

# Police Working with CCTV Monitoring Centres

|                               |                   |
|-------------------------------|-------------------|
| <i>Authorisation</i>          | Police User Group |
| <i>Signed version held by</i> |                   |

© NPIA (National Policing Improvement Agency) 2007

All rights reserved. No part of this publication may be reproduced, modified, amended, stored in any retrieval system or transmitted, in any form or by any means, without the prior written permission of the National Policing Improvement Agency or its representative.

For additional copies, or to enquire about the content of the document, please contact Marketing and Communications on 0208 200 3231 or [jacquie.fowler@npia.pnn.police.uk](mailto:jacquie.fowler@npia.pnn.police.uk)

For copyright specific enquiries, please telephone the NPIA National Police Library on 01256 602650.

## Table of Contents

|   |           |
|---|-----------|
| <b>Controlling documents .....</b>                      | <b>3</b>  |
| <b>1 Purpose of Document &amp; Target Audience.....</b> | <b>4</b>  |
| <b>2 General Local Authority Use of Airwave.....</b>    | <b>4</b>  |
| <b>3 CCTV .....</b>                                     | <b>5</b>  |
| <b>4 Licensing .....</b>                                | <b>6</b>  |
| <b>5 Confidentiality Agreements .....</b>               | <b>7</b>  |
| <b>6 Cipher Keys.....</b>                               | <b>7</b>  |
| <b>7 Vetting.....</b>                                   | <b>8</b>  |
| <b>8 Physical Security of Equipment.....</b>            | <b>8</b>  |
| <b>9 Physical Security of Monitoring Centres.....</b>   | <b>8</b>  |
| <b>10 Security Checks .....</b>                         | <b>8</b>  |
| <b>11 Operational Talk Group Access .....</b>           | <b>8</b>  |
| <b>12 Traffic on Operational Group .....</b>            | <b>9</b>  |
| <b>13 Risk Assessments .....</b>                        | <b>9</b>  |
| <b>14 Control page .....</b>                            | <b>10</b> |

## Controlling documents

This section will contain reference to any source material used in the preparation of the document. This should include reference to relevant standards or guides.

| Description   | Document number | Revision              |
|---|-----------------|-----------------------|
| Airwave Lead Group on Sharers, CCTV Sub Group Report. |                 | V. 1.1 (January 2007) |
|   |                 |                       |
|   |                 |                       |

## **1 Purpose of Document & Target Audience**

The purpose of this document is to set out the Code of Practice for interoperability between Police and Local Authorities, with particular reference to Local Authority managed CCTV monitoring centres.

Of all aspects of sharers' access to Airwave the specific issues relating to Local Authority access are the most complex and potentially emotive. Statutory provisions relating to the establishment of Crime and Disorder Reduction Partnerships impose a clear mandate for the sharing of information between the Police and their Local Authority partners, while at the same time other statutory provisions relating to data protection and the management of police information seem to impose a requirement not to do so.

Particular attention must be paid to the operation of CCTV monitoring centres by Local Authority staff. Nobody can refute the enormous benefits that CCTV can bring to Police work, but it is true that the implementation of CCTV schemes across the country has shown no consistency of form. In some cases the monitoring centres are managed by Police staff; in others by employees of the Local Authority. A similar lack of consistency applies to methods of communication between Local Authority CCTV monitoring centres and the Police. In some cases contact is restricted to the telephone, whereas in others the CCTV centre has a Police Airwave radio, and can communicate directly with patrolling officers and the Police Control Room.

It is acknowledged that working practices have evolved in a number of areas where the sharing of Police communications with Local Authority CCTV monitoring centres are integral to effective Policing. These forces will argue their case with fervour, whereas other forces will totally disagree. The purpose of this paper is to steer a middle course, offering mechanisms whereby those forces with a requirement to interoperate with Local Authority CCTV schemes using common operational talk groups can continue to do so, but with safeguards in place that will satisfy those who seek to restrict the sharing of operational information.

The proposed security arrangements for the sharing of operational groups are divided into categories of Mandatory and Recommended. It should be stressed that these relate solely to those forces that wish to operate in this way. There is no compulsion on those that wish to operate without direct radio access to accord this facility, which will always remain at the discretion of the individual Police force.

## **2 General Local Authority Use of Airwave**

There is no mandate for proscription by the Police of the general use of Airwave by Local Authority users. Provided the LA is an approved sharer, and is in possession of a TEA2 licence, it should be largely self-governing in this regard, as should be the case for all sharers within the "statutory responders" category.

The LA will have its own range of talk groups for use for the day to day management of its own affairs. There will rarely be any need for LA Airwave users of these talk groups to have contact with a Police Control Room, and any deployment or other "dispatcher" functionality will be managed within the LA (possibly from within the CCTV monitoring centre).

