Closed Circuit Television (CCTV) Management and Operations Manual

(Adopted as Policy by the Shire of Plantagenet on 8 February 2011)

CCTV Management and Operations Manual/Policy

Note: Original documentation prepared by Chris Cubbage, Director & Principal Consultant *BSc(Sec)Hons, GAICD, AdvDip BusMgt, Dip CrimInv, Dip Pol*
Amlec House Pty Ltd.
for Office of Crime Prevention, Western Australian Police.

CONTENTS

1. CCTV POLICY SUMMARY

POLICY NUMBER & REFERENCE:	
CCTV SYSTEM OWNER & OPERATOR:	Shire of Plantagenet
REPORTING BODY:	CHIEF EXECUTIVE OFFICER (CEO)
ADOPTED BY COUNCIL:	
DATE/ COUNCIL MINUTES REF:	
REPLACES POLICY:	
CCTV OPERATION REPORTS/AUDITS:	
POLICY AMENDED / REVIEWED:	
CCTV SYSTEM SUMMARY:	
*WA POLICE BLUE IRIS REF:	

*Blue Iris – a register of WA based CCTV systems aimed at mapping the locations of CCTV systems that can be used by police investigators.

DISTRIBUTION OF COPIES

REVISION No.	COPY FOR	QUANTITY	ISSUED TO	DATE

COUNCIL AUTHORISED OFFICERS

Chief Executive Officer	Manager Works and Services
Deputy Chief Executive Officer	Manager Community Services
Manager Development Services	Manager Library and Information Services
Principal Building Surveyor	

2. FOREWORD

The public perception of CCTV systems in Australia is maturing and concerns of privacy have dissipated over the recognised safety advantages afforded by public space CCTV. It is the responsible and appropriate management of the CCTV system and recorded footage which is the primary focus for public attention and scrutiny.

The CCTV Operation should be recognised as a significant and contributing asset to the Shire of Plantagenet. The broad application of the CCTV Operation in Local Government Management is widely evident and should be acknowledged for its contribution to a range of local and state government activities. There is an inherent but often hidden value which is difficult to document and measure in real dollar terms, however each local government should continue to seek out measurable returns on investment as CCTV Operations develop.

The development of the CCTV Management and Operation Manual is to provide a functional means of managing CCTV in accordance with the WA CCTV Guidelines and related publications, legislation and standards. The Manual is designed to form the basis on which to align strategic and operational functions. Importantly, the manual will provide a ready reference for any issue pertaining to the CCTV system's management, operations, technical specifications and functionality.

3. TERMS and DEFINITIONS

'Authorised Personnel' means any delegated officers of the Shire of Plantagenet and WA Police Commissioner.

'CCTV' or Closed Circuit Television is defined as a television system that transmits images on a 'closed loop' basis, where images are only available to those directly connected to the transmission system. The transmission of closed circuit television images may involve the use of coaxial cable, fibre-optic cable, telephone lines, infra-red and radio transmission systems. A hand held camera is not included in this definition unless it is connected to the Shire of Plantagenet's CCTV transmission system or operated as a covert camera.

'CCTV Operations' means all aspects of public space CCTV surveillance management, use, recording, maintenance and access to recorded material.

'Covert or mobile camera' is a camera without a designated, fixed location and is used either to record activity covertly or for short periods of time in a target area. Covert or mobile cameras operated by the Shire of Plantagenet for the purpose of detecting criminal offences or behaviour will be considered to form part of CCTV Operations and will be managed and operated in accordance with this Manual.

'Designated Surveillance Operation Area' means any room or record relating to CCTV Operations, CCTV hardware, control software administration and where access to recorded material may be gained or available.

'Public place' refers to public reserves, public roads or streets, public bridges, with the addition of public transport and car parks, public wharfs, public baths or swimming pools.

'Private premises' refers any area not openly accessible to the general public, including semi public spaces and includes private residences and private or commercial businesses.

'Situation of concern' means a situation which may lead to a breach of Statute Law, where it appears that a person(s) may be in physical distress, or a situation likely to cause a public disturbance.

'Situation of interest' means any situation which may verify area activity or potentially escalate to a situation of concern.

'Stakeholder' means any organisation or group who has a reasonable and justified interest in aspects of public space CCTV surveillance management, use, recording, maintenance and access to recorded material

'Surveillance Officer' means the delegated officer in charge of CCTV Operation, nominated under Authorised Personnel.

4. CCTV POLICY STATEMENTS

4.1. OWNERSHIP AND CONTROL OF CCTV OPERATIONS

The CCTV Operation is owned by and is the sole property of the Shire of Plantagenet;

The Shire of Plantagenet will conduct CCTV Operations in accordance with approved CCTV Management Practices and Authorised Personnel will abide by the Code of Conduct, provide in this Manual.

The Shire of Plantagenet Surveillance Officer has delegated control over the CCTV Operation.

This Shire of Plantagenet CCTV Policy establishes the purpose, key functions, and control parameters set by the Shire of Plantagenet, in order to achieve the following:

1. Maintain best practice and standards with reference to the Western Australian CCTV Guidelines, available at www.crimeprevention.wa.gov.au.
2. Manage CCTV Operations in compliance with Australian Standards 4802:2006, Parts 1 – 4, and future or superseding standards.
3. Manage CCTV Operations in compliance with Commonwealth and Western Australia legislation and amendments which may affect the use of CCTV and recorded material. The relevant and primary areas of compliance are privacy laws, camera field's of view and recording parameters, data storage, access control, and freedom of information provisions.
4. Operate, use and maintain CCTV Operations in accordance with the Code of Conduct, acknowledged and signed every two years by Authorised Personnel in accordance with the Council's Policy review practices.
5. Operate, use and maintain CCTV Operations to maintain effective oversight of Monitoring, Review, Auditing and Reporting.

4.2. ROLE AND PURPOSE OF CCTV OPERATIONS

The Shire of Plantagenet conducts CCTV Operations in order to:

1. Deter, detect and respond to criminal offences and anti social activities against person or property;
2. Facilitate and support an effective response by Shire of Plantagenet Authorised Personnel, WA Police Officers or other emergency services personnel to situations of concern or interest; and
3. Manage and maintain community safety for residents, traders, retailers, workers, visitors and Shire of Plantagenet staff.

4.3. ORGANISATION POLICY FOR CCTV OPERATIONS

This Shire of Plantagenet CCTV Policy provides for the manner in which the CCTV Operation will be operated, managed and the reporting protocols to the Shire of Plantagenet's CEO and WA Police.

