FOI Disclosures July 2024

Index

This month we have responded to questions relating to the following topics:

If you require a full copy of any of the embedded attachments, please contact Requestinfo@policeconduct.gov.uk quoting the reference number from the relevant response.

Ref 5024920 Back to top	**Time taken to produce investigation reports**
Request	*Please provide the average time taken to produce the investigation report from investigations which started in 2023. Please separate out the investigations as follows:* *1) Independent* *2) Directed* *3) Local*
Response	It is significant to note that we consider an investigation is completed on the date when the final report is approved. The following data therefore includes investigations that were started between 1 January 2023 and 31 December 2023 and show as completed up until 26 June 2024. You should take into consideration the following caveats when considering this data: •Data is for illustrative purposes only. •An investigation is counted as completed on the date when the final report is approved. •The duration on an investigation is calculated in working days from referral received date to final report approved date and does not include the duration of any subsequent investigation(s) or proceedings. •This information is taken from live data and as such may differ from previously published data and statistics.

	From the investigations that were started in 2023 and show as completed (i.e. final investigation report approved date), it took us on average: 1)153 working days to complete the Independent investigations; 2)236 working days to complete the Directed/Managed investigations. Local investigations are conducted by police forces and therefore we do not hold this information relating to local investigations. You should redirect this part of your request to police forces.
Ref 5024930 Back to top	**IOPC printers and photocopiers**
Request	*Various questions our printing and photocopying contracts.*
Response	*1. Number of MFDs (Multi-functional devices) & photocopiers at Independent Office for Police Conduct* 18 in live service and 1 as stock item. *2. Name of incumbent* Hewlett Packard / Canon. *3. Start/end date of contract (if expired, WHEN do you expect to revisit the marketplace)* The XMA Limited contract expired on 31 March 2024. A new procurement process (via suitable framework) is underway for the delivery of consumables. *4. Details of any extension options* N/A. *5. What framework / Route to market used* We purchase printers via CCS RM6147 Framework (Technology Online Purchasing Content) and this framework ends on 18 November 2024. *6. Number of regular/desktop printers (in addition to above)*

77 Portable printers; 48 Home Based Printers; 11 Network Printers (not MFD); 25 Printers (held as stock).

7. Is there a support contract on above, if yes please state start/end date

No. We deal with issues (e.g. regarding hardware) by calling in the device manufacturer each time.

8. Does IOPC have a Print Room

No.

9. If yes, name of supplier, number of devices and start/end date of contract, also details of any extension options

N/A.

10. Total annual print/copy volumes including, if applicable your Print Room, for (a) mono (b) colour

For the last 12 months (from 26/06/2023 to 26/06/2024), the overall page count was 689,815, of which 479,182 was in black and white and 210,633 in colour.

11. What Print software does IOPC run

Followme.

12. Your total annual spend on print

Total annual spend on print 23/24 was £15,421.

13. Who is responsible for this contract at the IOPC

Enquiries relating to these matters should be directed to the Head of ICT .

