Use of IT, Communications and Social Media

2.17 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.

2.18 The Policy aims to:

- Protect our interests and the reputation of the PCC
- 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

2.19 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.

2.20 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

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

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

2.23 All staff within the OPCC hold politically restricted posts. All use of media and communications must comply with these political restrictions.

2.24 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.

2.25 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 reasonable and limited.

2.26 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

2.27 If your duties require you to speak on behalf of the OPCC you must follow the details of this policy. This policy applies for in person communication as well as using the internet and social media. You may be required to undergo training before you do so and impose certain requirements and restrictions with regard to your activities.

2.28 Any media or social media content for external publication should be reviewed by the Head of Communications. This includes marketing, advertising and press releases, as well as interviews, public presentations, articles for publication and strategies, reports and documents for a public audience (this list is non-exhaustive).

2.29 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 with our normal procedures.

Use of Social Media

2.30 This policy deals with the use of all forms of social media and all internet postings, whether written, audio or video. Examples include, but are not limited to, Facebook, LinkedIn, Instagram, X and WhatsApp. All other internet postings, including blogs, videos and podcasts are also included. 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.

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

You should not refer 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.

2.32 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.

2.33 You should also be aware that the media use social media to gather information and are entitled to report on anything posted.

2.34 You must note that any comments made on social media will be deemed to be in the public domain and, potentially, 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.

2.35 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.

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

2.37 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. If you see content on 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.

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

2.39.2 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.

2.40 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)

2.41 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

2.43 All corporate social media accounts must have their usernames and passwords logged and stored on shared OPCC systems. The Head of Communications is responsible for enforcing this. The Head of Communications also controls staff access to the social platforms. Delegated staff are permitted by the OPCC to manage content on our social channels. This is delegated by the Head of Communications. When a team member leaves their access to social media accounts will be removed. This is the responsibility of the Head of Commmunications.

2.44 All social media accounts must be accurate and reflect the policies, views and opinions of the Police and Crime Commissioner, as well as kept up to date and relevant, with a regular flow of new content to maintain follower interest. Inaccurate posts should be removed or corrected immediately. The Head of Communications is responsible for social content and the quality of the content posted. Referral to the Deputy Chief Executive and Chief Executive should be sought where contentious or high-risk issues arise.

2.45 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 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.

2.46 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 and relevant copyright law.

2.47 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.

Use of the Internet

2.48 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.

2.49 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.

2.50 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.

2.51 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

2.52 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.

2.53 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.

2.54 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

2.55 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

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

2.57 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 follows 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).

2.58 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

2.59 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 may be asked to reimburse the organisation for costs incurred in personal use. Overseas calls are not allowed except for work related purposes.

2.60 You may be supplied with 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.

2.61 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.

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

2.63 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.

2.64 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.

2.65 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.

2.66 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

2.67 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.

2.68 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).

2.69 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.

2.70 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

2.71 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

2.72 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.

2.73 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