Police, Fire and Crime Commissioner for Essex

Use of Communications Policy

Version Control	Version 5.0	April 2020
Reviewed By	D Horsman	February 2019
Policy owner	P Brent-Isherwood	April 2020
First Published	J Drewett	January 2013
Next Review Date	D Horsman	April 2023

Version history

Version Number	Date	Reason for review	Comments
1.0	January 2013		First publication
2.0	February 2016	Update by J Klimkowski (Communications Manager)	
3.0	September 2017	Minor amendments by D Horsman (AD Communications and Public Engagement)	
4.0	February 2019	Scheduled review date	Amended to reflect change of governance model from PCC to PFCC. Reviewed alongside EP's policy to ensure consistency. New section added regarding remote working and mobile computing devices.
5.0	April 2020	Review by the Monitoring Officer	Managers' responsibilities in respect of staff leavers added. Reference added to relevant data protection legislation and Government Security Classifications. References to associated policies and procedures added where necessary.

1.0 About this Policy

This policy applies to persons granted use of the office of Police, Fire and Crime Commissioner for Essex's (PFCC's) and Essex Police's communication systems, including the PFCC, all permanent and temporary staff, agency staff, contractors and volunteers. It describes the specific user standards relating to the following:

- Internet access and usage;
- Email usage;
- Telephone systems including mobile telephones, and
- Remote working and mobile computing devices.

2.0 Risk Assessments / Health and Safety Considerations

No risks or health and safety considerations have been identified.

3.0 Policy

3.1 Internet Access

There will be **one, standard** level of access allowing access to most websites. A filter will be applied preventing access to inappropriate websites, for example those containing pornography, facilitating gambling etc.

3.2 Internet Usage

Whilst staff can on occasion use the internet for personal use, this should be during break periods.

All users will be expected to maintain a professional image when using any PFCC or Essex Police provided internet facility and must not compromise the high standards of the organisation or take any action likely to damage public perception of the organisation.

In particular they must not use any PFCC or Essex Police provided internet facility to obtain, store, access or use any material considered to:

- Contain pornographic material;
- Provide online gambling or gaming services;
- Breach discrimination laws or any PFCC policies or procedures, or
- Contain any offensive material.

In the event that a user inadvertently accesses or receives material outlined above they should immediately inform their line manager and

the Essex Police IT Service Desk to enable the problem to be looked into.

Users are not permitted to download, copy or distribute items of software, freeware, videos or games without the prior approval of the Essex Police IT (Information Technology) Department.

Subscription to any bulletin board, newsgroup, website or blog is not permitted other than for a work related purpose.

3.3 Email Usage

All users are reminded of the need to keep their use of email to a minimum as required by their role. It is primarily a business tool which is not meant to replace other, sometimes more appropriate, forms of communication such as formal business correspondence, face to face meetings or telephone conversations.

Emails must be treated in exactly the same manner as any other written correspondence and should observe the same degree of formality depending upon the intended recipient. Users should be aware that the contents of any email may be legally binding upon the organisation and should take care not to include any material they would not confidently say in any letter, or which they would not be prepared to release if required under relevant data protection legislation. Any email containing sensitive material should be appropriately protectively marked, in line with the Government Security Classifications. Email users should check the distribution list of any email carefully before sending it, in order to ensure that information is not sent to any individual not entitled or required to receive it.

The email system must never be used to create or send any material or other information which might be considered as offensive, hostile, harassing, intimidating or disruptive or which contains any form of profanity or undermines the professional and ethical standards of the PFCC.

In particular the email facility must not be used to forward any chain letters or junk mail. Any contravention of this procedure may lead to the email facility being withdrawn and / or disciplinary action being taken.

If an email is received contrary to the above then the recipient should immediately inform their supervisor or manager who should take all reasonable steps to identify the source of the material and to prevent further transmission.

Users will be allocated a standard size mailbox which should be checked on a regular basis (at least twice per day). Users should regularly maintain the contents of their mailbox to ensure the memory limit allocated is not exceeded. Should this occur, users will receive an

automated message informing them that they have exceeded the memory limit and providing additional guidance on how best to manage the content.

The Essex Police IT Department will ensure that all emails sent outside the PFCC or Essex Police will have a suitable disclaimer attached.

Authorisation for non-employees to use the email system must be granted by Essex Police Information Security. Essex Police form A343 (External Electronic Access to Essex Police Information) must be completed by an employee of the PFCC and sent to Information Security, who will (if appropriate) authorise the IT Department to create an account.

3.3.1 Email Account Access by Others

Generally the email account holder will be the only individual permitted access to an email account. However, where there is a genuine operational or business need, access to additional personnel will be granted.

