The 3PO Toolkit

3PO

Protecting police officers, police staff and their families from online harms

Common Online Harms against Police Officers, Staff and Families

Common Online Harms Types

SOCIAL MEDIA HARMS

- Psychological harm originating from active attacks through social media platforms[1].
- The source of the harm is often from members of the public. It can also originate from other officers and/or staff as an extension of workplace bullying, or from ex-officers and staff seeking to vent frustration or gain perceived retribution.
- **Five overall 'themes'** of social media harm (with subthemes) were identified:

1. **Reputation Harm**: Attempts to harm the professional reputation of individual officers/staff.
    a. **Defamatory Accusations**: Posts/comments about an individual's character in a way that undermines their public trust.
    b. **Misconduct Allegations**: Unsubstantiated claims of corruption and/or misconduct from specific officers/staff.
2. **Personal Harm**: Personal insults directed at individual officers/staff.
    a. **Hostile Sexism**: Sexist insults towards female officers/staff relating to their capability, physical attractiveness and/or sexuality.
    b. **Physical Presentation**: Non-sexual insults directed at the physical appearance and presentation of officers/staff.
    c. **Mental Capacity**: Insults about the perceived intelligence and/or age of police officers/staff.
3. **Abusive Protest**: Generally, abusive comments and posts are made around perceived political bias demonstrated by the police. Often targeted DEI initiatives within the police, such as supporting LGBTQ+ rights at Pride events, supporting black and minority ethnic officers and staff.
4. **Security Harm**: The personal identification of police officers/staff members, which may harm the security of the individual (i.e., doxing).
5. **Institutional Harm**: Abusive comments and posts about the police as an institution and a wider rejection of the authority of the police (e.g., ACAB, pigs). Harms the individual's pride as a police officer/staff, impacting retention.

EXPOSED ONLINE INFORMATION

The public availability of personal information about police officers/staff and/or Dependants. This can be exposed by a number of sources:

1. **Self-Published** by the officer/staff member, for example, sharing images or posts that indicate the area where they live or locations they frequent.
2. **Friends and Family** may post identifiable information about officers/staff on insecure social media accounts.
3. Posted by the **Police Force**, for example, neighbourhood teams posting names and photographs of local officers, which could be used maliciously by bad actors.
4. **The media** may publish information about police officers and staff, particularly following high-profile incidents.
5. **Members of the Public** may post information about officers (see Social Media Harms – Identification).

UNCLEAR GUIDANCE FOR ONLINE ACTIVITY

- Grey area of 'unprofessional' online behaviour below the criminal threshold.
- A poor definition can lead to officers/staff inadvertently engaging in unprofessional online behaviour.
- Also creates officer/staff fear around what they can/can't do online.

LIMITING ONLINE PRESENCE

- Indirect harm caused by officers/staff limiting their online activity.
- For example, disengagement from social responsibility, such as engaging with online school/parent groups.
- Reduced ability to establish professional networks – limits future options.

Contact

If you have any questions about this document, the 3PO Toolkit, or the project generally, please contact us at **centric@shu.ac.uk.** For more information about the project background, please visit **3po-project.co.uk**.

Access to the 3PO Toolkit

This document forms part of the 3PO Toolkit. To access the remaining elements of the toolkit, visit: **https://centric-research.co.uk/projects/3po/toolkit**.

Project Details

3PO (Protecting Public-Facing Professionals and their Dependants Online) was a three-year research project supported by the Engineering and Physical Sciences Research Council under UKRI's Strategic Priority Fund (Grant Ref: EP/W032368/1; duration April 2022 - March 2025).

3PO investigated the unique challenges and risks faced online by police officers, police staff, and their families. Whilst considerable research about online harms is being conducted on groups such as journalists and elected officials, the awareness of police officers and staff as potential victims remains limited. 3PO aimed to increase awareness and knowledge of this challenge by exploring the extent and nature of online harms faced by officers and staff in their policing roles and in their private lives, as well as the impact of these harms on them, their families, and police forces. It used these foundations to develop approaches and solutions to improve prevention, mitigation and support.

The 3PO project was led by CENTRIC (Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research) and brought together five universities (UCL, Cambridge, Oxford, Edinburgh Napier U/SIPR, Sheffield Hallam), six UK police forces, and the UK Home Office.

Contributors to this document

The typology is based on Merry, Oliver. (2026). What online risks and harms do police experience and to what extent? In P.S. Bayerl, K. Whitfield, I. Becker, J. Crapper, J. Crane, B. Akhgar (Eds), Online Harms and Risks against Police: From Management to Mitigation. Springer.

centric@shu.ac.uk