress-related flare-ups of existing conditions.

For disabled people, digital spaces are part of everyday life, social connection and self-care; for many, they are the only route to support and to health and wellbeing resources. When those spaces become unsafe, people lose support that help in managing long-term conditions and stay connected to services. Participants described feeling dehumanised, stigmatised, due to public misinformation and awareness level, fuelled by misrepresentation of disabled people politically and in public health messaging.

Key findings

- Cyber-victimisation was reported by 30.09% of participants, with 23.01% experiencing it during the pandemic.
- 44% of those who were targeted reported that online harassment disrupted their health management, including medication adherence, counselling, and lifestyle routines.
- Significant association between cyber-victimisation and disrupted health management ($p = 0.049$).
- Despite the harms, none of the participants reported incidents to police and only 22.7% received any form of support.
- NI context: exposure of health and political information, labelling as “a burden on taxpayers”, and heightened visibility in a small, politicised environment.
- Most participants received no formal support; none reported incidents to the police.
- Experiences were shaped by public attitudes, political context and the public health approach during the pandemic as an example of a public health emergency.
- Social media supported connection but also enabled targeting and disclosure of sensitive information.



Participants' voice

"I don't think the professional I have been dealing with really have any experience in dealing with disabled people to be honest."

Participant 7

"The impact, it was very, very frightening. I didn't know who to trust? I was worried for the safety of myself. I was worried for the safety of my children and my family. I was worried that perhaps my children would be targeted if they would be out and about. It had a major impact, to be honest […] it really, really did. It was a very, very frightening experience."

Participant 1

"Increased my anxiety and pain medication. Binge eating led to further obesity. Compounded my PTSD."

Participant 2

"Individual made specific reference to my worth as individual and questioned the purpose of me existing"

Participant 13

Accordingly, the priorities to address cyber-victimisation of disabled people in Northern Ireland include:

Human rights and equality framing

Cyber-victimisation of disabled people threatens dignity, equality and participation. A human rights approach recognises disabled people's rights to safety, privacy, health, accessible information, and participation in public life. In Northern Ireland, equality and disability duties require public bodies to prevent discrimination and promote inclusion. Treating cyber-victimisation as a rights issue shifts responsibility from the individual to systems that must protect, prevent and raise public awareness.

Inclusion and being safe in an online environment

Digital platforms were both a lifeline and a liability. Participants valued online communities and services, yet reported disclosure of sensitive health or political information, pile-ons and persistent targeting. If online spaces are not safe, access to services, including reporting, will not feel safe either; people may fear the information they provide could be used against them.
Safety by design, accessible reporting, rapid takedown and evidence preservation are needed. Locally, clear signposting, a simple referral pathway and trusted advocates can make disclosure safer and more effective.

Public health policy and multidisciplinary support

Cyber-victimisation should be recognised explicitly as a public health concern. Health and social care bodies can embed prevention and response within public health strategies, disability action plans and safeguarding frameworks, so that protection, early identification and support are routine rather than exceptional. Healthcare services can adopt clear care pathways that link primary care, mental health, routine and long-term condition services with advocacy partners and policing where appropriate.

Improve current pathways for referral and support

There is no single, published, end-to-end pathway linking health, safeguarding, advocacy and policing for cyber-victimisation, making public signposting fragmented and hard to navigate. Current routes include PSNI reporting via 999, 101 or the non-emergency online form; the Hate Crime Advocacy Service for advocacy and reporting support; Victim Support NI for practical support; and HSC Trust Adult Safeguarding Gateway Services where an adult is at risk of harm. These pathways will not be used if the environments in which they operate are perceived as unsafe. Co-design with disabled people, NGOs and relevant stakeholders is essential to ensure routes are accessible, trusted and effective.

Health-justice coordination and statutory duty

Given the multi-tiered nature of the issue, a formal interface between health and justice is required. Joint legislation or statutory guidance should create a duty on relevant bodies to have policies, clear procedures and referral pathways for responding to the cyber-victimisation of disabled people. This may include agreed standards for recording, risk assessment, evidence preservation, information-sharing compliant with data protection law, and warm handovers between health, policing and advocacy services. Regular multi-agency reviews would reduce fragmentation and improve access to both health and justice support. A statutory duty would standardise practice, reduce under-reporting and ensure victims receive coordinated support without having to navigate fragmented systems.

Recommendations

Short term (do now)

- Recognise cyber-victimisation within public bodies' disability action plans, in an approach that shifts responsibility from the individual to systems.
- Promote digital inclusion as a core equality issue, including accessible reporting mechanisms.
- Training for healthcare professionals to recognise patients who are being targeted and to offer appropriate support and prevent health complications.
- Provide training for frontline staff and community organisations on recognising, recording and responding to cyber-victimisation, with shared health–justice modules.
- Provide resources and awareness training on digital safety and the impact of online targeting for both disabled individuals and professionals.

Medium term (build coordination)

- Cross-sector collaborations for awareness-raising among the public on discrimination, rights, and tackling misinformation and misrepresentation of disabled people. Adopt the social model of disability and shift the narrative from "victim-blaming" to collective responsibility.
- Cross-sector collaborations to improve referral pathways between health, police, advocacy, and online platforms, with a single published pathway and service standards. (For example linking the Department of Health with PSNI, Victim Support NI and the Hate Crime Advocacy Service)

Long term (secure change)

- Establish a statutory duty, through joint legislation or guidance, requiring policies, procedures and monitoring for cyber-victimisation responses across health and justice; and regular multi-agency case reviews.

Dr Zhraa Alhaboby – Senior Lecturer in Biomedical and Health Sciences, The Open University

Jolena Flett - Head of Advocacy and New Projects, Victim Support Northern Ireland

Anna Pustelnik -Hate Crime Project Manager, Hate Crime Advocacy Service

This research was supported by the British Academy [Grant number: SRG23\230025].

PolicyWISE

The Open University

PolicyWISE is a unique UK and Ireland comparative policy, research, and knowledge exchange initiative. It brings people and research together to find solutions to cross-nation issues facing policymakers.

PolicyWISE is UK and Ireland by design (working across The Open University's unique four nations base), supporting policymakers and researchers across the nations to develop relationships, respect, and knowledge. Through their Wise in 5 briefings, training, and cross-nation research projects, PolicyWISE aims to improve and inform policymaking through comparative research and analysis.

The Open University
Open Societal Challenges

Dr Zhraa Alhaboby has led pioneering research in the UK on the cyber-victimisation of people with long-term conditions and disabilities. She has collaborated with general practitioners, police forces, organisations, and disability and victim support groups to explore this serious issue and promote change. Her work has generated evidence to inform policy recommendations on hate crime legislation and communication offences in the UK. The current British Academy–funded project in Northern Ireland is carried out in partnership with the Hate Crime Advocacy Service and Victim Support Northern Ireland. This study forms part of a broader programme at The Open University addressing the cyber-victimisation of disabled people as a societal challenge, aiming to enhance support through changes in policy and practice

Get in Touch:

www.policywise.org.uk

policywise@open.ac.uk

Follow us:

PolicyWISE