Leicestershire Police

Internet Access and Social Networking Procedure

This procedure supports the following policy:
Social Media Policy

Procedure Owner:	Superintendent
Department Responsible:	Professional Standards
Chief Officer Approval:	Deputy Chief Constable
Protective Marking:	Not Protectively Marked
Date of Next Review:	December 2017

This document has been produced in conjunction with the Leicestershire Police Legislative Compliance Pack

Review log

Date	Minor / Major / No change	Section	Author
Jan 2011	Live		DI Mick Edwards
Oct 2011	Minor	1	DI Mick Edwards
Oct 2013	Minor	All	DS Paul Woods
Apr 2014	Major	All	DS Paul Woods
Dec 2015	None	None	DI Dimmock

Contents

---

1. Internet Provision

1.1 The Chief Constable has permitted, in certain circumstances as defined below, limited use of the Leicestershire Police internet system for personal use. This is a privilege and may be withdrawn at any time.

1.2 Internet provision is automatically provided for each member of the organisation except where that privilege has been withdrawn, for example, where internet access is deemed to be inappropriate and in breach of this procedure.

1.3 The provisions within this procedure apply equally to any access that is conducted via a Force portable computer, laptop, Blackberry or other hand held computer device.

2. Monitoring

2.1 The Organisation will monitor internet use to:

- Prevent or detect crime.
- Ensure compliance with Force policies and procedures.
- Detect and investigate unauthorised use of the internet facility.
- Ensure the effective operation of the internet system.

2.2 Users should have **no expectation of privacy** in respect of their use of internet facilities. The Force utilises technology that scans, records, monitors and logs activity and content of all internet traffic including encrypted (https) sites.

2.3 All internet access is logged, traceable to a specific user and specific computer, and is subject to active monitoring using software monitoring tools.

2.4 Use of the internet service by a user indicates acceptance this procedure.

2.5 Where internet usage is found not to comply with this Procedure, the individual may be subject to withdrawal of internet access and/or disciplinary action or result in the commission of criminal offences. In the first instance violations will be reported to the user's line manager who will assess whether access should be removed. Where the abuse continues or is judged to be exceptional then PSD should be notified.

2.6 Investigative surveillance will only be carried out in line with the:

- Regulation of Investigatory Power Act 2000 Telecommunications (Lawful Business Practice)
- (Interception of Communications) Regulations 2000.

3. Managers Responsibilities

3.1 All managers have a responsibility to ensure the Internet Procedure is conveyed and explained to their staff.

3.2 Where there are concerns regarding a staff member's use of the internet, the line manager must report to the Professional Standards Department and request appropriate monitoring reports.

3.3 Staff must report incidents of inappropriate access or suspected security breaches to their manager. The manager should note details and report to the Professional Standards Department.

4. User Responsibilities

4.1 Staff are permitted to use the internet for a legitimate policing purpose as defined by the Code of Practice for the Management of Police Information:

- Protecting life & property
- Preserving order
- Preventing the commission of offences
- Bringing offenders to justice
- Any duty or responsibility of the police arising from common or statute law

4.2 Individuals may also access the internet for reasonable private use. This will normally take place outside of their official working hours and therefore is in their 'own' time (i.e. meal breaks or outside of work periods).

4.3 Any usage must not exceed one hour per day and providing that, in the Line Managers view, such usage does not affect the users performance in his/her day to day role, and on the understanding that they conform with all Force policies, procedures and standards. Users are advised to log off the browser when they have finished their personal usage.

4.4 Users must take care to ensure that others cannot use their accounts. Staff will be held responsible for all activities logged against their account.

4.5 It is noted that users may wish to conduct internet banking via a Force computer however they are advised to use their home computers as the Force cannot be held responsible for any financial or other loss. Security protocols exist for such sites and the Force systems may not be fully compatible with them.

4.6 As stated in section 2, there is to be **no expectation of privacy** and whilst the monitoring software used is designed NOT to capture passwords, users would be well advised to *expect* that everything done on a force system *is* being recorded and may be viewed by the Anti-Corruption Unit. (this applies to all force systems, not only internet usage).

4.7 Users must not make copies of copyrighted material such as music, onto Force equipment as this will be an infringement of the Copyright, Designs & Patents Act 1988 and unlawful action for which both the user and Force maybe liable.

4.8 Users should be aware that access to web pages identifies the Force therefore, those wishing to covertly access the internet for investigative

work should not do so from a networked computer as it may compromise their operations.

4.9 If a member of staff inadvertently accesses a prohibited area, they must report this to their Line Manager who will note the details and consider notifying the Anti-Corruption Unit within PSD.