CCTV Management Practices will ensure CCTV Operations will be conducted in accordance to the following policy statements:

1. The CCTV System will be operated within applicable law, and for the ethical and beneficial purposes for which it is established or which are subsequently agreed in accordance with these approved policy statements.
2. The CCTV System will be operated with due regard to the privacy and civil liberties of individual members of the public, including the rights to freedom of religious and political expression and assembly.
3. The public interest in CCTV Operations will be recognised by ensuring the security and integrity of recorded material.
4. All Stakeholders and Authorised Personnel will act in accordance with the CCTV Code of Conduct.
5. Access to Designated Surveillance Areas will be restricted to Authorised Personnel or with written authorisation from the CEO.
6. The Shire of Plantagenet will be accountable to its Stakeholders for the effective management and control of CCTV Operations.
7. CCTV Operations will be monitored and evaluated to verify compliance key performance indicators.
8. The Shire of Plantagenet will make public reports in relation to CCTV Operations.
9. Recorded material released to Stakeholders shall be verified for accuracy, relevance and must not exceed that necessary to fulfil the purposes of the written request.
10. The retention of, and access to any recorded material will be only for the purposes provided by CCTV Policy.
11. Recorded material will be retained for 31 days unless otherwise specified or required in relation to an approved police operation or the investigation of crime or events for court or formal review proceedings by the Shire of Plantagenet. Recorded material, hard copy or electronic will then be erased, deleted or destroyed, with released material destroyed following written confirmation on the original release request.
12. Contact and exchange of information between the Shire of Plantagenet and WA Police will be conducted in accordance with a signed Memorandum of Understanding (MOU).
13. Legitimate access may be allowed to live CCTV images which may be required by Council personnel to view public areas for convenient public area familiarisation or reviewing, monitoring or verifying Shire of Plantagenet maintenance services and public works.

14. Access to CCTV Operations should remain with existing Authorised Personnel of Council allowed to access the system.
15. CCTV Operations will make all reasonable attempts to serve the interests of all who may be affected by public space surveillance with a focus on community safety and crime prevention, and not be confined to the interests of the Shire of Plantagenet or operational needs of the WA Police.

5. CODE OF CONDUCT

THIS CODE OF CONDUCT HAS BEEN DEVELOPED TO ENSURE THAT THE HIGHEST ETHICAL STANDARDS ARE MAINTAINED BY ALL AUTHORISED PERSONNEL WHO WORK AT THE SHIRE OF PLANTAGENET AND WITHIN THE CCTV OPERATION.

NON COMPLIANCE WITH CODE OF CONDUCT

CCTV Operations require high standards of integrity and honesty. As a consequence, any breach of this Code of Conduct could result in disciplinary action, up to and including dismissal and criminal proceedings.

ETHICAL USE OF CCTV SYSTEMS AND RECORDED MATERIAL

The Shire of Plantagenet has the highest expectation of all Authorised Personnel to:

- At all times, act in an honest and legal manner to carry out duties which reflects community values.
- Treat all live and recorded images in an ethical manner and with the utmost of care, respect and dignity.
- Interact with WA Police and stakeholders in a timely, courteous and cooperative manner.

CONFIDENTIALITY

The Shire of Plantagenet expects Authorised Personnel to ensure confidentiality of information gathered by or from CCTV Operations by not disclosing or discussing any events with unauthorised personnel or associates who have no direct responsibility relating to CCTV Operations.

In addition, Authorised Personnel will explicitly not identify any involved person or party with family, friends, or acquaintances and will not disclose any information to third parties, including the media without prior written approval in accordance with this CCTV Policy.

OPERATING CONDITIONS

In recognition of CCTV Operation environments and Designated Surveillance Areas, Authorised Personnel will carry out duties in a calm, noise free manner, and will leave areas clean, neat and tidy.

Other than Authorised Personnel, written authorisation is required from the Surveillance Officer, for visitors to enter designated surveillance areas.

Written reports documenting the recording or reporting of situations of concern, will take place as soon as practicable. Reports must be written in simple, non-offensive English that will not cause offence or embarrassment should the record be made public or subpoenaed.

In the course of carrying out duties, CCTV Operations must not be used for personal benefit or invade individual or group privacy. Cameras should only be used in accordance with Section 4.2 of this manual and have priority for when there is an operational necessity or a reasonable belief that an offence has or is likely to occur.

Recorded material shall only be released when requested in writing on an approved application and authorisation by the CEO.

Recorded Material shall not be copied or taken from Designated Surveillance Areas without an approved written application and authorisation by the CEO.

CCTV Operational records (hard copy or electronic) can only be destroyed with written authorisation by the CEO and in accordance with approved CCTV Operating Procedures.

REPORTING A BREACH OF THE CODE OF CONDUCT

Should any person become aware that an officer of the Shire of Plantagenet's work behaviour is or was inappropriate, and the incident has not been dealt with through normal supervisory procedures, then the person is obliged to report the incident to CEO. In return, the CEO will guarantee that any reported matters will be handled with sensitivity and without repercussion.

I have read and understood the CCTV Operation's Code of Conduct and agree to abide by these conditions and implications for any breach.

Chief Executive Officer

SIGNATURE:..... DATE: 29 SEP 2011

Deputy Chief Executive Officer

SIGNATURE:..... DATE: 29/9/11

Manager Development Services

SIGNATURE:..... DATE: 29.9.11

Principal Building Surveyor

SIGNATURE:..... DATE: 29-9-11

Manager Works and Services

SIGNATURE:..... DATE: 30/9/11

Manager Community Services

SIGNATURE:..... DATE: 29/9/2011

Manager Library and Information Services

SIGNATURE:..... DATE: 05·10·2011

6. CCTV MANAGEMENT PRACTICES

6.1. INTRODUCTION

CCTV Management Practices establish the operational objectives and performance indicators for CCTV Operations, with a focus on nominated outcomes relevant to camera locations and other defined target areas. Each of the key Stakeholder relationships should be defined, with a focus on WA Police. Management protocols and guidelines are supported by the Code of Conduct and a MOU.

CCTV Management requires continued commitment for the monitoring, review and audit process, in addition to planning and finance procedures, relating to the CCTV Operations. Executive oversight and CCTV Management should constantly seek out areas for improvement for increased system efficacy.

6.2. KEY PERFORMANCE INDICATORS

Establishing clear and concise Key Performance Indicators (KPIs) for CCTV Operations will allow effective reporting and monitoring of system efficacy and quickly highlight trends concerning fundamental operations, which may require early intervention or closer monitoring by CCTV Management and the CEO.

Recommended CCTV Operation KPIs are to include the following:

1. Possible versus Actual Surveillance Hours conducted.
2. Number of Incidents detected.
3. Number of Incidents responded to.
4. Number of requests/applications for recorded material.
5. Time frame for responding to applications for recorded material.
6. Number of requests for maintenance or system repair.
7. Time frame for maintenance repair and response.

6.3. OPERATIONAL OBJECTIVES

The objectives established for CCTV Operations should be based on measurable criteria, which may include:

- Reducing Reported Crime and Incidents to Police
- Reducing Reported damage and graffiti to the Shire of Plantagenet
- Improving perceptions of safety and reducing fear of crime following community consultations.

