



<b>POLICY</b>	<b>Issue: 1.0</b>
<b>Airwave Communication System</b>	<b>Date: 11/06/2008</b>

## Policy Statement

The Airwave Communication System provides a secure and resilient method of, ensuring that policing communications in the Civil Nuclear Constabulary (the Constabulary) can take place without fear of compromise by terrorists, criminals, the media or the public. As well as a radio, it provides alternative ways of communicating including, telephone, data, text and status updating

The Constabulary is committed to making best use of its resources by taking full advantage of the technology provided. In order to do this and to safeguard security it will ensure that:

- Only trusted persons have access to the Airwave terminals.
- Such persons receive the required training in the use of Airwave.
- Take care is to ensure that persons not entitled to be privy to Airwave communications, cannot hear communications emanating from Constabulary terminals.
- Users are aware of their security responsibilities and data protection.

It is a mandatory requirement of the Constabulary's connection to Airwave that users comply with the Constabulary's security policies. The Constabulary will ensure this by:

- Ensuring the physical security of Airwave terminals, ensuring storage within secure buildings or vehicles which are lockable, treating the terminals as RESTRICTED items.
- Instructing that hand held Airwave terminals are not left unattended (in vehicles or premises) and are locked away securely when not in use. Vehicles fitted with terminals should always be locked when not attended.

The Constabulary Airwaves Operations Manager will:

- Ensure adequate physical security of all centrally stored Airwave terminals.
- Maintain an asset management database register of each Airwave terminal and ancillary equipment at BCU/Departmental level.
- Retain the master unlock code in the event that users lock themselves out of their Airwave terminals.

<b>Document Reference</b>	<b>CNC/POL/19.1</b>	<b>Page 1 of 2</b>
Uncontrolled when printed unless subject to controlled issue Refer to Index of Policies for current version		

- Conduct a regular audit (at least annually) of all Airwave terminals and ancillary equipment.
- Ensure that all procedures outlined in the UK Police Forces Codes of Practice and Code of Connection are adhered to by authorised users.
- Conduct inspections to ensure terminal Custodians are meeting their responsibilities.
- Report the loss of Airwave terminals and software upgrade devices to O2 Airwave, NPIA and the accreditation panel and International Standards Organisation (ISO) in a timely manner.
- Arrange the repair of Terminals and software upgrade devices at an appropriate secure facility.
- Investigate and report incident where tamper seals on terminals have been broken.
- Liaise between the service provider, the manufacturers, the accreditation panel, National police Improvement Agency (NPIA) and the Constabulary.

### **Aims of the Policy**

To ensure the secure use, handling and storage of Airwave terminals and equipment by trained and authorised users. To record and track the use, repair and upgrade of Airwave terminals, so that the Constabulary can be confident that it's communication systems can be operated without being compromised.

This policy is enacted by the following management system documents:

CNC Airwave Procedures Manual

<b>Document Reference</b>	<b>CNC/POL/19.1</b>	<b>Page 2 of 2</b>
Uncontrolled when printed unless subject to controlled issue Refer to Index of Policies for current version		