OFFICE OF THE POLICE & CRIME COMMISSIONER
IT, Communications, Internet and Social Media Policy

1. Purpose

1.1 The use of IT, Communications, Internet & Social Media applies to all members of staff including temporary members of staff, those on work experience, consultants, contractors, home workers and volunteers employed or engaged by the OPCC.

1.2 The Policy aims to:

- Set out the parameters of use of the telephone, email and internet permitted by the OPCC;
- Inform you of the monitoring we may undertake of telephone, email and internet use;
- Clarify which type of use may constitute a misuse of the telephone, email and internet;
- Provide guidance on the use of all forms of social media, including Facebook, LinkedIn, Twitter, Wikipedia, all other social networking sites, and all other internet postings, including blogs;
- Inform you of how non-compliance with the Policy will be treated; and
- Protect the OPCCs interests.

2. Principles

2.1 During your contracted hours of work you are required to devote your time and attention to OPCC business and to support its goals and objectives. Therefore, the telephone, email and internet systems are in place for work related matters only.

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

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

2.4 Inappropriate use of the telephone, email or internet may lead to claims against the OPCC 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.

2.5 You are expected to comply with this Policy at all times to protect the OPCC's electronic communications systems and equipment from unauthorised access and harm.

2.6 It is your responsibility to familiarise yourself with the Government Protective Marking guidelines.

2.7 We may take disciplinary action against you if you do not comply with any part of the Policy.

2.8 The examples of prohibited misuse or activities set out in this policy are non-exhaustive.

3 Telephone Use

3.1 You should use the telephone system primarily for your work and in the normal course of the OPCC business and dealing with members of the public. You may make private/personal calls but these should be short, infrequent and (if outgoing) within the UK. Overseas calls are not allowed except for work related purposes. If you feel your private use exceeds this requirement you are able to make a contribution via a payroll deduction for an amount to be agreed based on an agreed usage.

3.2 You may be supplied with a mobile device for work-related purposes. Private use of a supplied mobile is permissible but you must reimburse the OPCC for all private use. Examples of misuse of mobile technology include:

- Private or freelance business;
- Gambling;
- Pornography;
- Chat lines;
- Conducting political activity;
- Sending, forward or replying to offensive or obscene text or other messages or attachments;
- Passing on confidential information about the OPCC or any 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;
- Making or sending hostile, harassing or bullying calls or messages.

4 Postal Mail

4.1 All post, whether marked personal, private or confidential or in any other way will be opened and dealt with by the OPCC in accordance with our normal procedure.

4.2 You must not send out any private correspondence using our letterhead.

4.3 You may sign correspondence, invoices or orders for the OPCC only if you have authorisation and only in accordance with our normal procedures.

5 Email Use

5.1 You should use email, both internally and externally, primarily for your work and in the normal course of OPCC business. The standards 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.

5.2 Email should not be used to transmit information which should be protected by the grading of restricted and above by the Government Protected Marking System for documents.

5.3 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.

5.4 Use of internet for personal purposes is at the OPCC's discretion. A small amount of personal email use is permitted provided that:

- It does not interfere or conflict with business use;
- It is not undertaken during work time;
- The restrictions set out in this policy are adhered to.

Prohibited Uses/Activities

5.5 You must not:

- Send or circulate emails which contain language which is abrupt, inappropriate or abusive;
- Forward unsolicited junk email or other advertising material to others who did not specifically request such material, whether internally or externally;
- Accept or open any file received as an email attachment if you are in any doubt about its source or content;
- Access external personal email accounts;
- Create, transmit, download, print or store software, anything which may cause harassment or alarm or anything which breaches copyright or other intellectual property rights;
- Receive emails from internet sites which you have registered and which are not for business purposes;
- Disseminate information either within or outside the OPCC which you know to be confidential about the OPCC or its staff, customers, suppliers, unless you have the relevant authority to do so;
- Transmit, receive, retain, display, print, forward or otherwise disseminate material which we deem to be offensive, fraudulent, illegal, harassing, discriminatory, offensive, pornographic, obscene or defamatory;
- Deliberately or recklessly disseminate destructive programs such as viruses or self-replicating codes.

6 Internet Use

6.1 The Chief Executive (CEO) will have responsibility for maintaining the standards of our Internet site.

6.2 Any information about the PCC/OPCC that is to be published on the internet should be coordinated by the Head of Communications, in consultation with the CEO.

6.3 Only computers provided by the OPCC or authorised by the CEO may be used to access the internet on the OPCC network. Only approved software may be installed on our computer hardware. No software will be downloaded from the internet without the prior permission of the CEO (and ASC CIM and IT teams).

6.4 Laptops will not contain internet access software unless otherwise agree by the CEO.

6.5 Security of the laptop and the data stored thereon will remain the responsibility of the individual user. Encryption should be utilised whenever material is graded as Confidential or above by the Government Protective Marking Guidelines (advice can be sought from ASC IT dept).