Targets should be realistic and able to be monitored over a specified term, such as 12 months, supported by longer term 5 year plans.

6.4. WESTERN AUSTRALIA GUIDELINES

Western Australian guidelines relating to CCTV Operations should be read in association with this CCTV Manual include:

- WA State CCTV Guidelines
- WA CCTV Technical Advice
- WA CCTV Analogue to Digital CCTV System Migration Guidelines
- WA Planning Commission Designing Out Crime Guidelines.

6.5. AUSTRALIAN STANDARDS

Standards Australia's CCTV standards cover the latest CCTV technologies, procedures and are reported to be the most up to date CCTV standards available in the world In Australia, best practice CCTV Operation guidelines may refer to the following:

- AS 4806.1–2006–Closed circuit television (CCTV)–Part 1: Management and operation.
- AS 4806.2–2006–Closed circuit television (CCTV)–Part 2: Application guidelines.
- AS 4806.3–2006–Closed circuit television (CCTV)–Part 3: PAL signal timings and levels.
- AS 4806.4–2008–Closed circuit television (CCTV)–Part 4: Remote video.
- AS/NZS 1158:2005 Lighting for Roads and Public Spaces.
- AS 2201.1:2007 Security Installations;
- AS/ACIF S009:2008 Cabling Provider Rules;
- AS/NZS 1768:2007 Lightning protection.
- ISO 31000:2009 Risk Management (Supersedes AS/NZ 4360:2004)
- HB 167: 2004 Security Risk Management Handbook.
- AS 2342:1992 Development, testing and implementation of information and safety symbols and symbolic signs.
- AS2416:2002 Provides examples and the display of multiple hazard signage.

6.6. RELEVENT LEGISLATION

CCTV Operations with be conducted in accordance with Commonwealth and State Legislative requirements, which includes:

Commonwealth

Privacy Act 1988	Establishes and regulates privacy principles for individuals, corporate entities and personal information.
Surveillance Devices Act 2004	Regulates use of optical surveillance devices without warrant

Western Australia

Criminal Investigation Act 2006	Provides powers for the investigation and prevention of offences and for related matters.
Occupational Safety and Health Act 1984	Regulates the protection of persons at or near workplaces from risks to health and safety
Surveillance Devices Act 1998	Regulates use, installation and maintenance of optical surveillance devices
Security and Related Activities Act 1996	Regulates WA Security Providers
Security and Related Activities Regulations 1997	Regulates WA Security Providers

6.7. ACCOUNTABILITY

The Shire of Plantagenet is responsible for ensuring that CCTV Operations will be reviewed every five years subject to evaluation to identify whether its purposes are being complied with and whether objectives are being achieved.

Resources committed to CCTV Operations will include the cost of independent evaluations and public disclosure provisions.

Evaluation of CCTV Operations will include, as a minimum:

a) Assessment of its impact upon crime;

b) Assessment of its impact on neighbouring areas;

c) Assessment on its impact on improving perceptions of safety and reducing 'Fear of Crime' by members of the public.

d) The views of the public on the operation of the CCTV program;

e) Compliance with the Code of Conduct, protocols and standard operating procedures; and

f) Whether the purposes for which the CCTV Operation was established still exist.

The results of evaluations will be considered for future management and functioning of CCTV Operations.

6.8. BREACHES OF THE CODE OF CONDUCT

This CCTV Manual has been established to address the interests of all who may be affected by public CCTV surveillance and will not be confined to the interests of the Shire of Plantagenet.

Prime responsibility for ensuring the Code of Conduct is adhered to rests with the Shire of Plantagenet. This responsibility includes ensuring that breaches of the Code are investigated and remedied to the extent that breaches of the Code are within the ambit of Shire of Plantagenet power to remedy.

Complaints in relation to any aspect of CCTV Operations must be made in writing to:

The CEO, Shire of Plantagenet, PO Box 48, Mount Barker WA 6324

Shire of Plantagenet will cooperate with the investigation of any compliant about the Shire of Plantagenet CCTV Operations conducted by W.A. Police or Crime and Corruption Commission.

6.9. MANAGEMENT FRAMEWORK

The Shire of Plantagenet has implemented a management framework, namely the CEO with oversight responsibilities for CCTV Operations. The CEO will maintain a management overview of CCTV Operations with reference to CCTV Policy and Procedures, comprising of this manual.

6.10. COMMUNITY SAFETY AND CRIME PREVENTION PLANNING AND CCTV OPERATIONS

The CCTV Operation should be acknowledged in strategic crime prevention planning with a focus on monitoring priority crimes, providing key statistics on crime prevention initiatives and integrating system design, such as camera placement and acknowledging existing camera positions, with specific crime prevention approaches or initiatives.

6.11. KEY ROLES AND RESPONSIBILITIES

In developing this CCTV Manual, the discrete roles and responsibilities of the CCTV system owner, Surveillance Officer, Authorised Personnel and the police are explicit. The responsibilities of each include the following:

6.11.1. SHIRE OF PLANTAGENET RESPONSIBILITY

The Shire of Plantagenet is responsible for the following key functions:

a) a Local Crime Prevention Plan which incorporates CCTV strategies

b) appointing a Surveillance Officer to manage the implementation and operation of CCTV

c) implementing a comprehensive consultative program with business groups, individuals, government instrumentalities and organisations, and cultural/community groups affected by the program

d) implementing a community information program

e) financing the implementation and ongoing costs of CCTV. This includes an independent evaluation of its effectiveness

f) developing, implementing and monitoring the auditing procedures

g) developing and implementing an effective complaints handling mechanism

h) monitoring the effectiveness of CCTV as part of a crime prevention strategy

i) selecting appropriately qualified consultants/contractors to install CCTV

j) providing inductions and training to staff involved in operating and working with the CCTV program

k) ensuring that all relevant parties comply with the Code of Practice, Protocols and Standard Operating Procedures

6.11.2. WA POLICE RESPONSIBILITY

The WA Police is not responsible for funding or for the operation of the Shire of Plantagenet's CCTV Operation. Police involvement will only be to the level that its resources and priorities allow and will be determined by the local Officer in Charge. However, the WA Police should be consulted and involved in all phases of the process leading to the installation and operation of a scheme, including participation on or acting in an advisory capacity to conducting a crime assessment and determining evaluation procedures

These Standard Operating Procedures set out clearly the guidelines and protocols for communication with the police and the provisions in place for an adequate and appropriate police response to reported incidents. This would include the early identification of emerging incidents to facilitate the timely initiation of police response.

The WA Police will be responsible for:

a) providing information for and advice on the crime assessment
b) developing, in consultation with the Shire of Plantagenet the Protocols and Standard Operating Procedures between police and the Shire of Plantagenet in relation to their respective roles in accordance with the MOU.
c) training local police in their responsibilities in relation to the CCTV Operation as set out in the MOU
d) ensuring police officers comply with the Code of Conduct and in accordance with the MOU
e) participating in the evaluation and monitoring processes for the CCTV Operation
f) determining the appropriate level and priority of responses required to incidents identified by the CCTV cameras, according to available resources and existing priorities.

