Use of IT, Communications, Internet & Social Media Policy

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

Introduction

1. This Use of IT, Communications, Internet & Social Media Policy (the "Policy") applies to all members of staff including temporary members of staff, those on work experience, directors, consultants, contractors, trainees, home-workers, and volunteers ("you", "your") employed or engaged by the OPCC ("us", "we", "our"). It also applies to all members of the Strategic Policing and Crime Board. Third parties who have access to our electronic communication systems and equipment are also required to comply with this policy.

2. The Policy aims to:

    - set out the parameters of use of the telephone, e-mail and internet permitted by us
    - 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 we will treat any non-compliance with the Policy; and
    - protect our interests

General Principles

3. This policy does not form part of any employee's contract of employment and it may be amended at any time. We may also vary any parts of this procedure, including any time limits, as appropriate in any case.

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

5. Staff within OPCC hold politically restricted posts. All use of media and communications must comply with these political restrictions.

6. 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.

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

8. 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.

9. You are expected to comply with this Policy at all times to protect our electronic communications systems and equipment from unauthorised access and harm.

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

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

Telephone Use

12. You should use the telephone system primarily for your work and in the normal course of our business and serving our customers. 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.

13. You may be supplied a mobile phone for work-related purposes. All mobile phones should be switched onto silent/vibrate mode when on open working floors. Private use of a supplied mobile phone is permissible but you must reimburse us for all private use. 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

- Any member of staff working for the OPCC, volunteer for the OPCC, SPCB member or contractor working for the OPCC who is issued with an electronic mobile device by the OPCC or by West Midlands Police must sign a declaration of compliance. This does not apply to laptops because they are covered by a separate declaration, managed by West Midlands Police. The declaration is attached at Annex 2 to this policy.

- 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 messages

Postal Mail

14. All 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.

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

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

Email Use

17. 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.

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

19. 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.

20. Use of the internet for personal purposes is at our 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; and

    - the restrictions set out in this policy are adhered to

Prohibited Uses/Activities

21. 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 other users 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 with 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 us or our staff, customers or 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; or
- deliberately or recklessly disseminate destructive programs such as viruses or self-replicating codes

Internet/Intranet Use

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

23. Any official information about us that is to be published on the internet or intranet should be coordinated by the Chief Executive. Further guidance on the correct use of social media is included at the Annex to this policy. You must ensure that you are familiar with this policy and with the attached guidance.

24. Only computers provided by the OPCC or authorised by the Chief Executive may be used to access the internet or intranet on our 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 Chief Executive.

25. Security of a laptop and the data stored thereon will remain the responsibility of the individual user. Laptops must be used at all times in accordance with the guidance and instructions provided when the laptop was issued, and from time to time thereafter.

This is particularly important with regard to maintaining the security of the laptop and information it contains.

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

27. 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; and
- the restrictions set out in this policy are adhered to

28. If unsuitable material is accidentally accessed on the internet you should immediately report this 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.

29. 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 the IT support desk.

Prohibited Uses / Activities

30. You must not:

- 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 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

This is not an exhaustive list of prohibited activities.

Social Media

31. 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 our IT facilities or equipment belonging to you. Further detailed guidance is included at Appendix B to this policy and should be read alongside the policy.

Prohibited Uses/Activities

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

33. 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
- breach our Disciplinary Policy
- 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)

34. 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.

35. 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.

36. 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

37. 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.

38. 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. 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.

39. 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 Use

40. 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.

41. 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.

42. 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 Use

43. 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

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

Disciplinary Action

45. 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.

46. Examples of behaviour which may be treated as gross misconduct include but are not limited to:

- disseminating information either within or outside the Authority which you know to be confidential about us or 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 programmes such as viruses or self-replicating codes
- 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
- 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

47. Any other misuse (such as those set out elsewhere in this Policy) will be considered under the Disciplinary Policy in the light of the nature and seriousness of the misuse.