Ref 5024961

Back to top

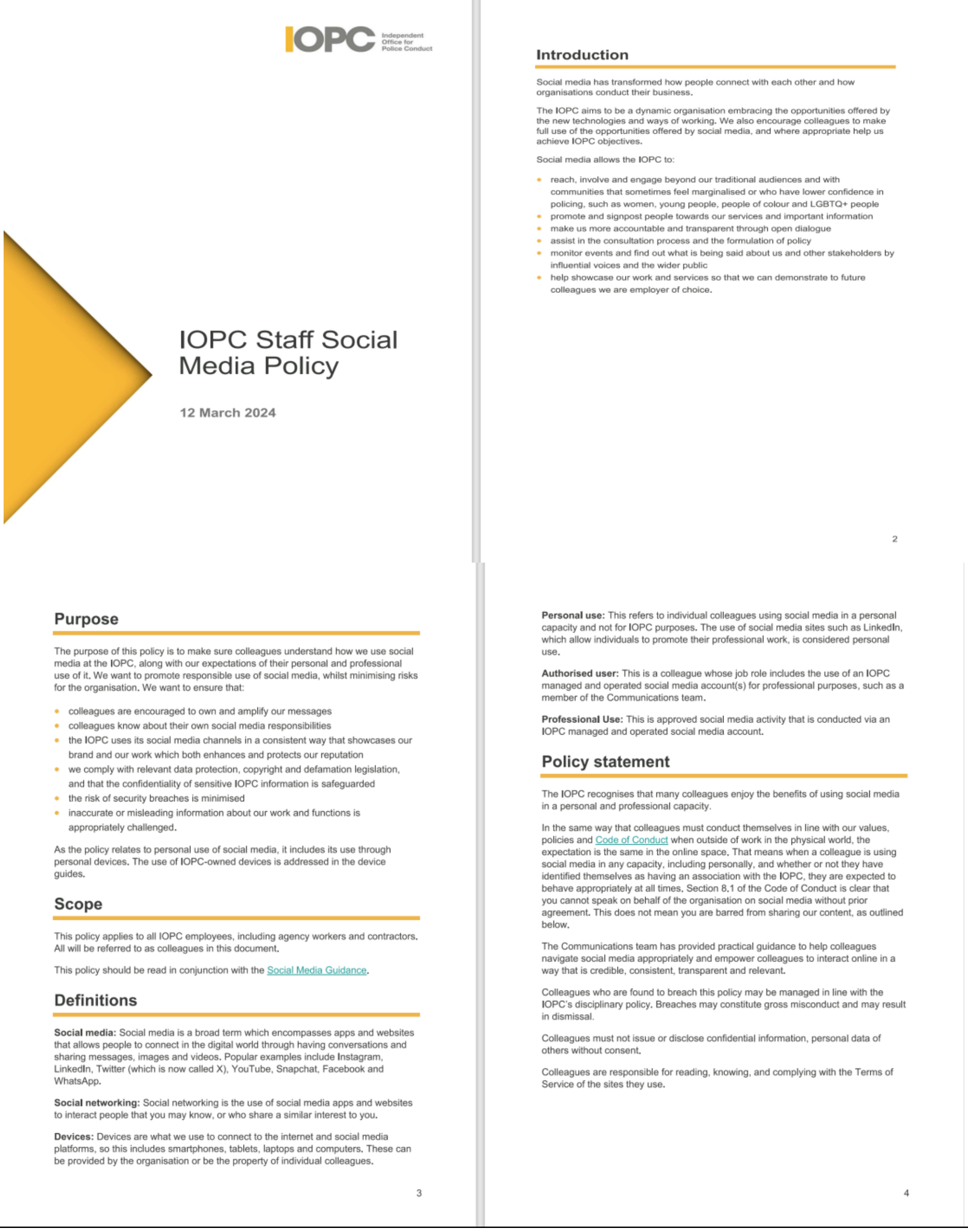
IOPC Social Media and Equality Policies

Request

I tried to locate your organisation's social media policy for staff and your equality policy on your website, but I could not find either. Could you forward me copies?

Response

Our social media policy is attached below:



Independent Office for Police Conduct

IOPC Staff Social Media Policy

12 March 2024

Introduction

Social media has transformed how people connect with each other and how organisations conduct their business.

The IOPC aims to be a dynamic organisation embracing the opportunities offered by the new technologies and ways of working. We also encourage colleagues to make full use of the opportunities offered by social media, and where appropriate help us achieve IOPC objectives.

Social media allows the IOPC to:

- reach, involve and engage beyond our traditional audiences and with communities that sometimes feel marginalised or who have lower confidence in policing, such as women, young people, people of colour and LGBTQ+ people
- promote and signpost people towards our services and important information
- make us more accountable and transparent through open dialogue
- assist in the consultation process and the formulation of policy
- monitor events and find out what is being said about us and other stakeholders by influential voices and the wider public
- help showcase our work and services so that we can demonstrate to future colleagues we are employer of choice.

Purpose

The purpose of this policy is to make sure colleagues understand how we use social media at the IOPC, along with our expectations of their personal and professional use of it. We want to promote responsible use of social media, whilst minimising risks for the organisation. We want to ensure that:

- colleagues are encouraged to own and amplify our messages
- colleagues know about their own social media responsibilities
- the IOPC uses its social media channels in a consistent way that showcases our brand and our work which both enhances and protects our reputation
- we comply with relevant data protection, copyright and defamation legislation, and that the confidentiality of sensitive IOPC information is safeguarded
- the risk of security breaches is minimised
- inaccurate or misleading information about our work and functions is appropriately challenged.

As the policy relates to personal use of social media, it includes its use through personal devices. The use of IOPC-owned devices is addressed in the device guides.

Scope

This policy applies to all IOPC employees, including agency workers and contractors. All will be referred to as colleagues in this document.

This policy should be read in conjunction with the Social Media Guidance.

