CCTV POLICY AND PROCEDURE

1. Introduction

1.1 Cove UK believes that CCTV is a powerful tool to assist with efforts to enhance customer and Team safety, and that the operation of CCTV should be controlled to avoid the potential of misuse. The Information Commissioner's CCTV Code of Practice provides a framework for the operation of CCTV. Cove UK supports this Code of Practice, which is applied in the context of Cove UK through this CCTV Policy & Procedure.

1.2 Any reference in this document to 'CCTV System', 'CCTV' or 'System' applies equally to the Cove UK CCTV System's (which predominantly operates inside the Venues or Offices with supplementary CCTV cameras on different locations on the Park. The cameras in the Venues or Offices and on Park are not actively monitored in the Cove UK Security Control Room and are only viewed by a licenced operator when there are security concerns and/or reports of an incident.

1.3 No cameras, including webcams, may be installed or operated on Cove UK property without the permission of the Resort Director or Head of Security and Caravan & Lodge Owners can only have CCTV which monitors their Caravan & Lodge and Veranda and cannot in anyway have any views/Images on other Owners Caravan & Lodges.

2. Objectives

2.1 This Policy aims to ensure that CCTV on Cove UK's premises is operated **to enhance safety, and the sense of safety**; and thereby assists in encouraging use of Cove UK's facilities, through the following subsidiary objectives:

(1) To assist in deterring crime

(2) To assist in detecting crime and to provide evidential material for court proceedings

(3) To assist in the overall management of buildings and land within the boundaries of Cove UK.

(4) To assist in monitoring, and planning for, emergency operations; and to assist the Police, Fire, Ambulance and Civil Emergency Services with the efficient deployment of their resources to deal with emergencies.

2.2 This Policy aims to ensure that CCTV is used transparently and proportionately to achieve the objectives identified in Section 2.1, in compliance with the law and the Information Commissioner's CCTV Code of Practice.

2.3 The reference in 2.1 (3) to "the overall management of buildings and land" incorporates such matters as monitoring of traffic flow, car-park capacity, defects in lighting, and damage to buildings.

3. Core Obligations

3.1 Cove UK will identify the locations of all cameras connected to the Cove UK CCTV System and will monitor, and manage, images shown on these cameras in accordance with this Policy and the associated Procedure.

3.2 All Team outside Contractors and Customers of Cove UK are subject to the CCTV Policy and are required to contribute, on request, to the application of this Policy.

3.3 Team who have been designated as having responsibility for the management and the operation of the CCTV system are required to undertake their responsibilities strictly in accordance with this Policy, and the associated Procedure. Such Team are required to operate the CCTV system fairly, within the law, and only for the objectives identified in this Policy.

4. Guidance

4.1 This Policy is accompanied by a Procedure and a Manual which regulate the operation of CCTV.

4.2 Guidance on the application of this Policy and the associated Procedure is available from the Resort Director or Head of Security.

5. Responsibilities

5.1 Cove UK is the "data controller "of the system and the "owner" of the data generated by the system.

5.2 Overall responsibility for the implementation of the Policy has been delegated by the General Manager of Cove UK to the Resort Director or Head of Security at Cove UK.

5.3 Breach of this Policy and the associated Procedure may result in disciplinary action being taken in accordance with Cove UK's Team Disciplinary Policy and Procedure.

6. Human Rights

6.1 Cove UK recognises that operation of the Parks CCTV system may be considered an infringement on privacy. Cove UK acknowledges its obligations under the Human Rights Act 1998. Cove UK also recognises its obligation to provide a safe environment for Team, Contractors and visitors; and regards the use of CCTV within Cove UK as a necessary, proportionate and suitable tool.

6.2 The CCTV system will only be used as a proportional response to identified problems and may only be used insofar as is necessary, in the interests of national security, public safety, the prevention and detection of crime or disorder, the protection of health, the protection of the rights and freedoms of others, the management of buildings and land, and assistance in the resolution of a factual disagreement which emerges during investigation of a grievance, complaint or disciplinary allegation.

6.3 Cove UK's CCTV system shall be operated with respect for all individuals, recognising the right to be free from inhuman or degrading treatment and avoiding discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

7. Data Protection

7.1 The operation of the system has been registered with the Information Commissioner's Office in accordance with current Data Protection legislation

7.2 All personal data will be processed in accordance with the Principles of the Data Protection Act 2018 (GDPR) which include, but are not limited to:

i. All personal data will be processed fairly and lawfully (The definition of 'processing' covers 'obtaining')

ii. Personal data will only be processed for the purpose specified

iii. Personal data will be adequate, relevant and not excessive

iv. Personal data will be accurate and where necessary kept up to date

v. Personal data will be held no longer than necessary

vi. Individuals will be allowed access to information held about them and, where appropriate, will be permitted to correct or erase it

vii. Procedures will be implemented to prevent unauthorised or accidental access to, alteration, disclosure, or loss and destruction of information.

