Use of IT, Communications and Social Media

1. This policy applies to all members of staff including temporary members of staff, those on work experience, consultants, contractors (including Board Members), and volunteers employed or engaged by the OPCC. Third parties who have access to our electronic communication systems and equipment are also required to comply with this policy. Individuals will be expected to make an annual declaration that they have read and understood this policy and will comply with the terms outlined within it.

2. The Policy aims to:
   - protect our interests and the reputation of the PCC and his office
   - clarify who may engage externally on behalf of the business, and the process to do this
   - clarify how you may use the internet and social media in respect of delivering your role
   - provide guidance on the use of all forms of social media
   - set out the permitted parameters of use of the electronic communications (telephone, e-mail and internet) and
   - inform you of how we will treat any non-compliance with the Policy; and

3. This policy therefore may be amended at any time. We may also vary any parts of this procedure, including any time limits, as appropriate in any case. You are expected to comply with this Policy at all time.

4. This policy should be read in conjunction with the Information Management Policy and the Staff Handbook. We may take disciplinary action against you if you do not comply with any part of the policy.

General Principles

5. Everyone must consider the impact of the PCC's reputation in the course of their work.

6. Good communication is essential for the PCC to deliver his role, and for the OPCC to enable him to do so.

7. With the exception of the Deputy PCC, all staff within the OPCC hold politically restricted posts. All use of media and communications must comply with these political restrictions.

8. During work you are required to devote your time and attention to our business and to support our goals and objectives. Therefore, the electronic communications systems are in place for work related matters only.

9. When using any of the telephone, email or internet, you must do so in a manner that is responsible, professional and is consistent with our normal standards of business. Any personal use of the telephone, email and internet is subject to this policy and may be permitted only if such use is reasonable and limited.

10. Users of our communications systems sometimes have access to highly sensitive information and staff are expected to maintain the highest professional and ethical standards.

External Communications

11. If your duties require you to speak on behalf of the OPCC you must have the express permission of the Chief Executive, and you must follow the details of this policy. This policy applies for in person communication as well as using the internet and social media. The Chief Executive may require you to undergo training before you do so and impose certain requirements and restrictions with regard to your activities.

12. Once permission has been sought all content for external publication should be reviewed by the Chief Executive (this function may be delegated). This includes press information as well as interviews, public presentations, articles for publication and strategies, reports and documents for a public audience (this list is non exhaustive). The office may also use the material as part of the communication strategy.

13. You should refer to the style guide and templates for letters and correspondence. You may not use the OPCC letterhead for personal letters or non-official correspondence. You may sign correspondence, invoices or orders for us only if you have authorisation and only in accordance with our normal procedures. All incoming post whether marked personal, private or confidential or in any other way will be opened and dealt with by us in accordance in our normal procedures.

Use of Social Media

14. This policy deals with the use of all forms of social media and all internet postings, whether written, audio or video. Examples include social media websites such as Facebook, LinkedIn, Twitter Wikipedia, and all other internet postings, including blogs, videos and podcasts. The policy applies to the use of social media for both personal and business purposes, whether this is done during business hours or otherwise. It also applies whether social media is accessed using our IT facilities or equipment belonging to you.

15. You may use social media to provide commentary on our, or related activities in a manner that is generally supportive and provides helpful comment or commentary. You may not use your own social media to give information ahead of corporate publication.

    If you see content in social media that disparages or reflects poorly on our organisation or our stakeholders, you should inform us. All staff are responsible for protecting our reputation.

16. Personal use of social media is never permitted during work time or by means of our computers, networks and other IT resources and communications systems.