Individual Police Forces may elect to make available specific talk groups to facilitate interoperability with their LA partners, particularly in the case of Local Authority wardens or "constabularies". These may be included in the fleetmap fill for the LA terminals, and may include the Police Sharers Hailing Group for that force, and Airwave Solutions Ltd provided interoperability groups (e.g. MAMAs and O2IAT). Other than in the case of CCTV however, there is little or no justification or requirement for Police operational talk groups to be made permanently available to these users. In the event that interoperability is required it will be possible to patch one of the permitted groups to an operational one, for the duration of a specific operation.

It is always open to a Police force to include a LA talk group within their CCI port allocation, to enable a patch to be established between a Police group and one regularly operated by the sharer organisation. It is acknowledged that current restrictions on the capacity of CCI ports mean that this situation is likely to be the exception rather than the norm.

Code of Connection considerations for these LA users will be managed wholly by the sharer organisation, in accordance with their requirements under the TEA2 licensing regime. This will include the vetting of personnel, which, as no access is to be accorded to Police operational talk groups, need only be to the BC or equivalent level required by the Airwave Accreditor. There is no requirement for Police involvement in this process other than in cases where the LA asks for the Police to carry out the vetting process on their behalf.

### **3 CCTV**

These basic principles may also be applied to LA CCTV monitoring centres, in those cases where the operators are not given access to operational Police talk groups. There are a number of such installations where contact is restricted to telephone, or to a dedicated radio talk group, which is then patched to an operational talk group if the need should arise. This process reflects that recommended in the initial guidance of the National Interoperability and Interworking Group.

Whilst this should still be regarded as optimal procedure it is recognised that many Police Forces have already granted access to operational talk groups to LA CCTV monitoring staff, and that their working practices would make a withdrawal of this facility difficult if operational efficiency is to be maintained. It is therefore necessary to issue recommendations and requirements to govern such access, in order to preserve the security of Police communications over the Airwave network.

Police radio communications frequently involve the transmission of sensitive and personal information, and those over Airwave may

legitimately be expected to be of RESTRICTED level. It is therefore incumbent upon a Police Force fully to risk assess the implications of allowing third parties access to this information, and to impose additional security requirements on those organisations.

These requirements must encompass confidentiality agreements, personnel vetting standards, the physical security of both the terminal equipment and the rooms in which they are operated, the number of operational Police talk groups that the terminals should be enabled to receive, and the nature of the traffic carried on them.

## **4 Licensing**

The LA must be individually recognised by OFCOM as an Airwave sharer, and be in possession of its own TEA2 Licence (Mandatory). Loan arrangements undertaken either informally or under the guise of the so-called Airwave Extension Service offend against European regulations in respect both of procurement and competition. Forces must therefore terminate any such arrangements as soon as it is practicably possible to do so. The loan of radio terminal equipment to approved sharer organisations (including those generically approved) is in breach of contract, save only in the permitted exception of Land Search and Rescue organisations.

There are two legitimate contractual routes that a sharer organisation may pursue in order to obtain access to the Airwave Service, Airwave Direct and Airwave Access.

Under Airwave Direct customers procure what is in effect a cradle to the grave managed service from O2, who supply terminal equipment and fleetmapping services. This may generally be considered to be the simplest mechanism by which a sharer may gain access to the Airwave Network. Nothing within contractual arrangements precludes a Police force from making a financial contribution to a sharer organisation to facilitate their acquisition of services under Airwave Direct.

Airwave Access is a more complex solution, where customers procure service on the network from O2, and then make their own arrangements to procure and manage terminal equipment, and perform their own fleetmapping. It would be open to a Police force to assist a sharer in this regard, by providing them with terminal equipment (title in which would transfer to the sharer organisation, and a new ISSI be assigned), and also offering them fleetmapping services and maintenance arrangements. Such arrangements would have to be carefully negotiated to ensure that there is no possibility of repeating the errors of Airwave Extension and turning the Police force into an effective re-seller of Airwave. This is prohibited by the contract.

In the event that radio terminal equipment is supplied to a Local Authority CCTV centre under Airwave Access arrangements by a Police Force, the radio will have an ISSI, supplied by Airwave that is clearly identifiable as not being part of the normal Police radio terminal range. This will also

NOT PROTECTIVELY MARKED

make the separation of cipher key allocation (see Section 6 below) easier to achieve.

## **5 Confidentiality Agreements**

Information passed over Police radio systems is likely to be of a RESTRICTED nature, and must be subject to strict confidentiality. In order to be satisfied that this confidentiality will be preserved any LA employed CCTV monitoring personnel must enter into an agreement that they will treat information heard on Police talk groups with strict confidentiality (Mandatory). This agreement should encompass the Official Secrets Act (Recommended).

## **6 Cipher Keys**

In preparation for the introduction of Over the Air Re-keying and increased security levels on the Airwave system, all Police talk groups have been allocated cipher keys; the Common Cipher Key, the Police Interoperability Key, or the Police Only Key. The Police user community has determined that the cipher keys will be used in such a way that, once OTAR is delivered, all radio terminals with an ISSI allocated from the Police range will have the ability to use either of the Police cipher keys, in addition to the Common Cipher Key.

The Police Only Cipher Key must not be installed in radio terminal equipment not under the full time control of Police users.