8. Release of Personal Data, Following a Personal Request for Information

8.1 Any request from an individual for the disclosure of personal data under the Data Protection Act, or for disclosure under the Freedom of Information Act, which he/she believes is recorded by virtue of the system, should be made, in the first instance, to the General Manager of Cove UK.

8.2 Under the Data Protection Act 2018 (GDPR) the rights of data subjects and others) shall be followed in respect of every request.

8.3 Any person making a request must be able to prove his/her identity and provide sufficient information to enable the data to be located.

8.4 The Resort Director or Head of Security, General Manager and the Club Group Manager are authorised to view CCTV images in order to process a Subject Access Request.

8.5 If a request can only be complied with by identifying another individual, or several individuals, arrangements must be made to safeguard the rights of that individual or individuals, such as obtaining permission from that individual or individuals or blocking of the image of that individual or individuals.

8.6 Where the General Manager or the Resort Director or Head of Security authorises a viewing of a CCTV image by the individual whose personal data is recorded on the image, that individual will be monitored at all times.

8.7 Authorised viewings of personal data will normally take place in the Head Security Office or the Office of the Club Group Manager.

9. Release of Personal Data as Required by Law

9.1 As required by law, the Resort Director or Head of Security may authorise Security Personnel to release personal data to members of the police service, or other agency having statutory authority to investigate and/or prosecute offenders.

9.2 Exemptions to the non-disclosure provision of information are provided in the Data Protection Act, which allows that personal data processed for the purposes of

- The prevention or detection of crime
- The apprehension or prosecution of offenders

Are exempt from the non-disclosure provisions in any particular case, “to the extent to which the application of those provisions would be likely to prejudice any of those purposes”. Each and every application will be assessed on its own merits and ‘blanket exemptions’ will not be applied.

9.3 Members of the police service, or other agency having a statutory authority to investigate and/or prosecute offenders, may release to the media details recorded by Cove UK only in an effort to identify alleged offenders, or potential witnesses, and only in accordance with their responsibilities as the new controller of the data.

10. Release of Personal Data to a Person who is not the Data Subject

10.1 A Cove UK Senior Manager* who is investigating a complaint, grievance, or disciplinary allegation, under a formal Cove UK process, must seek authorisation from the General Manager for release of the personal data contained in an image which has been obtained during surveillance of the Park, in accordance with the objectives stated in Section 2 of this Policy.

10.2 Cove UK's General Manger may grant such authority, in writing, where he/she is satisfied, either:

a) that there is prima facie evidence of an allegation which exists independently of the image, and prior to the request for authorisation or

b) that the allegation relates to criminal activity or

c) that both parties have agreed that it would be beneficial for the Senior Manager to view the image, or

d) that one (or more) party has already viewed the image (having submitted an application to view on the grounds of being recorded in the image).

10.3 In the absence of the General Manager he may appoint another member of the Senior Management team to act in his Place.

11. Complaints

11.1 Any member of Team or the general public wishing to register a complaint with regard to any aspect of the system may do so by contacting the ead of Security in the first instance. Data Protection concerns may be referred to the General Manager.

11.2 Should the matter remain unresolved; a formal complaint may be submitted to the General Manager.

12. Copyright

Cove UK retains ownership of copyright and of all material recorded by the system.

13. Relationship with Existing Policies, Standards and Legislation

This Policy and the CCTV Procedure take account of Cove UK's Data Protection Policy, the Information Commissioner's CCTV Code of Practice, and the following legislation:

- Criminal Procedures and Investigations Act 1996
- Human Rights Act 1998
- Data Protection Act 2018(GDPR)
- Crime and Disorder Act 1998

- Equalities Act 2010

14. Definitions

In this Policy and Procedure, the phrases “disclosure of data”, and “release of data” could incorporate a viewing of personal data and/or production of a copy of the personal data. The presumption under which this Policy and Procedure operates is that the viewing of data is sufficient for most circumstances. The release of a copy of personal data may only be authorised by the General Manager or Resort Director.

CCTV Procedure

This Procedure accompanies Cove UK's CCTV Policy which regulates the operation of Cove UK's CCTV system. The purpose of the CCTV Procedure is to support the objectives of the Policy by outlining how Cove UK will implement the CCTV Policy.

Extract from Cove UK's CCTV Policy

2. **Objectives**

2.1 This Policy aims to ensure that CCTV on Cove UK's premises is operated **to enhance safety, and the sense of safety**; and thereby assists in encouraging use of Cove UK's facilities, through the following subsidiary objectives:

(1) To assist in deterring crime

(2) To assist in detecting crime and to provide evidential material for court proceedings

(3) To assist in the overall management of buildings and land within the boundaries of Cove UK.

(4) To assist in monitoring, and planning for, emergency operations; and to assist the Police, Fire, Ambulance and Civil Emergency Services with the efficient deployment of their resources to deal with emergencies.