17. We may require you to remove any internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

18. You must not:
    - use social media in a way that breaks any of our other policies
    - break any rules of relevant regulatory bodies
    - break any obligations you have relating to confidentiality

- jeopardise our trade secrets and intellectual property
- use our logos, brand names, slogans or other trademarks, or post any of our
- confidential or proprietary information without prior written permission
- misappropriate or infringe the intellectual property of other companies and individuals
- defame or disparage us or our affiliates, business partners, suppliers, vendors or other stakeholders or make any communication which (in our opinion) brings us, or them into disrepute or causes harm to our or their reputation
- render us liable for copyright infringement or fail to accurately reference sources of information posted or uploaded
- harass or bully other staff in any way
- unlawfully discriminate against other staff or third party
- breach our Data Protection Policy (for example, never disclose personal information about a colleague online)
- comment on sensitive topics related to our work; or
- breach any other laws or ethical standards (for example, never use social media in a false or misleading way, such as claiming to be someone other than yourself or by making misleading statements)

19. You should ensure that you take steps to secure your social media accounts for personal safety. This should include: setting security settings to restrict access to those you don't know, not sharing personal information, such as email and home addresses, turning off GPS/location tracking options and being aware of the impact of your social media use on others. You should be careful about adding applications to social media accounts, as you will often be granting permission to account information to the third party provider, and therefore may compromise the security of your account. If you use third party apps make sure you read the small print before signing up.

Corporate Social Media Accounts

20. All applications for new corporate accounts must be approved in writing by the Chief Executive before they are opened by staff. Any individual who wishes to open an account must demonstrate that the account has a purpose to promote the work of the OPCC and that they understand their responsibilities in managing the account (as detailed in this document). Any individual who no longer wants to have an official account must either pass the account to another team member to carry on (informing the Chief Executive when this happens) or close the account down. Nobody can change an official account to a personal account.

21. All accounts should link back to the main OPCC website to provide context and background as well as to help drive traffic onto the main site.

22. The Chief Executive reserves the right to refuse new social media accounts, or close any social media accounts that do not comply with this policy. The Chief Executive will monitor all corporate social media accounts to ensure that they comply with policy and guidelines, and will issue guidance to individuals where appropriate.

23. All social media accounts must have their usernames and passwords registered with the Chief Executive to ensure that accounts can be protected and recovered if hacked. Individuals must also inform the Chief Executive when they change their password, name of account or owner of the account at the time of its change. All OPCC corporate social media accounts will be administered by the Chief Executive, and the Chief Executive may remove any material at his discretion. The Chief Executive will keep details of all staff members with access, and change passwords when team membership changes.

24. All social media accounts must be accurate, as well as kept up to date and relevant, with a regular flow of new content to maintain user interest. Out-of-date content should be removed as soon as it becomes out of date. The development of corporate sites will be the responsibility of the Chief Executive. Account owners will be responsible for the content of local sites. Managers will be responsible for monitoring the accuracy and relevance of local content.

25. All video footage, comments, text and photographs appearing on social media should reflect the corporate nature of the site. Nothing should be posted that could bring the OPCC into disrepute or conflict with our corporate message/style. No materials classified as SECRET or TOP SECRET using the Government Security Classification, should be published on the website. It is the responsibility of the member of individuals posting photographs or footage to ensure that they comply with legal or data protection requirements and, if necessary, a risk assessment, DPIA and/or EQIA should be carried out.

26. Uploading any information to social media is a form of disclosure and therefore must comply with data protection principles. Individuals should also ensure that they are familiar with the Freedom of Information Act 2000.

27. Social media accounts should not be used to liaise with journalists. All requests from journalists or information to be given out to journalists should be coordinated by the Chief Executive.

28. Whilst it is acknowledged you may choose to use your own personal mobile phones to update your corporate social media accounts, you are reminded to be careful about the security of your own equipment. If a personal mobile device with a police social network is lost, you should contact the IT Department as soon as possible.

Personal use of Social Media

29. You should not make reference to the OPCC on personal social media accounts if comments are critical, or ridicule the organisation or other colleagues. You should also consider carefully any indirect reference to your role or the organisation.You are accountable for whatever you put into the public domain even in a personal account. Inappropriate use or inappropriate disclosure of personal information on social media sites is subject to criminal proceedings (in accordance with Section 170 of the Data Protection Act 2018 it is a criminal offence to disclose personal information unlawfully) and/or misconduct procedures.

