POLICY

INSTANT MESSAGING POLICY

Policy owners	Director of ICT
Policy holder	Director of ICT
Author	James Nobbs

Approved by

Legal Services	N/A
Policy owner	12 September 2017
JJNCC	7 September 2017

Note: *By signing the above you are authorising the policy for publication and are accepting responsibility for the policy on behalf of the Chief Constables.*

Publication date	12 September 2017
Review date	12 September 2020
APP Checked	Yes
College of Policing Code of Ethics	Yes

Note: *Please send the original Policy with both signatures on it to the Norfolk CPU for the audit trail.*

Index

Legal Basis

(Please list below the relevant legislation which is the legal basis for this policy). You must update this list with changes in legislation that are relevant to this policy and hyperlink directly to the legislation.

Legislation/Law specific to the subject of this policy document

Section	***Act (title and year)***

Other legislation/law which you must check this document against (required by law)

Act (title and year)
Human Rights Act 1998 (in particular A.14 – Prohibition of discrimination)
Equality Act 2010
Crime and Disorder Act 1998
Health and Safety at Work etc. Act 1974 and associated Regulations
General Data Protection Regulation (GDPR) and Data Protection Act 2018
Freedom Of Information Act 2000
The Civil Contingencies Act 2004
Computer Misuse Act 1990
Official Secrets Act 1989
Management of the Police Information (MOPI)

Other Related Documents

- Mobile Device Policy
- Provision of ICT Equipment Policy
- College of Policing Code of Ethics
- Standards of Professional Behaviour for Officers and Staff

1. Introduction

1.1 Norfolk and Suffolk Constabularies have established a policy to provide clear standards and guidelines to police officers and staff regarding the use of Skype for Business, Blackberry Messenger Enterprise (BBM) and other instant messaging services.

1.2 The aims of this policy are to:

- Explain the appropriate use of instant messaging as a communication tool;
- Set out the responsibilities of all staff when sending and receiving instant messages, voice to voice calls or video conferencing;
- Outline how to contact partner agencies and other forces externally.

1.3 This policy applies to all police officers, special constables, police staff and police support volunteers.

1.4 Where the term ‘employee’ is used in this policy, it refers to all of those that fall within the above categories.

2. Background

2.1 The introduction of instant messaging (IM) services across the Norfolk and Suffolk Constabularies is intended to facilitate business-related communication, the sharing of corporate information and to enable internal users to communicate directly with each other using IM, voice-to-voice calls or video conferencing.

2.2 It is important to highlight that these services are not intended to replace traditional email but rather supplement the communication tools available to staff.

3. Monitoring

3.1 Both Constabularies will monitor the use of these services to ensure that they are being used for a valid policing or business purpose. The services should not be used for personal or social use.

3.2 All messages sent by IM services are logged and searchable for audit purposes.

3.3 Real-time ‘presence’ information is available on a number of services, including Skype for Business. The presence status is designed to enable a more productive working environment whereby users are fully aware if colleagues are available for contact

3.4 Presence is not an indication of time spent working and is not intended as a performance monitoring tool.

3.5 Information Management and Professional Standards are jointly responsible for auditing and ensuring all Constabulary ICT systems and data are only used in accordance with Force procedures.

4. User Responsibility

4.1 Employees are responsible for their own actions in relation to the use of IM services and should be aware that stored conversations can be disclosed:

- At court;
- As part of a Freedom of Information request;
- As part of a Data Protection request;
- As part of disciplinary or misconduct proceedings.

4.2 Employees should report any communication they receive which contains inappropriate content to the Professional Standards department.

4.3 IM services do not have an inbuilt protective marking facility meaning the software should only be used for content that is not protectively marked.

4.4 Staff must demonstrate awareness of their surroundings when discussing information of a personal or sensitive nature (e.g. investigative techniques, or investigations). This specifically applies when communicating via telecommunication services, IM (voice or video) calls, or any other devices while working away from Norfolk or Suffolk Constabulary premises.

4.5 Officers and staff should ensure that their IM status (if the software allows this feature) accurately reflects their availability. Users should not state they are offline, busy or in a meeting if they are available to answer queries or correspond with colleagues. Additionally, the application must not be closed (or otherwise configured) to prevent presence status visibility.

5. Unacceptable use

- Use of Constabulary communication systems to set up personal businesses or send chain letters;
- Forwarding of confidential Constabulary messages to external locations;
- Distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal;

- Distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist.

- Breaking into the Constabularies' or another organisation's system, or unauthorised use of a password/mailbox;

- Broadcasting unsolicited personal views on social, political, religious or other non-business related matters;

- Transmitting unsolicited commercial or advertising material;

- Undertaking deliberate activities that waste staff effort or networked resources;

- Introducing any form of computer virus or malware into the corporate network.

5.1 Employees should report any communications they receive which contain inappropriate content to the Professional Standards department.

6. Breach of Policy

6.1 Where it is believed that an employee has failed to comply with this policy they may face disciplinary proceedings.

6.2 Any breaches will be assessed by PSD and, where appropriate, will be dealt with under the relevant misconduct regulations.