To obtain additional access an email will need to be forwarded to the Essex Police IT Service Desk, authorised by a manager or the Chief Executive and Monitoring Officer, stating the reason(s) access is required. The account holder will receive notification that their email account is to be accessed by others, giving full details. The only exception to this will be where the initial access relates to an internal investigation and the notification would lead to the officer being alerted to the existence of that investigation.

The following specifies the correct level of authority for the most common types of access:

- Creation of an 'out of office' message – self authorised;
- Creation of an auto forward facility – Chief Executive and Monitoring Officer;
- To forward any read or unread email – Chief Executive and Monitoring Officer;
- To allow the mailbox to appear in another user's Outlook account – Chief Executive Monitoring Officer (and only in exceptional circumstances).

There may be occasions where an email has been incorrectly sent to a recipient and the sender has good reasons to require the email to be deleted. The sender should contact a manger explaining the reasons why deletion is necessary. Essex Police's IT Service Desk will only access an email account to delete the email on the authorisation of the manager. This measure is designed to stop a person who may deliberately have sent an inappropriate email arranging the deletion of that email from the recipient's email account in order to avoid detection.

3.4 Mobile Telephones

Mobile telephones may be issued to permanent, temporary or agency staff members for use with, or in connection with, the performance of their role on behalf of the PFCC.

On occasion, staff are permitted to use allocated mobile telephones to make calls and to send text messages which are of a personal or private nature provided it is of a reasonable level. However, the expectation is that personal calls are made on personal, non-work phones. Under no circumstances is an allocated mobile telephone to be used to convey any visual or audible message which could be considered to be offensive, obscene or menacing.

3.5 Remote Working and Mobile Computing Devices

Remote working (i.e. accessing Police information using a portable device) must be formally authorised by the Chief Executive and Monitoring Officer and must only be undertaken using corporately owned equipment. Such equipment will be provided by the Essex Police IT Department only, and will ensure approved and security accredited methods of remote access to the corporate networks.

Users must make their own assessments of their working environments to ensure that they are appropriately secure. This includes ensuring that the information they are processing cannot be overlooked, and that physical security measures are correct for the classification level of the information concerned.

Mobile devices (i.e. any device which can be used remotely to access police information) should be physically protected against theft, especially when left or operated in high-risk areas, such as vehicles, conference centres and hotel rooms. The use of security cables and lockable containers can help reduce the risks. Access tokens, such as smartcards, must never be stored with the computer.

Users must have received a formal briefing on the additional risks and security measures, and have signed written security operating procedures, from the person issuing / authorising the access before being issued with mobile devices.

Mobile devices must be connected to the network regularly (preferably, at least once a week) to ensure that they receive the latest software updates and that valuable information is backed up.

Mobile devices must not be taken or operated outside of the United Kingdom without written permission from the Chief Executive and Monitoring Officer. Users are also advised to notify Information Security and to check local laws - in particular, the rules for importing and

exporting encrypted media – before taking mobile devices issued by the PFCC or Essex Police outside of the UK.

4.0 Monitoring and Review

This policy will be reviewed by or on behalf of the Chief Executive and Monitoring Officer within three years of the date of publication, or sooner if required by changes in legislation, regulations or best practice.

Any communications made using the PFCC's or Essex Police's equipment may be monitored for any of the following purposes:

- To investigate or detect potential breaches of this policy;
- To prevent or detect crime, and / or
- For training or quality control purposes.

Where the monitoring of communications relates to any purpose other than training or maintaining the quality of communications originating from the Police, Fire and Crime Commissioner's office, and / or where monitoring activity is likely to result in the obtaining of confidential material or material which is the subject of legal privilege, written authority to intercept, monitor or record communications will be required from the Chief Executive and Monitoring Officer to the Police, Fire and Crime Commissioner.

It is the responsibility of all line managers to ensure that the Essex Police IT Department is notified of all staff leaving the employment of the PFCC, in order to ensure that associated accounts are disabled, and to ensure the recovery of all information and communications technology allocated to the leaver at the end of their contract.

5.0 Related Procedures

Government Security Classifications
Correspondence Standards
Ethics and Integrity Framework
Information Management Protocol between the PFCC and the PFCCFRA
Information Sharing Agreement between Essex Police and the Police, Fire and Crime Commissioner
Privacy Notice (global)
Employee Privacy Notice
Volunteer Privacy Notice

6.0 Related Policies

Access to Information Policy
Data Protection Policy
Staff Code of Conduct

7.0 Information Sources

Comparable Essex Police policies