30. If you use your personal details to contribute to social media you should take into consideration the fact you will be placing personal details into the public domain. This may impact on your own privacy, the security of family and friends, and may compromise your vetting status.

31. You should also be aware that the media use social media to gather information about public sector staff, including personal details, telephone numbers, e-mail addresses and links, images and interests, and are entitled to report on anything posted.

32. You must note that any comments made on social media will be deemed to be in the public domain and seen as official comment. Any comments could therefore be liable to a misconduct severity assessment. This applies to both personal and corporate sites. Comments made on personal sites should not reveal confidential information or jeopardise police operational matters.

33. When using personal accounts no use may be made of the Police and Crime Commissioner or his office in name, crest or insignia without the express permission of the Chief Executive. Consideration must also be given to any other matters of copyright. You also may not use OPCC photographs or images without the permission of the Chief Executive.

34. You should not set up unofficial or spoof groups, pages or accounts.

35. During election periods individuals should not post comments which could be judged to express political opinion on their own social media sites, or on other people's sites (in particular the political candidates). This is particularly important during elections for Police and Crime Commissioners.

Use of the Internet

36. The Chief Executive has responsibility for maintaining the standards of our Internet and Intranet sites and ensuring that the IT system complies with the agreed security measures.

37. In order to access the IT network you must only use devices provided by the OPCC or otherwise authorised by the Chief Executive. You may only install approved software on our computer hardware and you may not download any software without prior permission of the Chief Executive.

38. Security of devices and the data stored therein will remain the responsibility of the individual user. Devices must always be used in accordance with the guidance and instructions provided when issued or subsequently. This is particularly important with regard to maintaining the security of the laptop and information it contains.

39. Use of the internet for personal purposes is at our discretion. A small amount of personal internet use is permitted provided that:
    - It is not excessive
    - it does not interfere or conflict with business use
    - only browsing of the internet is undertaken
    - the activity is not undertaken during work time; and
    - the restrictions set out in this policy are adhered to

40. If unsuitable material is accidentally accessed on the internet you should immediately report this to your manager so that the circumstances can be explained and considered. Generally, no action will be taken for genuine accidental access to unsuitable material.

41. Where you suspect that any accessed file may contain a virus, you must immediately break the connection, stop using the device and report the matter to the IT support desk.

42. You must not use your work devices to:
    - access external personal email accounts
    - visit auction sites, sites promoting offensive or extremist views, sites promoting any form of discrimination or hate crimes, personal contact and dating sites, music and entertainment sites, games sites or any other sites which could bring us into disrepute
    - register to receive regular emails from such sites which are not for business purposes
    - download software or copyright information from the internet without prior permission

- take part in shares or securities dealing or undertake financial transactions related to a personal business
- post or disseminate information which you know to be confidential about us or our staff, suppliers or other stakeholders unless you have the relevant authority to do so
- gamble on the internet
- purchase private goods or services; or
- view, access, attempt to access, download or upload materials which we deem to be obscene, offensive, harassing, discriminatory, violent or pornographic

Use of Email

43. You should use email, both internally and externally, primarily for your work and in the normal course of our business and serving our customers. The standard and content of email messages must be consistent with the standards we expect for other written communications and email messages should always be presented in the approved corporate style.

44. You must ensure that at least one other member of staff has access to your work email account. This is to ensure continuity of work in the case of your being unavailable. It is your responsibility to ensure that you others who have access to your email account have been selected with recourse to the level of confidential information in your inbox.

45. Email should not be used to transmit information insecurely, or to an insecure site.

46. If emails being sent externally contain information about any individual then the sender should be aware that this might constitute the disclosure of personal data subject to the Data Protection Act. It must be ensured that such disclosure is in compliance with our policies on data protection and the disclosure of information. Where appropriate the Privacy Notice should also be sent (as a hyperlink or attachment to the email).

