

## Using the Internet, Instant Messaging and Social Media

### Contents

---

Policy Statement .....	2
Principles.....	2
Definitions.....	3
Responsibilities .....	4
All employees .....	4
Covert officers and Counter Terrorism Policing North East (CTPNE) staff .....	5
Additional Information.....	7

---

## Policy Statement

---

### Summary

West Yorkshire Police must ensure that employees who access the internet, whether on or off duty, do so appropriately as their behaviour could have an adverse effect on their professional reputation, that of the Force and affect public confidence in the police service.

While everyone is entitled to a private life, this must not be conducted in a way likely to bring discredit on themselves, the Force or the police service as a whole. This relates to the use of social networking and dating sites in particular.

The aims of this policy are to:

- Ensure employees who use the internet are aware of their obligations;
  - Detail what is deemed acceptable and unacceptable internet use;
  - Outline the rules for employees who use any social networking and dating sites in their work and private lives; and
  - Outline what is acceptable to use of download in relation to work devices.
- 

### Scope

This policy applies to all Force personnel, i.e. police officers, police staff, police community support officers, special constables, volunteers, partners and agency staff.

Throughout this document the term 'employee' is used to refer to the above personnel.

---

## Principles

---

### General

West Yorkshire Police will:

- Grant all Force employees access to the internet for purposes associated with police business, e.g. Internet investigations (Cybercrime).
  - With certain limitations, also allow employees to use the internet for personal use.
  - In order to protect the Force network, identify the types of monitoring that the Force will conduct and under what circumstances.
  - Take misconduct, disciplinary and/or criminal action against any employee whose conduct bring discredit on themselves, the Force or the police service as a whole or any breach of this policy.
- 

### Acceptable use

West Yorkshire Police will define acceptable use as:

- Overtly accessing research material, intelligence and other information on the internet for a valid policing purpose relevant to an individual's work.

- Occasional and reasonable use of the internet (browsing) for personal non-work related purposes during an authorised break or before or after working hours. This will be monitored by local line management and audited by Professional Standards Directorate.

Excessive personal internet use will be reported to the employee's line manager which may result in the internet access being withdrawn and/or disciplinary action taken against them.

---

**Unacceptable use**

West Yorkshire Police will define unacceptable use as using force computers or devices to:

- Access a personal social networking or dating account. Use of Force approved social networking accounts, such as NPT Facebook or Twitter accounts, is permissible by authorised personnel.
  - Create, download or transmit (other than for properly authorised and lawful research) data or other material or any data capable of being resolved into:
    - Obscene or indecent images;
    - Defamatory, sexist, racist, offensive or otherwise unlawful images;
    - Material designed to annoy, harass, bully, intimidate, inconvenience or cause needless anxiety to another person; or
    - Material that infringes or breaches copyright.
  - Publish information known to be, or might be considered by others to be, false, inaccurate, libellous, defamatory, pornographic, soliciting, vulgar, obscene, sexist, racist, homophobic, offensive or otherwise unlawful.
  - Conduct private or freelance business for the purpose of profit or commercial gain.
  - Canvas for religious or political purposes.
  - Gamble.
  - Download video or audio for entertainment purposes.
  - If unauthorised, post West Yorkshire Police telephone numbers (landline or mobile), email addresses, official West Yorkshire Police logos or artwork.
  - Present personal opinions as those of the West Yorkshire Police.
  - Spend excessive amounts of time 'surfing the net' (browsing without any real purpose) during work time thereby interfering with an individual's duties. This will be determined by line managers.
  - Subscribe to mailing lists for services which are not connected to West Yorkshire Police business.
  - Knowingly do anything that is illegal under English law or the law of any other relevant country.
- 

## Definitions

---

## General

- ‘Social’, ‘social media’ or ‘social networking’ are the terms commonly used to describe web sites and online tools which allow users to interact with each other in some way by sharing information, opinions, knowledge and interests.
  - The following terms are covered by the content of this policy (note: the below list is not exhaustive):
    - Micro blogging, e.g. Twitter
    - Blogging, e.g. WordPress, Tumblr and Blogger
    - Video sharing, e.g. Flickr, Instagram and YouTube
    - Social bookmarking, e.g. Reddit and StumbleUpon
    - Social sharing, e.g. Facebook
    - Professional sharing, e.g. LinkedIn
- 

## Responsibilities

### All employees

---

#### Dos

All employees are responsible for:

- Completing the e-learning package ‘Use of Police Information and Systems’ and agreeing to the terms of use. This training package is available via [bishopgarth.com](http://bishopgarth.com).
- Registering using their private email address and not their West Yorkshire Police email address, unless for a specific work-related reason or in relation to a police related matter and requires a police email account.
- Carefully considering what information they want to disclose. Some sites allow users to display personal details such as name, address, date of birth, marital status, sexual orientation, occupation, employer and job details etc.
- Being aware that some social networking sites change the default privacy settings making some personal information available to the public. It is good practice to periodically check to see what information associated to individuals and their family is available for all to see.
- Referring to the Information Security intranet page for more information on how to protect their personal information on line.

In addition, West Yorkshire Police recommends that all employees always consider setting up their user accounts with the highest possible privacy settings.

---

#### Don'ts

All employees are responsible for:

- **Not posting** any material either on work devices or personal mobile devices which:

- Includes details or images of West Yorkshire Police operational activities or case or work related issues.
- Includes pictures or images of scenes or property/evidence.
- Identifies non-public areas of West Yorkshire Police premises or other members of the Force.
- **Not** making contact through their personal social media or apps to any complainant, suspect or witness that they have met through their professional work, for any reason. Any approach by one of these parties to an officer/staff member's personal account must be reported to their line manager and no correspondence be entered into with the other party.
- **Not posting** on or using any end-to-end encrypted applications, such as WhatsApp, Signal, Telegram, Snapchat or Instagram, in relation to operational policing matters. This includes not putting anything onto these applications in relation to police activity that would be in breach of data protection and information management policies. This includes the following, but is not an exhaustive list:
  - Names, addresses, pictures of any nominals;
  - Pictures or location of scenes.

Arranging people to come into work to cover shifts or work overtime is permitted as long as it does not contain any operational policing information.
- **Not downloading** high volume media for personal use, such as videos, music, live recordings as this impacts on the performance of the network and could slow down the network performance required for operational purposes.
- **Not downloading** any end-to-end encrypted applications onto work devices, such as WhatsApp, Signal, Telegram, Snapchat or Instagram, unless authorised by the Force.

The only exceptions would be those employees who:

- Manage a website on behalf of West Yorkshire Police in compliance with the Force Web and Social Media Sites policy.
- Perform a role where they feature in, e.g. news bulletins, radio broadcasts or press conferences etc. which means they are identified as working for West Yorkshire Police.

---

## Covert Officers and Counter Terrorism Policing North East (CTPNE) Staff

---

### Don'ts

Covert officers and Counter Terrorism Policing North East (CTPNE) staff are responsible for:

- **Not posting** any material which identifies them as being:
  - Employed by CTPNE or West Yorkshire Police.
  - Involved in the counter terrorism network or covert policing.

- Engaged in anyway in counter terrorism or law enforcement activities.
-

## Additional Information

---

### Compliance

This policy complies with the following legislation, policy and guidance:

- APP Professional Standards
  - Information and Technology Usage policy
  - Whistleblowing policy
  - Force Web and Social Media Sites policy
  - Internet Intelligence and Investigations policy
  - Data Protection Act 2018
- 

### Further Information

Further guidance in relation to this policy can be sought from Professional Standards Directorate.

---