



POLICY	Issue: 2.0
Acceptable Use of IT	Date: 12/08/2009

Policy Statement

To ensure that the Civil Nuclear Police Authority (the Authority)'s Information Technology (IT) infrastructure remains stable and secure, the IT infrastructure needs to be used by Civil Nuclear Constabulary (the Constabulary) officers and staff within corporately agreed standards.

The standards also apply to all equipment designed for the storage of, or access to, information, known as computing equipment. This includes Personal Computers (PCs), laptops, Personal Digital Assistants (PDAs) and associated peripherals (such as removable memory devices (cards / sticks), floppy disk drives, compact disks (CDROMs), printers, scanners, modems) and other such media.

All computing equipment is the property of the Authority, and its use must adhere to these defined standards. The Constabulary IT & Communications Department has the right to remove any hardware or software that contravenes this policy and underlying procedures.

Access to the Authority's IT infrastructure is provided to users on the basis that:

- information, data and systems may only be used by authorised individuals to accomplish tasks related to their appointments;
- use of the information and systems for personal gain, personal business, or to commit a criminal offence is prohibited;
- information that is classified as 'Protect' or above must be protected, and must not be disclosed without authorisation; and
- unauthorised access, manipulation, disclosure or secondary release of information that is classified as 'Protect' or above constitutes a security breach, which will trigger a security investigation and may lead to disciplinary action.

Any failure to adhere to this policy may be grounds for disciplinary action up to and including termination of employment.

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.

Document Reference	CNC/POL/20.5	Page 1 of 3
Uncontrolled when printed unless subject to controlled issue Refer to Index of Policies for current version		

The following constitute unacceptable use of the IT infrastructure:

- to access sites that are or might be considered to be indecent, offensive (e.g. display material that uses racist/sexist terminology or contain nudity), pornographic, obscene, racist or illegal. The only exception to this is the authorised investigation of suspected criminal or misconduct activity which, as part of the investigation, requires access to such material; or
- to undertake activities that you know or should know will or could affect the performance of, damage or overload the network systems or hardware; or
- to download screensavers, wallpaper, video clips, games, utilities, image and sound files, patches or updates, unless you are authorised to do so by the Head of the IT & Communications Department; or
- to download or install unofficial or unauthorised software; or
- to encourage or promote activities which make unproductive use of your time e.g. surfing sites that have no relevance to your legitimate business need; or
- to engage in activities outside the scope of your responsibilities e.g. ordering goods for which you have no authority; or
- to engage in activities that might be defamatory or incur liability on the part of the Authority / Constabulary or adversely impact on its image; or
- to introduce packet sniffing or password detecting software; or
- to access social, real-time, chat rooms; or
- to install or access any internet based messaging service, such as MSN Messenger, unless you are authorised to do so by the Head of the IT & Communications Department; or
- to gamble online; or
- to knowingly attempt to access or download data which you know or ought to know to be 'Confidential' (Data Protection Act 1984); or
- to enter sites where access has been blocked or seek to gain access to restricted areas/information on the network; or
- to attempt to remotely access the network systems using non-official/unauthorised equipment, by way of a trapdoor program or other method, or to otherwise attempt to breach or circumvent firewalls or other security systems;

Aims of the Policy

- to safeguard the integrity of computers, networks, and data;
- to ensure that all users understand their responsibilities under this policy and associated policies and procedures;
- to protect the Authority / Constabulary against damaging legal consequences.

Document Reference	CNC/POL/20.5	Page 2 of 3
Uncontrolled when printed unless subject to controlled issue Refer to Index of Policies for current version		

This policy is enacted by the following management system documents:

Document Reference	Title
CNC/POL/2.3.4	Information Security Policy
CNC/CD/0524	CNC Misconduct Regulations
CNC/POL/20.2	Corporate Email Policy
CNC/POL/20.3	Internet Usage Policy
CNC/POL/20.4	Software Licence Compliance

Document Reference	CNC/POL/20.5	Page 3 of 3
Uncontrolled when printed unless subject to controlled issue Refer to Index of Policies for current version		