47. Examples of misuse of emails includes :
    - excessive use for personal purposes
    - sending or circulating emails which contain language which is abrupt, inappropriate or abusive
    - forwarding unsolicited junk email or other advertising material to other users who did not specifically request such material, whether internally or externally
    - accepting or open any file received as an email attachment if you are in any doubt about its source or content
    - creating, transmitting, downloading, printing or storing software, or anything which may cause harassment or alarm or anything which breaches copyright or other intellectual property rights
    - receiving emails from internet sites with which you have registered and which are not for business purposes
    - disseminating information either within or outside the OPCC which you know to be confidential about us or our staff, customers or suppliers, unless you have the relevant authority to do so
    - transmitting, receiving, retaining, displaying, printing, forwarding or otherwise disseminating material which we deem to be offensive, fraudulent, illegal, harassing, discriminatory, offensive, pornographic, obscene or defamatory; or
    - deliberately or recklessly disseminating destructive programs such as viruses or self-replicating codes

IT Equipment

Mobile Technology

48. Your access to telephone or video-conferencing facilities is to enable you to carry out your work. You may make personal calls but these should be short, infrequent, and within the UK. You must reimburse the organisation for costs incurred in personal use. Overseas calls are not allowed except for work related purposes.

49. You may be supplied a mobility device for work-related purposes. All mobility devices and personal mobile phones should be switched onto silent/vibrate mode when on open working floors.

50. You must not share your personally issued device with anyone else, even internal colleagues. Where pool devices have been provided, these devices will be shared only between named, designated users of the team who have also signed this agreement. Users are responsible for their own device (or the pool device) and all actions carried out upon it.

51. Users should avoid opening any attachments which are unexpected or from unsolicited sources.

52. Some of the settings on your device have been configured by your system administrator to help keep the information on it secure. Changing or circumventing these settings could put information at risk.

53. If using a device overseas, you must consult with Information Security at least 7 days before travel. You must take extra care to ensure that they cannot be overlooked and take all possible precautions to prevent their device being stolen. There are several legal issues surrounding the overseas carriage and use of cryptographic items that must be considered in addition to any specific handling procedures based on the perceived threat.

54. You must not use any personal devices to share confidential or sensitive information about individuals. This includes using personal mobile phones to take photos for media purposes.

55. Examples of misuse of mobile technology include:
    - private or freelance business
    - gambling
    - pornography
    - chat lines
    - conducting political activity
    - sending, forwarding or replying to offensive or obscene text or other messages or attachments
    - passing on confidential information about us or any of our work, or any other information which could bring us into disrepute or could amount to a security breach
    - making potentially libellous or untrue malicious statements; and
    - making or sending hostile, harassing or bullying calls or message

Security Incidents

56. If a force device has been lost/stolen you must contact the Help desk immediately on 3344 or 0121 626 8344 or if out of hours call 101. If you believe your password has been compromised and you have not always been in possession of the device you must contact the helpdesk immediately. You must also contact IT&D if your device appears not to be functioning as normal, or shows signs of physical tamperingYou must also contact

the OPCC Data Protection Officer (Head of Business Services) as this may be a data breach under the Data Protection Act 2018.

57. You must keep your mobility device locked when not in use and exercise care when entering your device password or pin code, and not disclose it to anyone (including IT&D support staff, managers or colleagues).

58. It is important that passwords are strong (i.e. random and difficult to guess). If a weak password is chosen, this could make it easy for sensitive data on the device to be accessed should the device fall into the wrong hands. You must adhere to the WMP Password Policy which includes
    - Do not use the same password for a mobile device as for any other system.
    - If the password is written down, it must be placed in an envelope marked OFFICIAL and treated accordingly (i.e. kept in a secure cabinet). Under no circumstances should a written copy of the password be carried along with the device.
    - If a user has any reason to believe that their password has been compromised, it must be changed immediately.

59. Mobile devices are an attractive target to thieves. In addition to the obvious inconvenience of having a device stolen, there is also a risk of sensitive data being extracted from a stolen device by an attacker. Therefore, users must take all possible measures to avoid their device being stolen – and not be left unattended in a public place.