Definitions

Social media: Social media is a broad term which encompasses apps and websites that allows people to connect in the digital world through having conversations and sharing messages, images and videos. Popular examples include Instagram, LinkedIn, Twitter (which is now called X), YouTube, Snapchat, Facebook and WhatsApp.

Social networking: Social networking is the use of social media apps and websites to interact people that you may know, or who share a similar interest to you.

Devices: Devices are what we use to connect to the internet and social media platforms, so this includes smartphones, tablets, laptops and computers. These can be provided by the organisation or be the property of individual colleagues.

Personal use: This refers to individual colleagues using social media in a personal capacity and not for IOPC purposes. The use of social media sites such as LinkedIn, which allow individuals to promote their professional work, is considered personal use.

Authorised user: This is a colleague whose job role includes the use of an IOPC managed and operated social media account(s) for professional purposes, such as a member of the Communications team.

Professional Use: This is approved social media activity that is conducted via an IOPC managed and operated social media account.

Policy statement

The IOPC recognises that many colleagues enjoy the benefits of using social media in a personal and professional capacity.

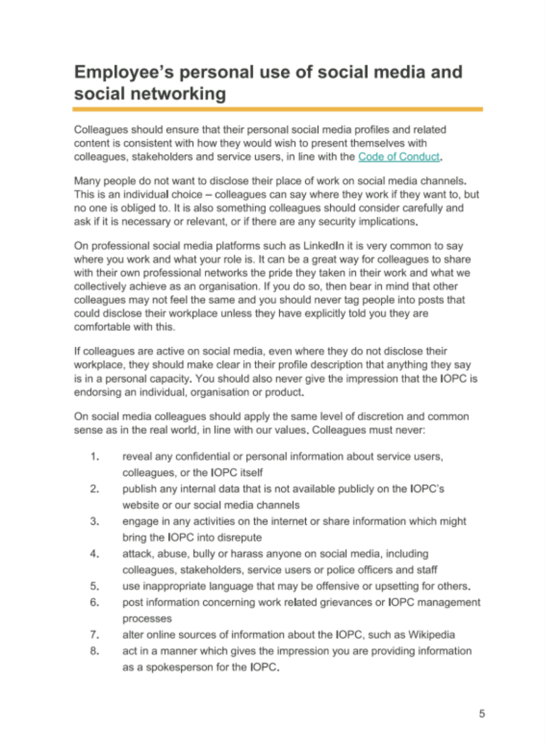
In the same way that colleagues must conduct themselves in line with our values, policies and Code of Conduct when outside of work in the physical world, the expectation is the same in the online space. That means when a colleague is using social media in any capacity, including personally, and whether or not they have identified themselves as having an association with the IOPC, they are expected to behave appropriately at all times. Section 8.1 of the Code of Conduct is clear that you cannot speak on behalf of the organisation on social media without prior agreement. This does not mean you are barred from sharing our content, as outlined below.

The Communications team has provided practical guidance to help colleagues navigate social media appropriately and empower colleagues to interact online in a way that is credible, consistent, transparent and relevant.

Colleagues who are found to breach this policy may be managed in line with the IOPC's disciplinary policy. Breaches may constitute gross misconduct and may result in dismissal.

Colleagues must not issue or disclose confidential information, personal data of others without consent.

Colleagues are responsible for reading, knowing, and complying with the Terms of Service of the sites they use.



Employee's personal use of social media and social networking

Colleagues should ensure that their personal social media profiles and related content is consistent with how they would wish to present themselves with colleagues, stakeholders and service users, in line with the Code of Conduct.

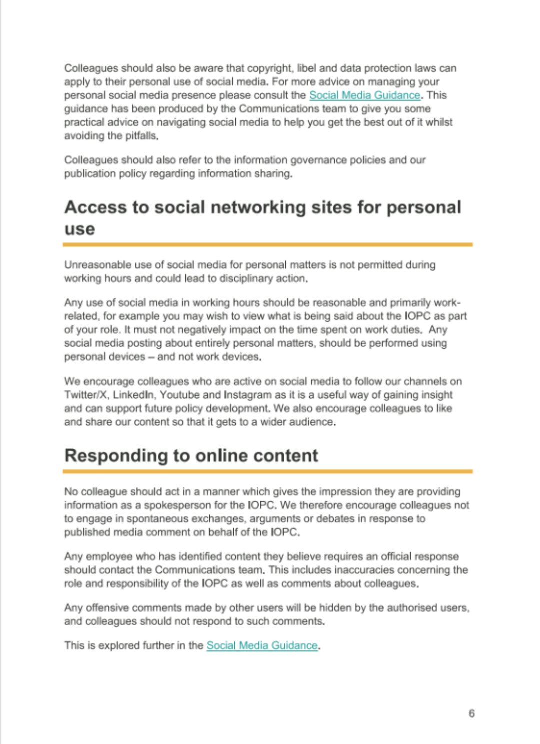
Many people do not want to disclose their place of work on social media channels. This is an individual choice – colleagues can say where they work if they want to, but no one is obliged to. It is also something colleagues should consider carefully and ask if it is necessary or relevant, or if there are any security implications.

