



<b>POLICY</b>	<b>Issue: 1.0</b>
<b>Corporate Email Policy</b>	<b>Date: 06/08/2009</b>

## Policy Statement

This policy sets out the principles that apply to Civil Nuclear Constabulary (the Constabulary) employees when using the Civil Nuclear Police Authority's (the Authority) email systems and integrated instant messaging systems and must be read in conjunction with the Information Security Policy

- 1.1 Only the Authority provided email systems are to be used for sending and receiving business email. This also ensures that all outgoing email carries a standard disclaimer/copyright statement and incoming email is scanned for viruses.
- 1.2 The Authority's email systems is primarily intended for authorised business in accordance with the supporting procedure CNC/PP/0428 Use of Corporate Email Systems. With the approval of your line manager or supervisor you may make occasional and reasonable personal use of the email system provided such use is not excessive, complies with the standards set out in the referred procedure and does not have an adverse effect on job performance or the Constabulary's business.
- 1.3 Any reported infringement of this policy or underlying procedures will be investigated initially through supervisor or other appropriate authority and action will be taken where individuals breach the policy.
- 1.4 All emails and instant messages may be monitored and subject to electronic or manual scrutiny by the Professional Standards Department and subject to regular audit by the Constabulary IT & Communications (CNC IT & C) department.
- 1.5 Users must report any security incidents or suspected security weaknesses to the CNC Security Manager (SyM) using form CNC/CD/0477.
- 1.6 Email messages, sent or received in the course of our business transactions, become a part of our corporate declared records and must be retained for as long as they are needed for our organisational requirements in accordance with the Records Management Policy.

The CNPA as employer reserves the right in all circumstances to disclose any information obtained in pursuance of or in breach of this policy to a third party for the purpose of pursuing a criminal investigation and or criminal proceedings.

<b>Document Reference</b>	<b>CNC/POL/20.2</b>	<b>Page 1 of 2</b>
Uncontrolled when printed unless subject to controlled issue Refer to Index of Policies for current version		

## Aims of the Policy

- 2.1 To provide employees and interested parties with clear and concise policy guidance to demonstrate management commitment and support for information security.
- 2.2 To ensure the Confidentiality, Integrity and Availability of Authority and Constabulary information in the support of operational and administrative work.

This policy is enacted by the following management system documents:

Document Reference	Title
CNC/SEC/01	Security Manual. (all sections).
CNC/POL/2.3.4	Information Security Policy.
CNC/POL/20.5	Acceptable Use of IT Policy.
CNC/POL/5.3	Records Management Policy.
CNC/PP/0428	Use of Corporate Email Systems Procedure.
CNC/CD/0477	Breach of Security / Security Weakness Form

<b>Document Reference</b>	<b>CNC/POL/20.2</b>	<b>Page 2 of 2</b>
Uncontrolled when printed unless subject to controlled issue Refer to Index of Policies for current version		