Monitoring

60. We may monitor you in the following ways:

Medium	**Nature of Monitoring**
Laptop or mobility device	• We may monitor your access to devices and any information you hold on them.
Telephone	• The number, duration and destination of telephone calls made and received may be monitored and reports produced. This is to ensure that no excessive or inappropriate use is made of the telephone system. • We may access your voicemail whilst you are absent, e.g. due to holiday or sickness, to check whether any messages are about your work or our business. • In certain rare circumstances, we reserve the right to record and listen to telephone conversations. This will be where we suspect you are carrying out illegal or criminal activity (including forms of discrimination, bullying or harassment), or activity which puts our interests at serious risk. We will only take this action if it is not possible, feasible or realistic to obtain the information/evidence in any other way.
Email	• We may monitor your individual email traffic, including the use of certain email addresses • We have the right to access your email account whilst you are absent, eg due to holiday or sickness, or after you have left our employment, to check whether any emails are about your work or our business. • We also reserve the right to retrieve and read any email you send or receive if we suspect you are carrying out illegal or criminal activity (including forms of discrimination, bullying or harassment), or activity which puts our interests at serious risk.

	We will only take this action if it is not possible, feasible or realistic to obtain the information/evidence in any other way. •
Internet	• We may monitor your individual internet traffic, including viewing which internet sites you have accessed. We may limit your access if we consider that you are making excessive or inappropriate use of the internet for private purposes.
Social Media	• We may monitor your individual social media postings and activities to ensure that our rules are being complied with and for legitimate business purposes.

Disciplinary Action

61. Inappropriate use of the telephone, email and internet may lead to legal claims against us and/or you. You must not knowingly use the telephone, email or internet to break the laws and regulations of the UK or any other country.

62. Failure to comply with this policy will normally be considered to be misconduct under the disciplinary policy, although serious misuse can be treated as gross misconduct. Examples of behaviour which may be treated as gross misconduct include but are not limited to:
    - posting or disseminating information which you know to be confidential about us or our staff, stakeholders or suppliers unless you have the relevant authority to do so
    - failure to comply with the Government Security Classification system
    - transmitting, receiving, retaining, displaying, printing, forwarding or otherwise disseminating material which we deem to be fraudulent, illegal, harassing, discriminatory, offensive, pornographic, obscene or defamatory
    - deliberately or recklessly disseminating destructive programmes such as viruses or self-replicating codes
    - gambling on the internet
    - bring us, or our affiliates, partners, suppliers, vendors or other stakeholders into disrepute; or
    - viewing, accessing, attempting to access, download or upload materials which we deem to be obscene, offensive, harassing, discriminatory, violent or pornographic

Version Control

Version No	Date	Author	Post	Reason For Issue	Date agreed by PCC	Review Schedule
1.0	Jul 2018	Richard Costello	Head of Media and Communications	General Review		Annual
2.0	Nov 2018	Polly Reed	Head of Business Services	Structural review		Annual
3.0	August 2021	Andrea Gabbitas	Head of Business Services	General Review		Annual
4.0	May 2022	Lucy Naylor	Human Resource Manager	General Review		Annual

Appendix A: Guidance about Political Restriction

Background

a. All OPCC employees are "politically restricted". This is a legal term derived from statute, and therefore a serious and important part of your contract with the OPCC. It is not guidance, but a legal requirement on all employed OPCC staff.

b. There are certain things you cannot do, which are above and beyond those that apply to members of staff in other public bodies. It does not mean that you have to be politically neutral; it places restrictions on your political activities. Compliance with these requirements is not only critical to maintaining public confidence in the work of the OPCC, but forms the bedrock of our working relationship with the current and future PCCs.