On professional social media platforms such as LinkedIn it is very common to say where you work and what your role is. It can be a great way for colleagues to share with their own professional networks the pride they taken in their work and what we collectively achieve as an organisation. If you do so, then bear in mind that other colleagues may not feel the same and you should never tag people into posts that could disclose their workplace unless they have explicitly told you they are comfortable with this.

If colleagues are active on social media, even where they do not disclose their workplace, they should make clear in their profile description that anything they say is in a personal capacity. You should also never give the impression that the IOPC is endorsing an individual, organisation or product.

On social media colleagues should apply the same level of discretion and common sense as in the real world, in line with our values. Colleagues must never:

1. reveal any confidential or personal information about service users, colleagues, or the IOPC itself
2. publish any internal data that is not available publicly on the IOPC's website or our social media channels
3. engage in any activities on the internet or share information which might bring the IOPC into disrepute
4. attack, abuse, bully or harass anyone on social media, including colleagues, stakeholders, service users or police officers and staff
5. use inappropriate language that may be offensive or upsetting for others.
6. post information concerning work related grievances or IOPC management processes
7. alter online sources of information about the IOPC, such as Wikipedia
8. act in a manner which gives the impression you are providing information as a spokesperson for the IOPC.



Colleagues should also be aware that copyright, libel and data protection laws can apply to their personal use of social media. For more advice on managing your personal social media presence please consult the Social Media Guidance. This guidance has been produced by the Communications team to give you some practical advice on navigating social media to help you get the best out of it whilst avoiding the pitfalls.

Colleagues should also refer to the information governance policies and our publication policy regarding information sharing.

Access to social networking sites for personal use

Unreasonable use of social media for personal matters is not permitted during working hours and could lead to disciplinary action.

Any use of social media in working hours should be reasonable and primarily work-related, for example you may wish to view what is being said about the IOPC as part of your role. It must not negatively impact on the time spent on work duties. Any social media posting about entirely personal matters, should be performed using personal devices – and not work devices.

We encourage colleagues who are active on social media to follow our channels on Twitter/X, LinkedIn, Youtube and Instagram as it is a useful way of gaining insight and can support future policy development. We also encourage colleagues to like and share our content so that it gets to a wider audience.

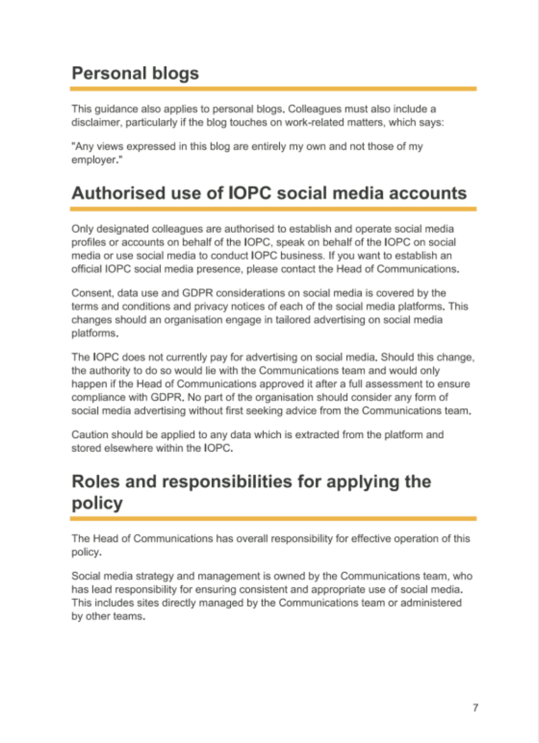
Responding to online content

No colleague should act in a manner which gives the impression they are providing information as a spokesperson for the IOPC. We therefore encourage colleagues not to engage in spontaneous exchanges, arguments or debates in response to published media comment on behalf of the IOPC.

Any employee who has identified content they believe requires an official response should contact the Communications team. This includes inaccuracies concerning the role and responsibility of the IOPC as well as comments about colleagues.