Forces must therefore ensure that any talk groups intended to be shared with CCTV (or any other user organisation) are set to the Common Cipher Key or the Police Interoperability Cipher Key only.

(Note: Standing advice is that the Police Only Cipher Key should be issued sparingly for use only on Specialist internal talk groups.)

In the case of operational Police talk groups shared with CCTV monitoring centres the groups should operate using the Police Interoperability GCK (Mandatory) and only those terminals installed in the CCTV monitoring centres be allowed to have that key installed. In the case of additional groups allocated for event management the allocation of the CCK will be sufficient. Any terminal equipment used by Local Authorities outside the CCTV monitoring centre must only be capable of receiving talk groups using the Common Cipher Key.

In the event that a Local Authority contracts out its CCTV operation to a third party organisation, that organisation may be permitted access to the Police Interoperability Cipher Key on terminals within the CCTV monitoring centre. The contractor organisation must be recognised as an Airwave Sharer, and have its own TEA2 licence for this concession to apply.

## **7 Vetting**

Vetting requirements for third parties having access to operational information should, of necessity, be more stringent than those normally employed in the case of LA staff. Staff employed in CCTV rooms with access to operational Police talk groups, and their managers, should be vetted to full NPPV standard (Mandatory) or such higher standard (e.g. SC) as the force dictates.

In the interest of consistency Police Officers and Staff employed in such rooms should also be vetted to this level.

## **8 Physical Security of Equipment**

Radio terminals which can access operational Police talk groups should not be capable of being easily removed from the CCTV monitoring centre. To this end the terminals should be desk mounted vehicle sets (Fixed Mobiles), firmly secured to prevent their removal (Mandatory). Terminal equipment should also be protected by PIN code access (Mandatory). PIN codes must be different from any used generically by the local Police Force. (Mandatory).

## **9 Physical Security of Monitoring Centres**

CCTV monitoring rooms should have restricted access arrangements, to prevent entry by staff not vetted to NPPV level (Mandatory). In the event that the room is not staffed continuously the key to the room should be held securely in an area that is staffed continuously (Mandatory). Personnel not vetted to NPPV standard may be admitted to the room for short periods under the supervision of a staff member with the required clearance, if this is essential (e.g. cleaners/maintenance staff).

## **10 Security Checks**

Police personnel shall be allowed access to CCTV monitoring centres at any time without notice, in order to check that security requirements are met (Mandatory).

## **11 Operational Talk Group Access**

LA CCTV monitoring centres may be permitted to access one designated operational Police talk group for each Police area that the scheme covers. In addition to this a further operational talk group may be provided in respect of each area, to act as a back up in the event that the primary group is required for the management of a critical incident, and regular traffic is moved to this secondary group.

At the discretion of individual Chief Constables terminals in CCTV monitoring centres may be permitted access to a number of secondary Event Management groups, to facilitate the monitoring of non critical events and operations, together with groups used for the management of local occasions, such as carnivals or football matches. No restriction is proposed in relation to permitting access to talk groups used non-operationally, and protected by the Common Cipher Key, such access being granted entirely on the basis of local discretion.

The over-arching principle behind allowing talk group access to LA CCTV monitoring centres is not to over-provide the facility. The Police Service must have a set of groups readily available to both operational and Control Room personnel that are not accessible by LA CCTV monitoring centres.

## **12 Traffic on Operational Group**

Optimally any operational groups to which LA CCTV schemes are permitted access should not be used to transmit sensitive information. Group traffic should, as far as possible, not contain personal information, the results of PNC checks, or local intelligence reports pertaining to individuals (Recommended). It is acknowledged that some forces may not wish to restrict traffic to this extent, but it still constitutes Best Practice, where access to operational groups is allowed.

## **13 Risk Assessments**

In every case where access to operational Police talk groups is permitted to a LA CCTV monitoring centre it shall be the responsibility of the Chief Officer of Police for the area to cause a Risk Assessment to be carried out. Separate assessments shall be conducted in the case of each of the following:

Requirement to accord access to an operational Police talk group;

Requirement to transmit personal information on the talk group;

Justification for use of the talk group for the transmission of PNC checks/results;

Justification for use of the talk group for the transmission of local intelligence information.

The Risk Assessment for each group must contain confirmation from the individual force's Information Security Officer that allowing access has been considered in the light of the force's requirements under the Data Protection Act and Management of Police Information under the Police Act, and has been deemed legitimate (Mandatory).

In all cases the risk assessments shall be made available for inspection by the Airwave Police Systems Accrerator (Mandatory) and may be submitted to him for consideration before access to the talk group is allowed to the LA (Recommended).

## 14 Control page

### Distribution list

| Recipient | Title | Location |
|-----------|-------|----------|
|           |       |          |

### Change control

| Version | Date | Authority | Evidence of approval | Record of change |
|---------|------|-----------|----------------------|------------------|
|         |      |           |                      |                  |
|         |      |           |                      |                  |
|         |      |           |                      |                  |

NOT PROTECTIVELY MARKED

File name

NOT PROTECTIVELY MARKED

Page 11 of 11