The 3PO Toolkit

3PO

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

Personal Guidance

To Better Protect Yourself & Your Family Online

Personal Guidance to Increase Protection for Yourself and Your Family Online

The **Personal Guidance** proposes various steps you and your family can take in order to better protect yourself and your family from online harms.

By online harms, we refer to '*behaviours online which may hurt a person physically or emotionally. It could be harmful information that is posted online, or information sent to a person*' (UK Online Harms Whitepaper, 2019).

The guidance is divided into three sections:

- **Steps suggested to improve the protection of your online information and accounts**
- **Steps to understand shared risks and manage common online needs**
- **Steps to ensure appropriate evidence collection**

Following the guidance will not protect you from all harms or malicious activities. If you have concerns about an online incident, please do speak to your line manager or other appropriate channels, and where possible, collect evidence.

STEPS SUGGESTED TO IMPROVE THE PROTECTION OF YOUR ONLINE INFORMATION AND ACCOUNTS	
CONTENT MANAGEMENT: manage and review the type of information available online	
Be cautious about revealing your role	We advise caution if • Mentioning your role in policing • Posting police-related content • Before liking or joining groups or pages that could expose your profession Rationale: While it may not be possible to control information that the public or your organisation posts, most often malicious online attacks use information from private accounts (e.g., home address or information about family, children, hobbies).

CONTENT MANAGEMENT: manage and review the type of information available online	
Reduce risks of inadvertent information leaks by family members, friends or colleagues	• Make relevant others (family members, friends, colleagues, etc.) aware of any information they should not post • Ask family, friends and/or colleagues not to forward, comment on or like posts that contain information about yourself, your work or your role Rationale: A considerable amount of data leaks occur due to online behaviours by close others such as family members, friends, clubs or colleagues.
Separate your private and professional lives	• Avoid using the same accounts, usernames, or email addresses for both • Consider using an alternative name and deleting identifiable profile pictures on social media • Stay consistent about when to use which account, email, etc. (e.g., for online purchases, logins to platforms) • Avoid using private devices for work purposes (e.g., OSINT) Rationale: Clear and consistent separation between private and professional accounts and online presences helps to avoid unwanted linkages of information from your professional and private lives.
Consider physical security risks	• Reduce information about locations such as where you live, spend time, or where you or your family travels to (travel plans, home-related details, expensive purchases) • Avoid checking into places in real-time or including location data in posts; if necessary, post about locations after leaving to reduce the risk of being tracked • Avoid providing details about your routines Rationale: According to our research, a small but relevant number of online incidents develop into physical threats. This can be visits from the attacker to your police station or even visits to your home address. It is therefore important to consider physical security risks next to online security.
Regularly check online information available about you and/or your family	• Search for your name online to check where it appears (e.g., reviews, public databases, discussion groups) and remove or adjust privacy settings where possible Rationale: Apps and platforms can change their privacy settings often without a clear announcement. Previously private information may then become visible online. Regular checks will also help find information other people may have posted (on purpose or inadvertently) about you and/or your family that you might prefer to stay hidden.

ACCESS MANAGEMENT: strategically decide who can see which information and set controls accordingly

Determine your privacy level	• Decide which risks you are willing to take for yourself • Decide what risks you are willing to take for your family and other people (friends, colleagues) • Determine what privacy level is appropriate Rationale: Personal risk levels will determine how locked down or open your online information and accounts need to or can be.
Manage who can see your information	• Regularly revise your friend and follower lists to ensure that they are the people you would like to have access to your profile, interactions and posts • Review the privacy settings of your social media accounts and other online presences to limit access to your profile, friends/followers list, posts, and location • Check that privacy settings across all your social media accounts and other online presences are consistent and thus afford the same level of privacy and protection • Check privacy settings regularly Rationale: Privacy controls and standard settings differ across platforms. It is therefore important to check that they are all at the desired level of protection. **Note:** The 3PO Self Assessment Tool (SAT) can help you adjust your privacy settings based on your desired visibility and risk level.