4.10 Staff are not permitted to register any Force email address or Leicestershire Police domain in any personal online transactions. However, websites belonging to legitimate, approved service providers e.g. office supplies can be used for work purposes. This does not apply to staff registering with web based accounts in line with the Social Media Policy e.g. an official Facebook account.

5. Prohibited Use

5.1 The Force internet facilities must not be used for any of the following.

- Subscription to, creation, transmission, downloading, browsing, printing or storage of:
  - Any inappropriate, offensive, pornographic, obscene, indecent or adult images, text, data or other material, or any data capable of being turned into inappropriate, offensive, pornographic, obscene, indecent or adult images, text, data or material.
  - Material which is racist, sexist, homophobic, threatening, harassing, bullying, insulting, offensive or discriminatory against an individual or group.
- Sending sensitive Force information to a private or non-police business web-site or email address.
- Disclose any unauthorised personal information.
- Be libellous
- Other business interests not otherwise connected with their role with the Force.
- Engaging in illegal activities
- On-line betting / gambling
- Movement of executables (e.g.*.COM, *.EXE etc). There are 2 categories of executables; mobile code & static downloads. Mobile code is typically downloaded by a web site without the user being aware and can be required for the website to work correctly. Static downloads are usually downloaded on request by the user and are traditionally '.exe' files. Executable code is a potential risk to the Force and therefore users are not permitted to download any, even if this causes a web site to function incorrectly.
- Representing the user's personal opinion as those of the Force.

- All forms of web based email including Hotmail, Yahoo & Gmail etc as activities in this area cannot be sufficiently scanned and may allow the passage of inappropriate material.
- Sites which are designed to circumvent monitoring, or control of access that may attempt to bypass our protective measures.

5.2 The above list is not exhaustive; however, any such unauthorised use may result in disciplinary and/or criminal action.

6. File Downloads

6.1 The ability to download software from the internet is restricted to specific authorised users (normally IT staff) in order to ensure that all such software is properly licensed and checked for viruses prior to loading on to the Force network.

6.2 Software products are often available for free download from the internet. Such software is normally offered as free or shareware. Although offered free, licensing conditions still apply to their use. Requests for downloads of software and other material should be directed to IT via the IT help desk. Such requests will be prioritised below support of business usage.

6.3 Data or information must not be uploaded unless it relates directly to the user and the user only.

6.4 Do not upload any software or code to any site on the internet.

7. Social Networking

7.1 This section is intended to provide guidance in relation to an individual's *personal* use of Social Media. For information regarding the use of Social Networking sites to represent the Force, please see the Social Media Policy.

7.2 When used appropriately online social networking sites can be a great way of finding old friends, sharing information, staying in touch with friends & families and joining interest groups.

7.3 Like any other profession, you have a right to a personal life. Using online social networking sites can be hazardous if confidentiality is breached by Police Officers and Police Staff discussing sensitive or confidential matters online. This could lead to criminal and/or disciplinary action being taken by Leicestershire Police.

7.4 Awareness is required in relation to:-

- **Breach of Trust or confidence**

  Police officers, Police staff and Police forces in general have a legal duty not to disclose information obtained from 3rd parties through the conduct of their official duties. Such information must not therefore be posted on the internet or social media.

  The public would be discouraged from confiding in the police service if they did not have a degree of confidence that information provided in confidence would be respected.

- **Unauthorised Disclosure of personal data**

  Police officers, Police staff and Police forces have access to a significant amount of personal and sensitive data which is protected under the data Protection Act 1998.

  The disclosure of personal data on the internet or social media which was obtained during the course of your duty is likely to amount to a criminal offence.

- **Bringing Discredit on the Police Service**

  Police conduct Regulations 2004 states- Whether on or off duty, Police officers should not behave in a way that is likely to bring discredit upon the Police Service.

  Behaviour by Police Staff, whether during work time or not which is likely to bring discredit on the Police Service may amount to gross misconduct under the terms of the police staff disciplinary codes.

  The expression of views or conduct which appears to support discrimination against any group, or encourages racial, religious or homophobic hatred will not be tolerated.

  Police officers are advised not to make any comment or post any images of behaviour on the internet or social media which are, or could reasonably be perceived to be, beliefs or conduct that are contrary to the expectations of behaviour outlined in Schedule one (code of conduct), regulation 3, Police (conduct) Regulations 2004 which provides *"Whether on or off duty, police officers should not behave in a way which is likely to bring discredit upon the police service".* The same standards are expected from Police Staff.

- **Revealing Personal information**

  Criminals and others may seek to use the internet and social media to identify personal information about police officers and police staff with a view to embarrassing, discrediting, harassing, corrupting or blackmailing them or their families for their own benefit.