6.6 You should only use the internet for your work in the normal course of our business and serving our stakeholders.

6.7 Use of the internet for personal purposes is at our discretion. A small amount of personal internet use is permitted provided that:

- It does not interfere or conflict with business use;
- Only browsing of the internet is undertaken;
- The activity is not undertaken during work time;
- The restrictions set out in this policy are adhered to.

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

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

Prohibited Uses/Activities

7.0 You must not use OPCC equipment of software to:

- Access private 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 on internet sites to receive regular emails from such sites which are not for business purposes;
- Download software or copyright information from the internet without 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 the PCC/OPCC staff, suppliers or stakeholders unless you have the relevant authority to do so;
- Gamble on the internet;
- Purchase private goods or services;
- View, access, attempt to access, download or upload materials which we deem to be obscene, offensive, harassing, discriminatory, violent or pornographic.

This is not an exhaustive list of prohibited activities.

7 Social Media

7.1 This policy deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, Wikipedia and all other social networking sites, and all other internet postings, including blogs. It 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 the OPCC IT facilities or equipment belonging to you. Further details guidance is included at Appendix A to this policy and should be read alongside this policy.

7.2 Every day, people discuss and debate policing issues in the region in thousands of online conversations. The Office of the Police and Crime Commissioner (PCC) recognises the vital importance of participating in these online conversations and are committed to ensuring that we participate in online social media the right way.

7.3 We encourage all of our staff to explore and engage in social media communities at a level at which they feel comfortable. Contribute, but be smart. The best advice is to approach online worlds in the same way we do the physical one – by using sound judgment and common sense.

7.4 The purpose of this policy is to promote the responsible use of social media and maintain the professional integrity of the PCC.

Prohibited Uses/Activities

7.2 If your duties require you to speak on our behalf in a social media environment you must still seek approval for such communication in general from the CEO, who may require you to undergo training before you do so and impose certain requirements and restrictions with regard to your activities.

7.3 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 logos, brand names, slogans or other trademarks or post any PCC/OPCC confidential or proprietary information without prior written permission;
- Misappropriate or infringe the intellectual property of other companies and individuals;
- Breach our Disciplinary Policy;
- Defame or disparage the PCC/OPCC or affiliates, business partners, suppliers, vendors or other stakeholders or make any communication which (in our opinion) brings us, or them into disrepute or cause harm to the PCC/OPCC 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 parties;
- Breach our Data Protection Policy (eg never disclose personal information about a work colleague on line);
- Comment on sensitive topics related to the OPCC work;
- 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);
- Personal use of social media is never permitted by means of the OPCC computers, networks and other IT resources and communications systems;

- 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.

Monitoring
Telephone calls

7.4 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.

7.5 In 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 the OPCC's 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 Use

7.6 We may monitor your individual email traffic, including the use of certain email addresses. We may limit your access if we consider that you are making excessive or inappropriate use of email for private purposes.

7.7 We have the right to access your email account whilst you are absent eg due to holiday or sickness, or after you have left employment, to check whether any emails are about your work or the OPCC.

7.8 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 or activity which puts the OPCC's interests at 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 Use

7.9 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

7.10 We may monitor your individual social media postings and activities to ensure that our policy is being complied with and for legitimate business purposes and you consent to such monitoring by your use of such resources and systems.

Twitter

7.11 The OPCC has Twitter policies for the following profiles:

- PCC
  http://www.avonandsomerset-pcc.gov.uk/Document-Library/Policies-procedures/Twitter-policy---updated-Jan-2014.pdf
- Custody Visiting and ASB Champion
  http://www.avonandsomerset-pcc.gov.uk/Document-Library/2014/Twitter-policy---Anna-Hill---updated-September-2014.pdf
- Youth Champion
  http://www.avonandsomerset-pcc.gov.uk/Document-Library/Policies-procedures/Twitter-policy---Amy---updated-Jan-2014.pdf

8 Disciplinary Action

8.1 Failure to comply with this policy will normally be considered misconduct under the Disciplinary Policy, although a serious misuse can be treated as Gross Misconduct.

Examples of behaviour which may be treated as Gross Misconduct include but are not limited to:

- Disseminating information either within or outside the OPCC which you know to be confidential about the PCC/OPCC, our staff or our work, unless you have the relevant authority to do so;
- Failure to comply with the Government Protective Marking 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 programs such as viruses or self-replicating codes;
- Posting or disseminating information which you know to be confidential about the OPCC or our staff, stakeholders or suppliers unless you have the relevant authority to do so;
- Gambling on the internet;
- Bring the OPCC or our partners, suppliers, vendors or other stakeholders into disrepute;
- Viewing, accessing, attempting to access, download or upload materials which we deem to be obscene, offensive, harassing, discriminatory, violent or pornographic.

8.2 Any other misuse will be considered under the Disciplinary Policy in the light of the nature and seriousness of the misuse.

Equality and Diversity

The OPCC is committed to the principles of equality and diversity. No member of staff, volunteer and job applicant shall be discriminated against on the grounds of age; disability; gender reassignment; marriage and civil partnerships; pregnancy and maternity; race; religion or belief; sex or sexual orientation.