6.12. SURVEILLANCE OFFICER/CEO

The role and duties of the Surveillance Officer/CEO include:

a) Act upon any Delegated Authority to ensure Council's Policies and requirements of relevant statutes are exercised and complied with. Report to the CEO on the requirement in respect of possible litigation or other legal action.

b) Report to the CEO on any significant need for CCTV System modifications or procedures, where appropriate.

c) Regularly liaise with the WA Police in respect to recorded incidents, requests for recorded material, crime statistics, general trouble spots and other relevant matters to ensure the activities of the CCTV Operation complement Police priorities.

d) Liaise with business and community group representatives to ensure their security needs are addressed and catered for whenever possible.

e) Take an active part in improving the effectiveness of the community safety and crime prevention planning in terms of CCTV Operations.

f) Implement CCTV surveillance strategies to problem areas.

g) Review this CCTV Manual in respect to the needs of the Shire of Plantagenet and recommend changes when necessary.

h) Keep abreast of CCTV technology, practices and all introduced amendments to related legislation and where necessary introduce changes to maintain operational and legislative compliance.

i) Monitor incident reports for correct completion in respect to names, addresses, vehicle descriptions if applicable etc.

j) Act under delegated authority in conjunction with the release and destruction of recorded material after assessing the evidence available and the circumstances of the matter.

k) Ensuring compliance with the CCTV Code of Conduct.

l) Act under delegated authority to allow visitors to access Designated Surveillance Areas when considered appropriate or necessary.

m) Ensure CCTV related complaints, correspondence and reports are effectively investigated, prepared and completed within required time frames.

n) Ensure that Authorised Personnel perform at a high level through the development, training and management of CCTV Operations.

o) Represent and promote CCTV Operations and the interests of the Shire of Plantagenet when required to attend various meetings, public forums or as a member of an advisory group.

p) Foster a high standard of public relations in support of CCTV Operations.

6.13. MONITORING, REVIEW and AUDIT REPORTS and PROTOCOLS

6.13.1. REVIEW AND REPORTING

A report should be prepared every five years to provide information on the operation and performance of the CCTV system. Except where there is a legitimate reason for non-disclosure or where restricted or classified by a government agency, this report should be a public document and should be made available by the Shire of Plantagenet.

The report to the CEO should include the following:

a) Achievement of Strategic Objectives and learning outcomes.

b) Acceptance of KPI's and recommendations.

c) The number and type of incidents reported.

d) CCTV System faults, types and recommendations.

e) Evaluate trends or spikes of activity throughout the years and set targets for review.

f) Annual System real dollar value and projected depreciation.

CCTV System Reports should be written with a view of being released to the public on the Shire of Plantagenet website. The topics covered within the report should include details of the following:

a) A description of the system and the geographical area(s) of operation.

b) The system's policy statement.

c) The purpose and scope of the system.

d) Any changes to the operation or management of the CCTV system.

e) Any changes that have been made to the policy.

f) Any proposals to expand or reduce the operation of the system.

g) Details of the CCTV Operation's achievements. The assessment of the system's performance should include an assessment of the CCTV system's impact on crime levels and types of crime in the area covered by the system.

h) The aims and objectives for the next five years.

i) The amount and type of data that has been stored, and whether this amount is excessive in terms of likely need.

j) The amount and type of data that has been destroyed, and whether the data has been destroyed in accordance with privacy and other compliance criteria.

6.13.2. INDEPENDENT CCTV OPERATION AUDITS

In accordance with AS4806.1:2006 Part 3.4 where CCTV Systems operate within the public domain, consideration should be given to an independent audit. An independent CCTV Operation Audit should be conducted every two years.

CCTV System Operation Audit should be submitted to the CEO for management of audit recommendations. Audit reports are not required to be released to the public. The audit should consider the following:

a) Independent verification of the attainment of objectives and procedures.

b) Audits of the access and data logs and the release and destruction of recorded material.

c) Review and evaluate CCTV Policy and compliance.

d) Review and evaluate procedures and costs for the release or viewing of information.

e) Review of any proposed System Expansion/Upgrade, Commissioning and Testing protocols;

f) Review and verification of the existing or suitable CCTV network configuration, coverage, functionality, effectiveness and efficacy.

g) Review of the existing or suitable CCTV Surveillance design and functionality;

h) Evaluation of current and future land use expectations and forecasts, particularly those involving licensed premises and entertainment outlets;

i) Assessment of future land use expectations, needs, including traffic management considerations;

j) Assessment of related strategic planning and vision statements;

k) Independent assessment of the CCTV Operation's financial management, including a review of budgeted and real costs, operational costs, such as system maintenance.

6.14. PUBLIC AWARENESS & MEDIA MANAGEMENT

6.14.1. CCTV SIGNAGE

The importance of effectively placing CCTV signage in the monitored area cannot be underestimated. Location, height and existing visual distractions are major factors which

contribute to the effectiveness of a sign when installed. CCTV signage should be considered to be a safety orientated sign and used for crime prevention purposes.

Signage can play a critical role in a CCTV Operation's effectiveness on influencing behaviour and perceptions of safety within the public space. It is recommended that signs be erected at formal or high traffic access points within the monitored area. Signs should be checked regularly for damage or theft.

As referred to in AS4806.1:2006, Part 11, signage at all CCTV system site entries (as a minimum) shall comply with the applicable Federal, State and Territory Privacy and Surveillance Legislation and shall comply with the requirements of AS 2342. For other examples and the display of multiple hazards, also refer to AS2416-2002.

It is important that CCTV signage be installed in positions which allow the best opportunity to capture the attention of pedestrians and thus improve safety and crime risk management.

6.14.2. PUBLIC INFORMATION

The Shire of Plantagenet will make available this Manual on the Shire of Plantagenet website.

Public inquiries in relation to the Shire of Plantagenet CCTV Operation must be made in writing to:

CEO, Shire of Plantagenet, PO Box 48, MOUNT BARKER WA 6324

6.15. CCTV OPERATION ACCESS CONTROLS

Access to the Designated Surveillance Area will be restricted to Authorised Personnel.

6.16. CAMERA MANAGEMENT

6.16.1. CAMERA SELECTION

Cameras should be risk assessed for the public area's environmental and lighting conditions, mounting options, the type of area activity to be expected.

The selection criteria for each camera placement and location should be documented and the effectiveness of the installation should be measurable and reviewed. An objective measurement is the camera's purpose, either to *detect, recognise* or *identify*. The effectiveness of the camera should therefore be found to directly attribute to safety, perception of safety, control of crime or assist Council management functions. This design base will allow documented design, commissioning, performance and monitoring of each camera and subsequently, the whole system.