CYBER HYGIENE: ensure basic cyber hygiene for yourself and your family

Passwords, PIN codes, and biometrics	• Always lock your devices using strong passwords, PINs, patterns or biometrics • It's unrealistic to remember unique passwords for every account; consider using a password manager to store and generate strong passwords. Built-in password managers (e.g., Apple's iCloud Keychain, Google Password Manager) are good options when protected with a strong master password. ◦ *BETTER*: consider using a standalone password manager (e.g., KeePassXC, BitWarden and 1Password); they provide greater control and security • Don't share passwords within your family or, if required, discuss associated risks

CYBER HYGIENE: ensure basic cyber hygiene for yourself and your family

Two-Factor Authentication (2FA)	For more sensitive accounts and information:
	• Turn on 2FA for important accounts (email, banking, social media) or use an authentication app (e.g., Google Authenticator, Microsoft Authenticator, Authy) or SMS codes
	• Keep backup codes in a safe place:
	  ◦ A physical location: write them down and keep them in a locked drawer, safe, or fireproof box
	  ◦ Store them in a password manager (see above) or an encrypted file on your computer or cloud storage
	  ◦ *BETTER*: save them on a USB drive encrypted with a password, or a secure digital space
	
	Rationale: 2FA helps protect your account by requiring a second step, such as a code sent to an app or via text message, especially when logging in from a new device or location.

Device updates	• Turn on automatic updates for your devices (e.g., phone, computer, tablet, printer, gaming consoles) and apps • Regularly check for updates if automatic updates aren't available
Public Wi-Fi	• Use mobile data whenever possible, especially in places like trains, coffee shops, and airports If you must connect to public Wi-Fi: • Avoid accessing sensitive accounts, such as banking or email, to reduce the risk of data theft • Consider using a Virtual Private Network (VPN) to encrypt your connection

STEPS TO UNDERSTAND SHARED RISKS AND MANAGED COMMON ONLINE NEEDS

PRIVACY AGREEMENTS: having open discussions about privacy expectations and needs

Agree on acceptable and unacceptable risks	• Discuss with relevant people (family members, friends, colleagues) which online risks you and they are willing to take • Aim to make clear agreements on responsibilities to manage your and others' online information and behaviours Rationale: Open discussion on online risks creates a shared understanding of what is acceptable and the responsibilities each of you has for protecting from online harms.
Make your own privacy needs and expectations transparent	• Talk to family, friends, and colleagues about your privacy needs and expectations to ensure they respect your preferences • Let them know if you prefer not to be tagged, mentioned, or have personal details shared online Rationale: Transparent communication about your expectations gives others guidance on what they can or cannot disclose about you.

PRIVACY AGREEMENTS: having open discussions about privacy expectations and needs

Ask before posting or tagging others	• Ask for consent before sharing, tagging, or mentioning photos; friends, family, and colleagues may have stricter privacy needs than you do

CHILDREN: include children in your conversation about online protection

Have conversations with your children	• Promote open, friendly and age-appropriate communication about online risks related to your role in the police • Aim to understand whether they encounter any challenges online because of your role in the police (e.g., due to negative online news or videos about police or negative reactions by friends) • Demonstrate and encourage safe online behaviour and best practices, including posting, friending, privacy settings, digital footprints, and the consequences of private/personal information being publicly available Rationale: Parents and caregivers should take a managed and informed approach when addressing children about online harms.
Steps for keeping them safe	• Stay informed and up to date on social media platforms that your children use • Use parental controls if required • Monitor online activity responsibility Rationale: Parents and caregivers should take a managed and informed approach when discussing online harms with children.

EVIDENCE COLLECTION: capture incidents that worry you

Capture incidents that worry you	• Capture incidents in good quality and with metadata, where possible
	• Screenshot or cut/paste of social media pages/photos
	  ◦ The harmful content itself (e.g., post, message, comment)
	  ◦ Profiles of author(s) of said harmful content
	  ◦ Video screenings
	  ◦ URL links
	
	Note: Screenshots are the best way to secure evidence, as URL links can be deleted.
	
	• Note and record any identifying features of the person responsible for the harmful content/incident
	  ◦ The name(s) of the suspect(s) if known
	  ◦ Other online identifiers, e.g., usernames and profile IDs on social media platforms, additional profile URLs (on Facebook), or mobile numbers (on WhatsApp).
	
	Note: If suspect identity details are not known, you should not conduct any enquiries to establish these. This includes enquiries on police systems. Make a report in your force instead.
	
	Rationale: Online content can disappear quickly. If an online incident concerns you, it should be captured in sufficient detail to be useful for further investigation, if required.

EVIDENCE COLLECTION: capture incidents that worry you

Report problematic incidents to your police force	• Report online threats or harms to your police force Rationale: If threats or harms are related to your role in the police, your force should be made aware of the incident(s).

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

Chris Rowley KPM, Prof P Saskia Bayerl, Dr Marcel Obst, Dr Lasara Kariyawasam, Dr Shane Horgan, Dr Ingolf Becker, Dr Kris Christmann, Dr Kate Whitfield, Dr Charlotte Coleman, Adam Bates, Prof Katrin Mueller-Johnson

centric@shu.ac.uk