Any offensive comments made by other users will be hidden by the authorised users, and colleagues should not respond to such comments.

This is explored further in the Social Media Guidance.



Personal blogs

This guidance also applies to personal blogs. Colleagues must also include a disclaimer, particularly if the blog touches on work-related matters, which says:

"Any views expressed in this blog are entirely my own and not those of my employer."

Authorised use of IOPC social media accounts

Only designated colleagues are authorised to establish and operate social media profiles or accounts on behalf of the IOPC, speak on behalf of the IOPC on social media or use social media to conduct IOPC business. If you want to establish an official IOPC social media presence, please contact the Head of Communications.

Consent, data use and GDPR considerations on social media is covered by the terms and conditions and privacy notices of each of the social media platforms. This changes should an organisation engage in tailored advertising on social media platforms.

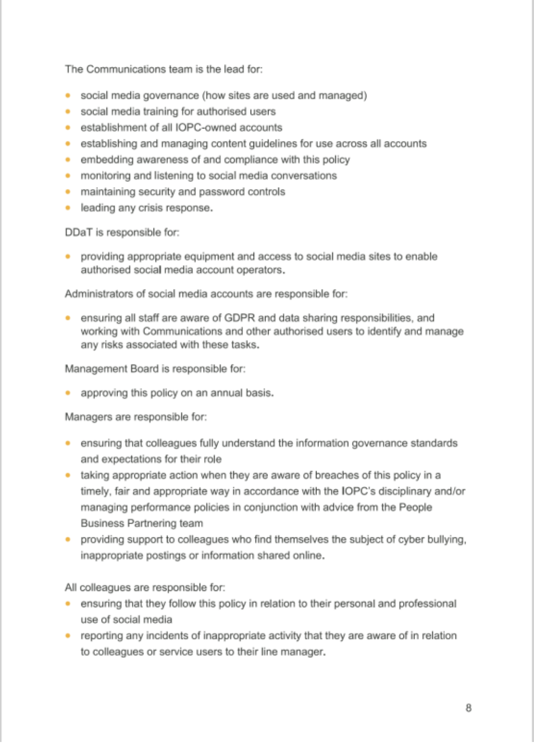
The IOPC does not currently pay for advertising on social media. Should this change, the authority to do so would lie with the Communications team and would only happen if the Head of Communications approved it after a full assessment to ensure compliance with GDPR. No part of the organisation should consider any form of social media advertising without first seeking advice from the Communications team.

Caution should be applied to any data which is extracted from the platform and stored elsewhere within the IOPC.

Roles and responsibilities for applying the policy

The Head of Communications has overall responsibility for effective operation of this policy.

Social media strategy and management is owned by the Communications team, who has lead responsibility for ensuring consistent and appropriate use of social media. This includes sites directly managed by the Communications team or administered by other teams.



The Communications team is the lead for:

- social media governance (how sites are used and managed)
- social media training for authorised users
- establishment of all IOPC-owned accounts
- establishing and managing content guidelines for use across all accounts
- embedding awareness of and compliance with this policy
- monitoring and listening to social media conversations
- maintaining security and password controls
- leading any crisis response.

DDaT is responsible for:

- providing appropriate equipment and access to social media sites to enable authorised social media account operators.

Administrators of social media accounts are responsible for:

- ensuring all staff are aware of GDPR and data sharing responsibilities, and working with Communications and other authorised users to identify and manage any risks associated with these tasks.

Management Board is responsible for:

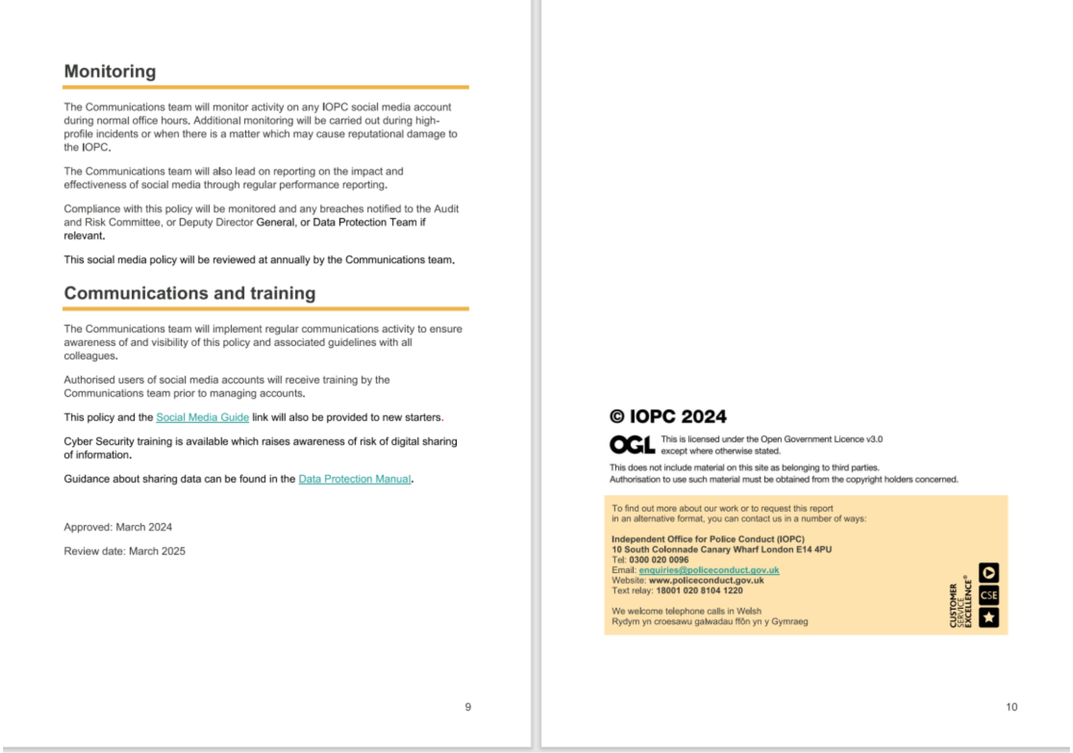
- approving this policy on an annual basis.

Managers are responsible for:

- ensuring that colleagues fully understand the information governance standards and expectations for their role
- taking appropriate action when they are aware of breaches of this policy in a timely, fair and appropriate way in accordance with the IOPC's disciplinary and/or managing performance policies in conjunction with advice from the People Business Partnering team
- providing support to colleagues who find themselves the subject of cyber bullying, inappropriate postings or information shared online.

All colleagues are responsible for:

- ensuring that they follow this policy in relation to their personal and professional use of social media
- reporting any incidents of inappropriate activity that they are aware of in relation to colleagues or service users to their line manager.



Monitoring

The Communications team will monitor activity on any IOPC social media account during normal office hours. Additional monitoring will be carried out during high-profile incidents or when there is a matter which may cause reputational damage to the IOPC.

The Communications team will also lead on reporting on the impact and effectiveness of social media through regular performance reporting.

Compliance with this policy will be monitored and any breaches notified to the Audit and Risk Committee, or Deputy Director General, or Data Protection Team if relevant.

This social media policy will be reviewed at annually by the Communications team.

Communications and training

The Communications team will implement regular communications activity to ensure awareness of and visibility of this policy and associated guidelines with all colleagues.

Authorised users of social media accounts will receive training by the Communications team prior to managing accounts.

This policy and the Social Media Guide link will also be provided to new starters.

Cyber Security training is available which raises awareness of risk of digital sharing of information.

Guidance about sharing data can be found in the Data Protection Manual.

Approved: March 2024

Review date: March 2025

9

To find out more about our work or to request this report
in an alternative format, you can contact us in a number of ways:

Independent Office for Police Conduct (IOPC)
10 South Colonnade Canary Wharf London E14 4PU
Tel: **0300 020 0096**
Email: enquiries@policeconduct.gov.uk
Website: **www.policeconduct.gov.uk**
Text relay: **18001 020 8104 1220**

We welcome telephone calls in Welsh
Rydym yn croesawu galwadau ffôn yn y Gymraeg

10

Our Equality Policy for staff is available here: https://www.policeconduct.gov.uk/sites/default/files/documents/EDI-Policy-FINAL.pdf

Objective 2 of our Equality, Diversity & Inclusion Strategy 2022-25 relates to service users. This is: “To deliver an equitable, culturally competent service to all of those we come into contact with throughout our work”. Please see pages 10 to 12 for further information.

Ref 5024962 Back to top	**IOPC training and guidance relating to cases involving vulnerable adults**

Request

I am seeking information related to the IOPC’s cases where the police handle cases involving vulnerable adults. Specifically, I would like to request the following:

1. Policies and Standards:

- *All current policies related to the management of vulnerable adults.*
- *Any standards or guidelines followed by the police regarding vulnerable adults.*
- *Copies of meeting minutes where policies were approved, including any notes, alterations or changes (board, executive committee etc.).*
- *Internal memos or correspondence related to the policy changes.*
- *Training materials and schedules.*

2. Procedures and Processes:

- *Detailed procedures for handling cases involving vulnerable adults.*

- *Flowcharts or process maps illustrating the management of vulnerable adults.*
- *Risk assessments and compliance reports*

Response

In addition to asking for police policies on this subject, we have understood your request as asking for the IOPC's policy, guidance or standards that we apply when assessing our cases that involve complaints, conduct matters or other incidents relating to the treatment of vulnerable adults by police.