Each camera should be housed in a vandal resistant, tinted environmental dome, rated to IP66, which both protects the camera and ensures that the camera itself, such as lens direction, is not clearly visible or accessible from the ground.

The location of the cameras should be clearly apparent to the public.

The CCTV System should be reviewed and specified to ensure maximum resolution and picture quality.

A replacement or upgrade program based on system value should be considered for the proceeding five years to seven years.

6.16.2. CAMERA RISK ASSESSMENTS

AS/NZS 31000:2009: Risk Management describes how the objectives of analysis are to separate acceptable risks from major risks. Risk analysis involves the consideration of the sources of risk, their consequences and the likelihood that those consequences may occur.

It is important to recognise how the CCTV camera will influence the consequences of any particular risk event which will impact in different ways within the target area. Financial costs, personal harm (physical and psychological), legal consequences and damage to reputation may all result from a single incident.

6.16.3. CONTROL AND OPERATION OF CAMERAS

FIXED CAMERAS

Fixed cameras should be selected for defined fields of view which have a designated and defined purpose, either to detect, recognise or identify. Refer to the WA CCTV Guidelines for detailed information on fixed cameras.

Any misuse is to be treated as a breach of the Code and subject to disciplinary action.

No audio will be recorded in public places.

Only Authorised Personnel will have access to camera operating controls

All Authorised Personnel will be made aware that recordings are subject to audit and they may be required to justify their interest in a particular member of the public or premises.

6.16.4. MAINTAINING CAMERA OPERATIONS

At any time, CCTV Management should provide an overview of the CCTV Operation, as follows:

1. Maintenance of CCTV recording equipment in a fully functional working order;
2. Maintenance of clear, recorded vision from each camera with records of down times.
3. Monitoring for obstructions (foliage, umbrellas, street trees and signage) and report on treatments against obstructions;
4. Ensuring any equipment fault is recorded and attended to in the shortest possible time frame;
5. Ensuring all Authorised Personnel contact lists are updated and current;

6.16.5. RECORDED MATERIAL

The retention of and access to recorded material will be only for the purposes provided by the Code of Practice and retrieved and treated in accordance with the Code of Conduct.

Recorded material will be retained for 31 days unless they are required in relation to the investigation of crime or for court proceedings.

Remnant recorded material will be purged following 31 days.

Access to and use of recorded material will only take place:

a) in compliance with the needs of police in connection with the investigation of crime; or

b) if necessary for the purpose of legal proceedings.

Recorded material will not be sold or used for commercial purposes or the provision of entertainment. Such practice will be a breach of the Code of Conduct and subject to disciplinary proceedings.

The showing of recorded material to the public will be allowed only in accordance with the media management policy or in accordance with the needs of the police in connection with the investigation of crime or in any other circumstances justified and authorised by law. The CEO must formally approve any such action.

Use of recorded material by the media should only occur to gain public information with respect to the identity of a person/s wanted in connection with a criminal investigation. Subject to the concurrence of the Police, the CEO may approve such releases. In such case the recognisable characteristics of other people in the footage shall be obscured.

Appropriate security measures and audit trails will be established against unauthorised access, alteration, disclosure, accidental loss or inadvertent destruction of recorded material.

Recorded material will be treated according to defined procedures and audit trails to ensure continuity of evidence.

6.16.6. CONTACT WITH POLICE

Contact related to CCTV Operations between Shire of Plantagenet Authorised Personnel and the W.A. Police will be conducted strictly in accordance with the Code of Conduct.

Police officers will not be permitted to remove any recorded material, operate CCTV equipment or have contact with recorded material at any time unless under the terms of this Code of Conduct or specified in the MOU or following the execution of a search warrant or other relevant, lawful process.

The Mount Barker Police have and maintain a live feed from the Council CCTV System for operational purposes.

7. CCTV OPERATING PROCEDURES

7.1. INTRODUCTION

These Operating Procedures (OPs) provide an initial framework for the establishment of tailored procedures specific to the CCTV Operations implemented by the Shire of Plantagenet. The objectives of the OPs are:

a) To provide personnel with all the safety, health, environmental and operational information necessary to perform their roles and responsibilities properly.

b) To ensure that CCTV Operations are performed consistently to maintain quality control of processes and recorded material.

c) To ensure that CCTV Operations continue with minimal disruption and are conducted to a prescribed standard.

d) To ensure that any system failures or faults are detected and responded to efficiently and rectified as soon as possible

e) To ensure that approved procedures are followed in compliance with Shire of Plantagenet and legislative requirements.

7.2. CCTV MANAGEMENT

The Shire of Plantagenet Surveillance Officer shall record all requests for recorded material, all material copied, number of surveillance hours, system faults and maintenance, and access to Designated Surveillance Areas.

The CCTV records shall be kept in a secure location and shall not be altered or have information removed at any time without the approval of the CEO.

Exchange of information between WA Police and the Shire of Plantagenet is to be noted and recorded subjectively.

7.3. MAINTAINING COMPLIANCE AND LOCAL GOVERNMENT BEST PRACTICE

7.3.1. REVIEW

These procedures shall be reviewed every five years and a report on KPIs is to be submitted to the CEO and Coordinator of the WA Blue IRIS Program.

7.3.2. COMPLAINTS HANDLING

Wherever a complaint indicates that an information privacy security principle has been breached, the Shire of Plantagenet must conduct an internal review, subsequently reviewable by a statutory body or independent third party.

Complaints which do not indicate a breach of the *Privacy Act 1988* can be handled in the manner set out by the Shire of Plantagenet's complaints handling practice.

7.4. AUTHORISED PERSONNEL - SELECTION AND RECRUITMENT

All Authorised Personnel must be duly authorised by the CEO to undertake defined roles.

All Shire of Plantagenet Authorised Personnel shall have a police clearance certificate.

All Authorised Personnel shall follow these procedures at all times.

All Authorised Personnel shall sign the approved Code of Conduct.

The employment of Authorised Personnel will comply with all relevant Shire of Plantagenet policies and in accordance with relevant industrial awards and legislation, including equal opportunity and occupational health and safety.

The Shire of Plantagenet will ensure that the selection process provides for thorough validation of the suitability of candidates to work in a CCTV Operations environment.

Authorised Personnel will be subject to disciplinary proceedings in the event of actions that do not comply with the conditions of the Code of Conduct. Where it is proved that personnel have breached any of the conditions of the Code of Conduct, these personnel will not be permitted to access to Designated Surveillance Areas.

The Surveillance Officer will ensure all visitors are briefed regarding the requirements of the Code of Conduct.

The Surveillance Officer will provide a formal induction to recruited Authorised Personnel on CCTV Operations and the CCTV Management and Operations Manual .

7.5. SELECTION OF SECURITY CONTRACTORS AND CONSULTANTS

There is a role for private sector security providers to assist the Shire of Plantagenet in the provision of CCTV Operations and related services, including CCTV design, system installation, system maintenance.