Police officers and staff in rural locations, in sensitive posts, with uncommon names, or in high profile posts are particularly vulnerable to such attempts.

It is recommended that you:-

- Remove personal details from the edited electoral role;
- Ensure telephone numbers are ex-directory;
- Opt all family members out of online commercial search facilities such as 192.com
- Ask “Google Maps” to remove pictures of your house, car or persons from their site; http://www.ehow.com/how_5723475_remove-street-photos-google.html
- Register to avoid unwanted telephone calls. http://www.tpsonline.org.uk/ctps/number_type.html
- Register to avoid unwanted mail. http://www.mpsonline.org.uk/mpsr/mps_choosetype.html
- Ensure privacy setting for social media are set to the highest level;
- Do not register on social media using a pnn.police.uk e-mail address;
- Are careful when accepting “friends” to access your social media;
- Are not associated with inappropriate material on “friends” social media;
- Are not associated with social media of criminals;
- Are not associated with social media of persons involved in serious or organised crime;
- Remember that online users may not be who they purport to be;
- Ensure that all computers and mobile devices have up to date security and anti-virus software installed;
- Use strong passwords and never share them;
- Shred all paperwork containing personal details;
- Contact the Anti-Corruption Unit if you become subject of online abuse linked to your occupation, if a “spoof” social media account is established purporting to be used by you, or if a genuine social media account is cloned, hacked or taken over.

7.5 You are advised not to post any of the following information on the internet or social media:-

- Details of your employer
- Details of your post
- Images of uniform
- Mobile telephone numbers
- Home address
- Personal e-mail address
- Family members' details
- Hobbies and places frequented
- Details of vehicles
- Sensitive personal data
- Images or details of colleagues without their consent.

7.6 **Revealing Operational Material or tactics**.

The police service has a duty to prevent and detect crime, prevent disorder and protect the vulnerable. Tactics used by the police service, including covert tactics, must remain matters for the police service if they are to remain effective and serve the interests of the public.

The unauthorised disclosure of operational and tactical information can have serious consequences for public safety, can reduce the effectiveness and efficiency of the police service and is a serious criminal offence.

The Official Secrets Act 1989 provides that, in summary, any police officer or member of police staff is guilty of an offence if without lawful authority they disclose and information, document or other article, the disclosure of which:

- Results in the commission of an offence
- Facilitates an escape from legal custody or the doing of any other act prejudicial to the safekeeping of persons in legal custody
- Impedes the prevention or detection of offences or the apprehension or prosecution of suspected offenders; or
- Such that it's unauthorised disclosure would be likely to have any of those effects.

8. Violations

A failure to comply with this procedure may result in the removal of an individual's right to access the internet for personal use. In more serious cases this may result in disciplinary and/or criminal proceedings.

Appendix A: Examples of Inappropriate Social Media Usage

- An investigating officer for a serious offence receives a “Friend Request” on Facebook from the victim, they innocently accept. The case proceeds to Crown Court. The defence become aware of this and raise the issue of the officer’s impartiality to the court. The officer is required to take the stand and try to convince the judge that this was an innocent mistake.

- An officer posts on Facebook a message regarding their forthcoming Saturday night shift working the City Centre. This includes comments including looking forward to getting into fights. One of their “Friends” realises the damage this could cause to public confidence and reports to PSD.

- A member of the Police Service, clearly very proud of their job, shows themselves as working for Leicestershire Police and their profile picture is of them in uniform on Facebook. They “Like” a comment posted by Nick Griffin (BNP). Again a colleague sees this and reports their concern to PSD.

- An officer clearly identifies themself as a Police Officer on Facebook. They have pictures posted which are viewable to friends of friends. There are several pictures clearly taken on a night out that show the officer to be heavily intoxicated including images of them in a state of undress.

- A film crew are filming inside a Police Station. No one realises that a CIS Intel log is on display on a monitor in the background. A “helpful” colleague from another force advises us via Twitter that by pausing the TV programme, a viewer is able to read the log. Clearly not realising that they have inadvertently disclosed the details on the log to the whole world.

There has been much coverage in the press in relation to officers disciplined for their Social Networking usage. Click each link for the relevant articles:

- The Guardian,
- BBC
- The Telegraph

This article on Facebook demonstrates that once something is on the internet, it is there forever, even if originally posted in error.

In short – Assume that everything you put on a Social Media site *could* well be seen by *anyone*.

Then ask yourself if you are happy for your boss and a journalist to see it, safe in the knowledge that it would not bring discredit to yourself or the force.