Our responses to each part of your request are set out below.

- *Any standards or guidelines followed by the police regarding vulnerable adults.*

The IOPC does not hold this information. Each police force has its own policies/guidance relating to vulnerable adults and the results of our searches of police websites suggest that the information you would like to see is likely to be contained in a range of documents relating to the various operational contexts in which the police come into contact with them.

We would therefore recommend that you make a request to police forces for this information. When doing so it may be helpful if you were to identify the type of policing situation in which you are interested (e.g. detention of persons with mental health conditions, victims of sexual offences etc.), as this should reduce the amount of information that they would have to search before they could answer your request.

The following information issued by the police service is available to you online and would appear to be relevant to your request:

- The College of Policing Authorised Professional Practice (APP) is the official source of professional practice for policing. This includes a significant amount of content under this category, please see for example: Adults at risk | College of Policing

- Right Care Right Person – Humberside Police | College of Policing (the IOPC's statement on right care right person can be accessed here: right-care-right-person-position-statement-march-2024_0.pdf (policeconduct.gov.uk))

- Recognising and responding to vulnerability related risks: Guidelines (college.police.uk)

- national-vulnerability-action-plan-2020-2022.pdf (npcc.police.uk)

- *All current policies related to the management of vulnerable adults.*
- *Copies of meeting minutes where policies were approved, including any*

notes, alterations or changes (board, executive committee etc.).

- *Internal memos or correspondence related to the policy changes.*
- *Training materials and schedules.*

We have carried out a key word search of our digital document management system using the term ‘vulnerable adults’ and the results do not include information within the scope of these bullet points about how the IOPC assesses police conduct in relation to ‘vulnerable adults’ specifically.

It may help you to know, however, that in practice any such assessment would be carried out in reference to the force policies and procedures that officers are expected to apply in the relevant policing context (e.g. detention and custody), as well as the NPCC and College of Policing information sign-posted above.

The information on our website may help you to understand the nature of our work relating to vulnerable adults who come in contact with the police. Our ‘key areas of work’ include several categories that frequently relate to incidents involving vulnerable adults. We have published a significant amount of information relating to these key areas, as set out below.

Our Key areas of work page on our website summarises our thematic work, which includes violence against women and girls (VAWG), race discrimination, abuse of power for sexual purpose (APSP), domestic abuse, mental health and welfare and vulnerable people.

You may find it helpful to read our learning recommendations. When we complete our independent investigations or reviews, we sometimes share learning recommendations with the police. Using this table, you can carry out a learning recommendations search which can be filtered by our ’key areas of work’, together with other key words, to find recommendations that would be likely to relate to vulnerable adults.

Our Learning the Lessons series of publications aims to support the police in improving policy and practice. For example, Issue 40 takes an in-depth look at APSP. You can use the case factor table to find Learning the Lessons articles on specific themes or police operational areas that may involve vulnerable adults.

We would also recommend that you visit the IOPC’s Annual deaths during or following police contact statistics | Independent Office for Police Conduct (IOPC). We examine the circumstances of all deaths referred to us to produce these statistics and decide whether the deaths meet the criteria for inclusion in this report under one of the following categories:

- road traffic fatalities
- fatal shootings
- deaths in or following police custody
- apparent suicides following police custody

- other deaths following police contact that were subject to an independent investigation

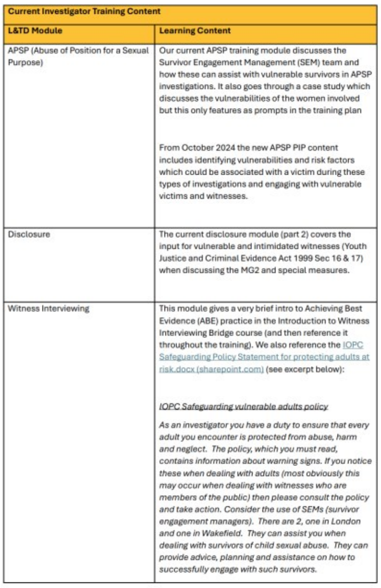
The final category refers to our thematic case selection and separates our independent investigations according to the reason for contact with police. These reasons include self-harm/suicide/mental health.