c. If you are uncertain, speak with your line manager in the first instance. Much better to get a manager's view than trying to decide unilaterally whether something is appropriate. As an overarching principle, we must each act in such a way as to maintain the confidence of the PCC. However, we must also bear in mind that we must act in such a way that the next PCC can have the same level of confidence in us, whoever that person may be. This principle is drawn from the Civil Service Code, which colleagues should read. Colleagues should take every care to avoid any embarrassment to the PCC which could result, inadvertently or not, from bringing themselves prominently to public notice in party political controversy.

d. Deliberate failure to comply with the requirements of political restriction would generally constitute gross misconduct which, if proven, can lead to dismissal.

e. The PCC, Deputy PCC and contractors are not employees and are not politically restricted. Employee colleagues are accountable to their manager and ultimately me as Head of Paid Service and Monitoring Officer for their conduct.

What political activities are restricted?

f. OPCC employees cannot stand for election in local, parliamentary or European elections. For the purposes of political restriction, "local elections" include PCC elections. If a member of staff wishes to stand in an election, they need to let their manager know as soon as possible - there are protocols to follow. “Stand” is not defined, but is broader than merely being on the Statement of Persons Nominated for a given election; it includes seeking the candidacy for a given party. Political restriction also means that OPCC staff cannot act as election agents or subagents. OPCC staff can seek roles in the administration of elections – Presiding Officers, Poll Clerks etc – subject to management approval.

g. OPCC employees cannot hold an office in a political party, or the branch of a political party, where this involves the general management of a party or a branch, or acting in a role that includes contact with non-party members. "Political party" is not defined, but acting in such roles for anyone seeking office in local, parliamentary or European elections would not be permitted. Colleagues are advised to seek advice before taking any active political role that could be perceived as supporting a given candidate or party, even where they are of the view that it does not involve general management or contact with non-party members. Colleagues are reminded that failure to report activity later found to constitute misconduct can itself be grounds for disciplinary action, and can aggravate the seriousness of any misconduct.

h. OPCC employees cannot canvass on behalf of a party or candidate (or a potential candidate) in local, Parliamentary or European elections. "Canvassing" is actively contacting individuals with the intent of securing their support for a candidate or party. Thus a member of staff may, for example, display a poster supporting a candidate or party at their home address or on their car, but they may not do anything that actively seeks to secure support for a party or candidate (or potential candidate). This could include speaking positively to a third party regarding a candidate,

even if that third party were not an ordinary member of the public. Staff may seek to encourage participation in elections in a general sense, but cannot do so in such a way as to appear to support a particular candidate or party. The OPCC therefore seeks to increase public awareness of PCC elections, but does so in collaboration with the Police Area Returning Officer, who is responsible for the administration of the election.

i. OPCC employees are not permitted to speak in public where there is an apparent intention to affect public support for a political party or a candidate. “In public” is not defined. Family and social functions are excluded, but the definition would not merely be limited to what are ostensibly political events. Again, colleagues should seek management advice.

j. OPCC employees are not permitted to publish any written or artistic work whether as author or editor, nor can they authorise or permit another person to publish such work, if the work appears to be intended to affect public support for a political party or candidate. “Speaking in public” and “publishing” includes social media activity, and colleagues are advised to avoid “likes”, “shares”, “retweets” and their equivalents, even where they are using a personal social media profile not ostensibly connected with the OPCC, where the original social media post could be perceived as lending support to a political party or candidate.

k. As is the case for all public sector employees, no resources of the OPCC can be used for party political purposes, such as to support a particular candidate. This includes work email, phones, IT equipment generally (including software), police premises, and printers. There is no exemption for activity that takes place in one’s own time. OPCC employees should not attend political events in work time, except with a manager’s approval (thus, for example, we may participate in party conferences to promote a policy area).

Conclusion

l. A core function of an OPCC is the delivery of the political objectives of a PCC as expressed in the Police and Crime Plan, and legitimised by the public mandate secured by the democratic elections process. Thus delivery of a political mandate is part of our job. However, we are politically restricted because we must be able to fulfil that function for whoever is elected PCC. The public’s confidence in the governance of the police rests on this presumption, and colleagues must act within the limits this requirement creates.