All security providers to the Shire of Plantagenet must provide appropriately qualified personnel and hold relevant licences in accordance with the *Security and Related Activities Act 1996* and preferably should hold current membership of a Security Industry Association guided by a Code of Conduct.

7.5.1. WA POLICE CONTACTS and BLUE IRIS REGISTER

For the day-to-day purposes, the Shire of Plantagenet's contact officer with the Police will either be the Officer in Charge of the local police station or the Police call number 131 444. As appropriate, the Officer in Charge or delegated police officers will liaise with the Shire of Plantagenet Surveillance Officer in regard to police activity with significance for the operation and management of the CCTV System.

Approval for the police use of the CCTV system in any manner will be subject to their agreement to comply with the MOU and Code of Conduct.

The presence of a Police Officer in Designated Surveillance Areas for a pre-planned operation or ongoing incident is permitted, subject to authorisation being given by the CEO. Police Officers may direct the operation of cameras.

The Shire of Plantagenet CCTV System will be registered with the WA Police Blue Iris program. If sought by police and viable, a remote control facility at the Police Operations Centre may be allowed. The WA Police must advise the Shire of Plantagenet Surveillance Officer should they wish to access the Shire of Plantagenet CCTV System and may direct cameras during a live incident, provided the actions requested comply with this Manual.

A written record will be maintained of any use of the system at the request of the Police. This record will include details of the Police Officer making the request, details of an authorising officer, time and date of the request and reasons for the request.

7.5.2. JOINT OPERATIONS WITH WA POLICE

The WA Police and the Shire of Plantagenet have entered into a MOU for CCTV Operations.

The Shire of Plantagenet acknowledges the WA Police as a key stakeholder in CCTV Operations.

Members of the WA Police may request the cooperation of the Shire of Plantagenet CCTV Operations for the purpose of surveillance relating to lawful WA Police operations and investigations.

Joint operation requests shall be made by the WA Police officer responsible for coordinating the operation or investigation. The request shall detail the times and general purpose for which surveillance support is requested.

The CEO may decline to provide cooperation in accordance with the Code of Conduct.

The CEO may withdraw cooperation at any time during the operation in accordance with the Code of Conduct.

7.6. CAMERA OPERATION

7.6.1. CONTROL AND OPERATION OF THE CAMERAS

Control Room equipment and the remote control of cameras will only be operated by Authorised Personnel or persons/staff under training. All these people will act with the utmost probity.

All use of cameras and recording equipment will accord with the purposes and key objectives of the CCTV System, as developed in training and specific operational instructions, and shall comply with the Code of Conduct.

Cameras will not be used to look into private property without cause. Operational procedures shall be adopted to ensure restraints upon the use of cameras in connection with private premises.

Camera positioning should be designed to provide sufficient fields of view of the public space and capabilities to provide identification, recognition or detection footage.

The List of Cameras and Locations is to be maintained.

7.7. TROUBLESHOOTING, FAULTS AND MAINTENANCE;

All faults and maintenance activity is to be recorded.

Faults and Maintenance activity are to reported.

7.8. DATA STORAGE

All recorded material will be retained for 31 days.

Images on reusable media should be copied from the original storage medium in the original file format onto a secure media. This secure media could be Write Only Read Many (WORM) or secure network storage. The term 'secure server' should be taken to mean an environment, including a security management system, which is accredited to a level of at least 'RESTRICTED', as approved by the Surveillance Officer. Once the images and associated data have been copied onto the secure media, it should not be possible to have the data overwritten or altered.

The generation of the secure copy should be carried out as soon as possible after the capture to reduce the time and opportunity for the accidental or malicious alteration to images. All imagery Master or Working Copies should be appropriately identified in order to facilitate the storage, retrieval and eventual disposal of case material.

In terms of evidential value there is no difference between bit-for-bit copies of the data on the Master, Working Copies and the images on the storage medium. This does not remove the necessity to protect the Master as an exhibit in case of challenges to evidence handling procedures or image manipulation. The software required for viewing proprietary formats must be available otherwise the images will be inaccessible. It is advisable to store any replay software with each recording to assist with the correct viewing of the files.

The choice of using network storage or WORM should be guided by factors such as volume of data, predicted storage time and longevity of WORM media. Master evidence not stored on WORM requires equivalent levels of protection such as access control and tamper-proof usage logs.

7.9. DATA ACCESS

7.9.1. ACCESS TO DESIGNATED SURVEILLANCE OPERATIONS AREAS

Only Authorised Personnel are permitted entry to the Designated Surveillance Area.

Other visitors to the Surveillance Area must be authorised by an Authorised Personnel and a record made of the purpose of the visit;

7.9.2. ACCESS TO AND SECURITY OF THE MONITOR

Access to view the monitors, whether to operate the equipment or view the images is strictly limited to staff with that responsibility.

Visits by no more than four Police Officers at any one time will be permitted provided that they are on duty and the visit is in connection with liaison, training or purposes of the system. Visit protocols should be in accordance with the MOU.

7.10. CONTINUITY OF EVIDENCE

Evidence, in terms of a still image or video footage, is the presentation of visual facts about a crime or an individual that the prosecution presents to the court in support of their case. The image will be presented either as hard copy or on a screen. it is possible to make a bit-for-bit identical copy of a digital image file.

In evidential terms there is no distinction between the copy and the primary or original file because the files are the same and have the same evidential weight. It is not important whether the file is on a stand-alone or networked computer, a server, or on any type of storage medium. This assumes the operation of adequate security against unauthorised and unrecorded access.

If no discipline is applied there can be any number of identical files. For evidential purposes it is essential to be able to demonstrate that the images are authentic and have originated from the files captured in the camera and recorded to the first medium.

Integrity verification is the process of confirming that the data (image, CCTV clip, etc) presented is complete and unaltered since time of acquisition. Relevant questions concerning integrity might include: 'Has data been added to, or removed from the file?'; 'Has the data within the file been changed?'

Authentication is the process of substantiating that the data is an accurate representation of what it purports to be. Relevant questions concerning authentication would deal with issues such as: 'Was the image taken at the time stated?'; 'Was the image taken at the place stated?'

It should be noted that standard image processing techniques such as lightness or contrast changes would affect the image integrity but not the image authenticity; however, a change to the clock on a CCTV system could affect the image authenticity but not affect the image integrity. Robust audit trails are required in order to maintain image authenticity.