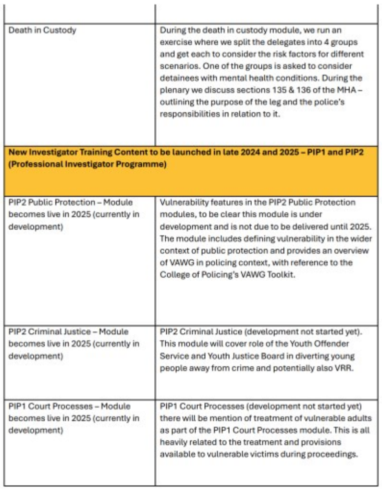
You can search the content of these reports by keyword to help you find any cases that may be of interest.

This super-complaint investigation would also appear to be relevant: Police perpetrated domestic abuse: Report on the Centre for Women's Justice super complaint - GOV.UK (www.gov.uk) The information published by IOPC about this investigation is available here: Police must improve how they respond to domestic abuse allegations against officers and staff | Independent Office for Police Conduct (IOPC)

Our web site includes a facility to carry out an Investigations summaries search which can be filtered by key area of work so that you may then narrow down your search using key words to refine results filtered by, for example, 'violence against women and girls' and 'welfare and vulnerable people'.

In regard to your request for training materials and schedules, we attach a document containing information about the parts of our investigator training programme that relate to vulnerable adults. Please note that only some of this relates to the policing of vulnerable adults (e.g. the training in relation to the detention of persons with mental health conditions), as distinct from training in how to safeguard the interests of vulnerable adults with whom we come into contact.





Current Investigator Training Content	
L&TD Module	**Learning Content**
APSP (Abuse of Position for a Sexual Purpose)	Our current APSP training module discusses the Survivor Engagement Management (SEM) team and how these can assist with vulnerable survivors in APSP investigations. It also goes through a case study which discusses the vulnerabilities of the women involved but this only features as prompts in the training plan From October 2024 the new APSP PIP content includes identifying vulnerabilities and risk factors which could be associated with a victim during these types of investigations and engaging with vulnerable victims and witnesses.
Disclosure	The current disclosure module (part 2) covers the input for vulnerable and intimidated witnesses (Youth Justice and Criminal Evidence Act 1999 Sec 16 & 17) when discussing the MG2 and special measures.
Witness Interviewing	This module gives a very brief intro to Achieving Best Evidence (ABE) practice in the Introduction to Witness Interviewing Bridge course (and then reference it throughout the training). We also reference the IOPC Safeguarding Policy Statement for protecting adults at risk.docx (sharepoint.com) (see excerpt below): *IOPC Safeguarding vulnerable adults policy* *As an investigator you have a duty to ensure that every adult you encounter is protected from abuse, harm and neglect. The policy, which you must read, contains information about warning signs. If you notice these when dealing with adults (most obviously this may occur when dealing with witnesses who are members of the public) then please consult the policy and take action. Consider the use of SEMs (survivor engagement managers). There are 2, one in London and one in Wakefield. They can assist you when dealing with survivors of child sexual abuse. They can provide advice, planning and assistance on how to successfully engage with such survivors.*
Death in Custody	During the death in custody module, we run an exercise where we split the delegates into 4 groups and get each to consider the risk factors for different scenarios. One of the groups is asked to consider detainees with mental health conditions. During the plenary we discuss sections 135 & 136 of the MHA – outlining the purpose of the leg and the police's responsibilities in relation to it.
New Investigator Training Content to be launched in late 2024 and 2025 – PIP1 and PIP2 (Professional Investigator Programme)	
PIP2 Public Protection – Module becomes live in 2025 (currently in development)	Vulnerability features in the PIP2 Public Protection modules, to be clear this module is under development and is not due to be delivered until 2025. The module includes defining vulnerability in the wider context of public protection and provides an overview of VAWG in policing context, with reference to the College of Policing's VAWG Toolkit.
PIP2 Criminal Justice – Module becomes live in 2025 (currently in development)	PIP2 Criminal Justice (development not started yet). This module will cover role of the Youth Offender Service and Youth Justice Board in diverting young people away from crime and potentially also VRR.
PIP1 Court Processes – Module becomes live in 2025 (currently in development)	PIP1 Court Processes (development not started yet) there will be mention of treatment of vulnerable adults as part of the PIP1 Court Processes module. This is all heavily related to the treatment and provisions available to vulnerable victims during proceedings.