Policy Statement Information	
Policy Owner (Job Title)	Chief Executive
Date to be Reviewed	March 2020
Date Last Review Completed	
Effective Commencement Date	April 2016

Appendix A
Additional Guidance on use of social media

This guidance forms part of the IT, Communications, Internet and Social Media Policy.

When using social media, all members of staff should follow the guidance set out below.

1. Ensure that your security settings on social media accounts are set to the maximum for personal safety.

2. When posting information on social media sites, both personal and corporate, consider the risks:

    - Personal safety and exploitation of personal information. Avoid providing addresses, phone numbers, email addresses etc.

    - The security of the organisation.

    - Security of information relating to family, friends and other contacts.

    - Indirect reference to your role or the organisation.

    - If you are using a mobile device, consider turning off any GPS / location tracking options within social media apps that identify your location.

3. Staff should not make reference to the OPCC on personal social media accounts, particularly if comments are critical, or ridicule the organisation or other colleagues.

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

5. Any lost phones or computers with the OPCC social media accounts should be reported to IT so that the account can be protected.

6. The administrator of any social media account is responsible for the management of the account's password. The administrator should observe appropriate security levels in relation to these shared account passwords. Administrators should keep details of all staff members with access, and change passwords when team membership changes.

7. 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.

8. If you use third party apps make sure you read the small print before signing up. For example, any photos added to Twitpic are then owned and can be used by Twitpic.

Private use of social networking and video sharing sites

9. All staff are accountable for whatever they put into the public domain even in a privately held account. Inappropriate use or inappropriate disclosure of personal information on social networking and video sharing sites is subject to criminal proceedings (in

accordance with s55 of the Data Protection Act it is a criminal offence to disclose personal information unlawfully) and/or misconduct procedures.

10. Members of staff who use their personal details to contribute to social networking, blogs and video sharing websites should take into consideration the fact they will be placing personal details into the public domain. This may impact on their own privacy, the security of family and friends, and may compromise their vetting status.

11. Users 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.

12. All staff 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.

13. In order to protect our reputation users should not express personal views which may be controversial, derogatory towards colleagues or conflict with organisational views on social media pages.

14. Comments made on personal sites should not reveal confidential information or jeopardise police operational matters.

15. When using private social networking, blogs and video sharing websites, no use may be made of the Avon & Somerset Office of the Police and Crime Commissioner's name, crest or insignia without the express permission of the Chief Executive. Consideration must also be given to any other matters of copyright.

16. When using private networking no use may be made of OPCC photographs or images without the permission of the Chief Executive.

17. No member of staff should send messages about the OPCC without authority to do so.

18. To protect our reputation staff should not set up unofficial or spoof groups, pages or accounts.

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

The corporate use of social networking and video sharing sites

20. All applications for new corporate accounts must be approved by the Chief Executive before they are opened by staff.

21. Any member of staff who wishes to open an account must demonstrate that the account has a purpose to promote the work of the OPCC that they understand their responsibilities in managing the account (highlighted throughout this document) and they have familiarised themselves with the appropriate guidance documents. **N.B**. All applications must be submitted in an email to the Chief Executive.

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.

23. Head of Communications will be responsible for monitoring and supervising the content of the account.

24. 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.

25. Staff 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.

26. All OPCC corporate social networking and video sharing sites will be administered by the Chief Executive.

27. Social media should always be considered as one channel for communication, and should not be used in isolation.

Management of content

28. All social networking, blogs and video sharing sites 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. Head of Communications will be responsible for monitoring the accuracy and relevance of local content.

29. The Chief Executive or one of the SLT will have access to all sites and will be capable of removing inappropriate material. Therefore login account details must be forwarded to the Chief Executive, who will maintain a list of all accounts. Changes to login details and passwords should be notified to the Chief Executive.

30. The Chief Executive or one of the SLT will monitor all corporate social media accounts to ensure that they comply with policy and guidelines, and will issue guidance to staff where appropriate.

31. Any serious complaints, issues, discrepancies or breach of this policy or accompanying guidance with any OPCC accounts will be dealt with by the Chief Executive.

32. All video footage, comments, text and photographs appearing on social networking sites 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 information that would be considered Restricted or above should be posted on the site.

33. It is the responsibility of the member of staff posting photographs or footage to ensure that they comply with legal or data protection requirements and, if necessary, a risk assessment should be carried out.

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

35. Where possible, links back to the main OPCC website should be used to help provide context and background as well as to help drive traffic onto the main site.

36. All pages will clearly display an agreed disclaimer.

37. 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 Head of Communications.

38. Any member of staff 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.

39. Keep records. It is critical that we keep records of our interactions in the online social media space and monitor the activities of those with whom we engage. Because online conversations are often fleeting and immediate, it is important for you to keep track of them when you're officially representing the PCC. Remember that online PCC statements can be held to the same legal standards as traditional media communications. Keep records of any online dialogue pertaining to the PCC and send a copy to the internal email address that you have been provided.