The audit trail should include the following information (with date and time of action) when available and if appropriate:

a) Details of the case.

b) Classification of the image (and any special handling instructions, if relevant) and the name of the person who classified the image.

c) If the image is third-party generated, information about point of transfer including whether the image is the Master copy, a Working Copy or an exhibit derived from a Working Copy.

d) Information about capture equipment and/or hardware and software used, including details of the maintenance log relating to capture equipment and calibration of hardware and software.

e) Identity of the capture operative including third parties and image retrieval officers, where applicable.

f) Details of exhibits and disclosure officer(s).

g) Description of the images captured, including sequencing.

h) Details of retrieval or seizure process and point of transfer, if applicable.

i) Creation and definition of the Master copy and associated metadata.

j) Storage of the Master copy.

k) Any access to the Master copy.

l) Viewing of the Master and Working Copies, including a record of any associated viewing logs.

m) Details and reasons for any selective capture.

n) Any editing applications which may alter the image.

o) Any details of processing applications allowing replication by a comparatively trained individual.

p) Electronic history log of processing applications.

q) Any copying required to ensure longevity of the data.

r) Cross References on the Master and Working Copies.

s) Any copying carried out as part of a migration strategy to ensure the replay longevity of the image.

t) Disposal details and retention time periods.

7.10.1. VIEWING OF RECORDED MATERIAL

WA Police officers, legal representatives acting on behalf of individuals engaged in legal proceedings related to a recorded incident or individuals acting as their own legal counsel in relation to a recorded incident may request to view recorded material relating to an incident or investigation.

Such a request must specify the date, time and location of the incident which the person wishes to view.

Requests by legal representatives and individuals shall be made in writing and lodged with the CEO who will then refer the request to the Police for a determination.

Requests to view recorded material shall be referred to the Police as soon as reasonably practicable and otherwise within five working days. Police requests are to be dealt with as a priority and response times noted as a KPI.

7.10.2. COPYING OF RECORDED MATERIAL

In most cases a CD or DVD writer will suffice for exporting single images and short video clips under about 10 minutes in length.

For exporting longer video clips and for large scale archiving, the system should provide one of the following:

- the ability to export video to an external 'plug and play' hard drive via a USB or Firewire connection
- Network port
- Removable hard drive

The CEO may authorise the copy of original material where a recorded incident is the subject of police investigation, prosecution or legal proceedings;

Copying of original recorded material is to be made only by Shire of Plantagenet Authorised Officers.

Recording Mediums are to be marked 'original' (one only) and 'copy' and certified as such by the Surveillance Officer.

Certified copies of recorded material may only be released to the WA Police, and once authorised to legal representatives acting on behalf of individuals engaged in legal proceedings related to a recorded incident, or individuals acting as their own legal counsel in relation to a recorded incident

Certified copies will only be released to the parties named in the written request when permission to do so has been received from the Police and the CEO on the completion of the appropriate documentation.

7.10.3. RELEASE OF ORIGINAL RECORDED MATERIAL

Original recordings and still photographs shall not be released to any person or third party unless requested under a search warrant or by court summons or by a recognised legal instrument; and

At no time shall original or copied recordings or still photographs be released to any media organisation, journalist or other individual or group without the approval of the CEO.

7.10.4. VIDEO IMAGES

To allow ease of current and future use of the recordings for investigations and appeals, etc, the CD/DVD should include:

a) the image sequence or sequences clearly identified;

b) an easily-read text file stating any requirements for special hardware or software for replay;

c) all associated metadata (time and date should be bound to the relevant images); and

d) licence-free software enabling the sequences to be viewed correctly.

Other items that could be included:

a) text data about the originating camera or system;

b) audit trails;

c) authentication or verification software; and

d) short test sequence to confirm that the recorded image sequences are being replayed correctly.

7.10.5. MASTER COPY SAFEGUARDS

There are various media on which images can be captured, both reusable and non-reusable. Irrespective of their nature, early transition from 'capture' to 'defining the

Master' phases is extremely important. The integrity of images needs to be protected at the earliest stages as this reduces the opportunities for challenges at court.

Accidental alteration or erasure could be detected by noting image number sequences and prevented by:

a) designating the image file as read only;

b) activating the mechanical write protect mechanism; and

c) transferring to WORM (Write once read many) media

Protection can also be achieved by controlling access to the file or media by electronic password and/or controlling the viewing of images by electronic encryption.

The Procedure does not rely on any form of 'electronic' protection but neither does it preclude its use. There are several methods for 'electronically' verifying the integrity of an image file. Once applied, any change to the pixel values will be detected although the nature and location of the changes may not be indicated.

7.10.5.1. File integrity techniques

If a 'hash' function is applied to an image, a unique numerical value is calculated for the whole image. The number is embedded in the metadata of the image file. A change in pixel value causes the 'hash' function value to change. This is the basis for most 'authentication' software. Manufacturer specific software for image integrity is becoming increasingly prevalent, as are non-destructive (i.e. fully reversible) editing techniques.

7.10.5.2. Watermarking

Watermarking describes visibly insignificant changes made to the pixel values to incorporate information which changes if the image file is altered. The watermark may then become visible on the picture or even make it unreadable. The primary use for watermarking is to protect the intellectual property rights of the photographer or film maker. Its use may lead to claims that the image is not authentic because the pixels have been changed, therefore the use of watermarking is not recommended for image integrity.

7.10.5.3. Encryption

The image file is encrypted so that the file cannot be opened except with the correct decryption key. This has particular value if images are to be transmitted to or from remote sites. Loss or corruption of either the key or the data may make files unrecoverable.

7.10.5.4. Handling

Images should also be protected from accidental deletion by the careful handling of media. Media should be stored in clean, dry environments and kept away from strong magnetic fields, strong light and chemical contamination. Some media such as CDs and SmartMedia will be damaged if allowed to become dirty or scratched.

The Master is defined and will be documented as such. It will then be stored securely pending its production (if required) at court as an exhibit. Only in the event of any doubt being cast on the integrity of the images will the Master be viewed.

A Working Copy is usually produced simultaneously, or immediately after the Master is defined. The Working Copy, as its name implies, is the version that will be used for investigation and to assist in the preparation of the prosecution file.

All use and movement of the Master will be logged in the audit trail. Similarly any significant use, enhancement and distribution of Working Copies should be logged. The aim is to support the presentation of evidence through legal proceedings. All audit trails should be disposed of when the image files and any analogue copies are disposed of.

7.10.5.5. Define Master and produce Working Copy

The core of the Procedure is the production, definition and storage of a Master which can be examined if required by the court to confirm the integrity of the images. The Master should be:

a) labelled or named (with due care to the longevity of label and readability of medium);

b) stored in a form and manner, with software if required, so that the images may be viewed in the future;

c) kept in accordance with exhibit protocol; and

d) never used, except to make further copies together with appropriate audit trail, or by order of the court to verify integrity.

Police policies should be developed to cater for these requirements. Image files should be in the same format as:

a) received by the police in the case of third party images;

b) first captured on medium in/or attached to camera; and

c) as recorded after transmission from camera.

7.10.5.6. Produce Working Copies

Working Copies can be in many forms. The files can be copied onto any suitable medium or distributed electronically (if a secure system is in place) for circulation to the investigating officers and Shire of Plantagenet. Issues of quality control, security and resource management need to be considered.