Annex One - Additional Guidance on use of social media

This guidance forms part of the IT, Communications and Internet 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 Section 55 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 Office of the Police and Crime Commissioner West Midlands 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 peoples 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. Line managers 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. Line supervisors will be responsible for monitoring the accuracy and relevance of local content.

29. The Chief Executive 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 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 *(see GPMS).*

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 and/or EQIA 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. Official social media users must follow the guidance laid out in the relevant social media guidance document. This is available from the Chief Executive or on the Force Corporate Communications Department intranet site.

38. The Chief Executive may send messages to social media users with directions or instructions. These should be followed by all social media users.

39. 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.

40. 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.

Annex Two

Mobile Devices– Staff Agreement to Compliance with Working Practices

This agreement should be read and signed by all members of the OPCC that have access to a mobile electronic device supplied by the OPCC or WMP Force. This includes smart phones, BlackBerrys, IPADs and other tablets if applicable. The agreement does not include laptops that are covered by another agreement.

1 Mobile Devices - General Guidance

Users must exercise great care when entering their device password in a public place and do not disclose their password to anyone (including IT&D support staff, managers or colleagues). This includes any pin code.

Users must lock their device when not in use.

There must be no sharing of personally issued devices with other internal PCC colleagues or to anyone external of the organisation (This includes: partner agencies and other police force 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 that of a pool device) and all actions carried out upon it. They must not allow any other individual to use their personally issued device for any reason and where pool devices are in operation, users must be named designated users who have also signed this agreement.

The device is approved for the processing of data up to OFFICIAL only. Users must not enter or record information of a classification higher than OFFICIAL into the device, whether in an email message, calendar appointment, memo, task, photograph or any other device application.

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 – it must be locked when not in use and not be left unattended in a public place.

It is easy for somebody standing near a mobile device to view the device's display. Therefore, users should not work on classified or sensitive data while in a public place.

It is particularly important that users exercise great care when entering their device password in a public place. It would be fairly easy for a bystander to learn the password from watching the user type it. Therefore, users must not enter their password into the device if there is any possibility of being overlooked.

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

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. If you are unsure about any of the settings, or what to do in particular situations, please contact the Service Desk on extension 805 3344.

2 Passwords

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. Users must adhere to the WMP Password Policy which can be found here:

http://intranet2/content/B_PRD/Policy_Portal/Policy_Documents/Access_Management.pdf

Users must adhere to the following guidance relating to the choice and use of passwords.

- Do not use the same password for a mobile device as for any other system.
- Never, for any reason, disclose passwords to anyone, whether in person, by phone, or by email.
- 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.

3 Overseas

- 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.
- If using a device overseas, users must consult with Information Security at least 7 days before travel. Users must take extra care to ensure that they cannot be overlooked and take all possible precautions to prevent their device being stolen.

4 Security Incidents

- If a force device has been lost/stolen the user must contact the Help desk immediately on 805 3344 or FCC 0121 626 4040 and request they contact “IT&D Team 10” out of hours to report the incident.

- Users that believe their password has been compromised and have not always been in possession of the device must contact their helpdesk immediately.
- If the users device appears not to be functioning as normal, users must contact the IT&D help desk for further advice.
- If the user's device shows signs of physical tampering, the user must immediately cease use of the device and inform the IT&D help desk.

5 Security Operating Procedures - Form of Undertaking:

This form must be endorsed electronically and an email with the attached form completed and returned to Business Support in the OPCC. By signing below the user confirms the following:

- I have read and understood the OPCC agreement for mobile devices.
- I have received and understood data protection and protective marking training.
- If I suspect that my device has been compromised I will inform my Line Manager or the Security Team as soon as possible in line with force information security incident policy.
- I will inform IT&D Service Desk if and when I no longer need these rights or any equipment which I have been issued.
- I undertake to observe this agreement and to take all reasonable precautions to ensure that I do not breach the security of the OPCC.
- I understand that if I fail to observe this agreement, I may prejudice the OPCC, I may have my user account suspended and/or be liable to disciplinary action or criminal proceedings.

Name: ---------- **Post:** ----------

Signature: ---------- **Date:** ----------