7.11. RECORDING AND STORAGE

7.11.1. RECORDING OF IMAGES

CCTV images may only be recorded by the Shire of Plantagenet and the WA Police

All information recorded, collected and collated by means of CCTV Operations shall remain the sole property of the Shire of Plantagenet

Any incident recorded and selected for review shall be noted in the daily register including date, time and category of incident. The date, time and category of incident shall be noted on the recorded medium (CD Rom, DVD, USB, HDD) and electronic file name.

All recorded material shall be kept in secured storage, including electronically, under the control of the Shire of Plantagenet

All original residual recordings shall be erased after 31 days after the date of the recording unless the footage has been reviewed or a request is made in writing for it to be held.

All written requests for access to original video recordings shall be filed.

Authorised Personnel may view any footage on a random basis in accordance with the Code of Conduct.

7.12. SOFTWARE SYSTEM OVERVIEW AND MANUALS

All CCTV System's Operation and Technical Manuals will form part of this CCTV Manual. Electronic Copies may be provided and stored for ease of access.

7.13. SYSTEM WARRANTIES AND MAINTENANCE

A record of system warranties and maintenance requirements will be formulated and integrated with maintenance and cleaning schedules.

7.14. GAPS ANALYSIS AND ERROR REPORTING

CCTV Operational gaps and errors must be acknowledged and rectified wherever possible.

8. OPERATION REDUNDANCY AND DISASTER RECOVERY

Refer to the CCTV System's Operation and Technical Manual for detailed Redundancy Configuration Requirements and recovery of data following power outages, system faults and other impediments to operations.

9. MEMORANDUM OF UNDERSTANDING

This MEMORANDUM OF UNDERSTANDING is made on DATE

BETWEEN:

SHIRE OF PLANTAGENET: CEO

And

WESTERN AUSTRALIA POLICE: Regional Inspector or Office in Charge (Mount Barker)

PURPOSE

The CCTV Operation was established by the Shire of Plantagenet to contribute to the safety and security of persons and property within the confines of the Mount Barker CBD.

Western Australia Police are concerned with enhancing the quality of life and well-being of the community by contributing safety and security.

The purpose of this agreement is to facilitate a collaborative cooperative approach to enhancing the safety and security of persons and property within the Shire of Plantagenet.

SHIRE OF PLANTAGENET CONTRIBUTION

The Shire of Plantagenet is responsible for the operation of the CCTV System.

The CCTV Operation will be operated in accordance with the Shire of Plantagenet policies and procedures developed in conjunction with Ministry of Justice guidelines.

The Shire of Plantagenet will maintain a record of occurrences, incidents and visitors to the CCTV designated surveillance area.

The Shire of Plantagenet will maintain appropriate systems and processes to ensure the secure retention and disposal of recorded material.

The Shire of Plantagenet will provide operational and evidentiary assistance to Western Australia Police to facilitate policing operations and the successful investigation and prosecution of offences.

WESTERN AUSTRALIA POLICE CONTRIBUTION

Western Australia Police will provide appropriate support and response to identified incidents and issues.

Western Australia Police will maintain an effective record of occurrences, incidents and activities for the CCTV Operations target areas.

Western Australia Police will seek approval from the Shire of Plantagenet prior to conducting operations which utilise CCTV Operations.

Western Australia Police will have access via a dedicated feed of the CCTV data to the Mount Barker Police Station.

CONFLICT RESOLUTION

Conflicts which cannot be resolved by operations personnel will be directed to the CEO, Shire of Plantagenet and the Officer in Charge, Mount Barker Police Station for resolution.

TERM

The term of this memorandum of understanding is five years from the date this undertaking is signed.

REVIEW AND TERMINATION

Prior to the expiry of this agreement, the parties agree that the Memorandum of Understanding will be reviewed in order to determine whether both the Shire of Plantagenet and Western Australia Police agree to continue.

Following such a review, either party may terminate its obligations under this Memorandum of Understanding by sending notice of such termination to the other party in writing.

AGREEMENT

The parties understand and agree that this Memorandum of Understanding is a clear statement of their intentions as to the matters stated and that the agreement will not be legally binding.

SIGNED for and behalf of

the **SHIRE OF PLANTAGENET by**: Signature

NAME

CHIEF EXECUTIVE OFFICER

SIGNED for and behalf of

WESTERN AUSTRALIA POLICE

by: Signature

NAME

RANK

STATION

10. RELEASE FORM FOR RECORDED MATERIAL

REQUEST FOR RECORDED IMAGES FROM CCTV SURVEILLANCE RECORDS

To: Chief Executive Officer, Shire of Plantagenet

It is requested that Copy Marked _____ or Photograph showing an Incident on (date/s) _____ between time(s) _____ and _____ be released to me for the purpose of Evidence / Investigations which are subject to Police / Ranger / Security/ Civil Litigation inquires or proceedings.

We / I accept full responsibility for this Copy / Photograph whilst it is in our/my possession and understand that We / I am **NOT** at liberty to make or release copies of the footage or permit other persons to make copies or lend it to persons other than for the purpose for which the copy was made.

The Copy/Photograph will **NOT** be released to the Media under any circumstances unless authorised by the Chief Executive Officer of the Shire of Plantagenet and the Western Australia Police.

We / I accept responsibility for advising the Shire of Plantagenet as to the estimated date of return or destruction of this property and that it be returned in the same serviceable condition as obtained.

INCIDENT TYPE

- ❑ Offence against the Person (Type _____)
- ❑ Offence against Property (Type _____)
- ❑ Police Operation or Investigation (Type _____)
- ❑ Security or Ranger Services (Type _____)
- ❑ Civil Litigation or Subpoena Served (Type _____)

COPY HANDED TO

SIGNED:_____

NAME:_____

RANK and NO:_____

DATE:_____

STATION/SECTION:_____

DATE:_____

SHIRE OF PLANTAGENET

SIGNED:_____

CEO

COPY/PHOTOGRAPH RETURNED:
Date:_____Signed_____

COPY/PHOTOGRAPH DESTROYED:
Date:_____Signed_____

11. CCTV Incident Report

Location: **Report No:.....**

Incident	**Other Emergency**	**Local Authority**	**Other**
Assault – minor	Fire	Repair/maintenance	List...
Assault – serious	Water	Environment	
Malicious Damage	Medical	Traffic	
Traffic	Power	Waste	
Trespass		Health	
Stealing		Ordinance/breach	
Robbery		Safety	
Intoxicated Person	**Community**	**CCTV Maintenance**	
Information only	Cash escort	Cameras	
Security	Demonstrations	Recording equip.	
Street offence	Special Events	Monitoring equip.	
Other...	Parade	Optic fibre	
	Security	House keeping	

Organisations Responding Police / Fire / Ambulance / Shire of Plantagenet

Ref No. TIME NOTIFIED TIME RESPONDED

NARRATIVE

FOOTAGE TIME(s)

Officer Name **DATE**

Incident Recording Details

Camera No(s)

Other References

This page has been left blank.