CONTENTS

1. General Principles

1.1 Lawful – The system will be operated in accordance with the law, including, in particular, the Data Protection Act 2018 (GDPR) and the Human Rights Act 1998. The CCTV system may not be used where the privacy of individuals would clearly be violated, provided a criminal offence is not taking place.

1.2 Restricted Application – The system shall be operated fairly, within the law, and only for the purposes stated in the CCTV Policy. Any individual or authority/organisation utilising the CCTV

system must comply fully with this Procedure and will be held accountable under the CCTV Policy and this Procedure.

1.3 Overt – The location of all cameras are visible in all Venues or Offices and on the Park Locations. The CCTV system will not be used for covert surveillance.

1.4 Balanced – Cove UK will balance the Team and public interest in achievement of the objectives of the CCTV system and the public interest in the operation of the CCTV system, including the security, transparency and integrity of all operational procedures in relation to CCTV. Consequently, a formal structure has been put in place, including a complaints procedure, by which it can be demonstrated that the CCTV system is accountable, and is also seen to be accountable.

2. Cameras and Coverage

2.1 The areas covered by Cove UK's CCTV system, to which this Procedure refers, are both Team and public areas and areas within the responsibility and/or perimeter boundaries of Cove UK.

2.2 The number and location of all of the cameras is located in this Document.

2.3 Signs will be placed at the main entrance points to Bunn Lesiure.to indicate:

- The presence of CCTV
- The purpose of the CCTV system
- Ownership of the system
- Contact details

Signage will also be placed at entrances to the buildings where internal CCTV cameras are in operation.

2.4 Some cameras may be enclosed within all-weather domes for aesthetic or operational reasons, but the presence of cameras connected to Cove UK's CCTV system will be identified by appropriate signs.

2.5 On occasions, transportable or mobile cameras connected to Cove UK's CCTV system may be temporarily sited within the boundaries of Cove UK. The use of such cameras, and the data produced, will conform to the objectives of Cove UK's CCTV system, and will be governed by Cove UK's CCTV Policy and Procedure.

3. Monitoring and Recording Facilities

3.1 The security control room (referred to as "Security control"), Teamed by Cove UK Security Team, is located on West Sands Opposite the Windmill.

3.2 Cove UK CCTV operators are able to record images in real-time, replay images, and produce hard copies of recorded images, in accordance with this Policy and Procedure. This applies equally to images derived from the core system and from the supplementary system, but images from the supplementary system are not normally viewed in real time. Viewing and recording equipment may only be operated by trained and authorised operators.

3.3 The Resort Director or Head of Security and Club Group Manager may view all cameras from their Offices, but cannot control the movement of cameras from this location.

3.4 In certain circumstances, Cove UK Team other than the CCTV operators may be granted viewing rights (live images only) for one or more cameras on the supplementary CCTV system. Applications for the right to view should be submitted in the first instance to the Resort Director or Head of Security .The right to view such a camera does not entail the right to control the camera, which remains solely with the CCTV operators in the control room.

4. Operation of the System

4.1 All persons operating CCTV cameras must act with the utmost probity at all times. Operators are required to sign a declaration of confidentiality.

4.2 The Resort Director or Head of Security is required to provide all individuals operating the CCTV system with a copy of the CCTV Policy and Procedure. All relevant Team are required to sign to confirm that they fully understand their obligations as set out in the CCTV Policy and Procedure.

4.3 A Manual containing technical instructions on the use of the equipment will be housed in the control room.

4.4 The control room and monitoring system must be Teamed, at all times, by at least one Security officer. Any unauthorised use or abandonment of Cove UK's control room and its systems and equipment for any purpose whatsoever (apart from evacuation in an emergency) may amount to gross misconduct under Cove UK's Team Disciplinary Procedure. If the control room must be vacated in an emergency, for safety or security reasons, the Manual must be followed.

4.5 Only members of Team authorised by Cove UK to operate the CCTV system may have access to the operating controls. Those operators will have primacy of control at all times.

5. Maintenance of the System

5.1 To ensure compliance with the Information Commissioner's Code of Practice, and to ensure that images recorded continue to be of appropriate evidential quality, the system shall be maintained in accordance with the requirements of the procedural manual under a maintenance agreement. User requirements can be maintained by a member of Security Personnel. Faults will need to be maintained by a CCTV Engineer.

5.2 The maintenance agreement will make provision for:

- Regular service checks on the equipment, including cleaning of any all weather domes or housings, checks on the functioning of the equipment and any minor adjustments that need to be made to the equipment to maintain picture quality.
- Regular overhaul of all the equipment and replacement of equipment which is reaching the end of its serviceable life.
- "Emergency" attendance by a specialist CCTV engineer on site to rectify any loss or severe degradation of image or camera control.

5.3 The maintenance agreement will define the maximum periods of time permitted for attendance by the engineer and for rectification of the problem, depending upon the severity of the event and the operational requirements of the system.

5.4 Appropriate records of faults must be maintained by the Security Operations Manager in respect of the functioning of the cameras/system and the response of the maintenance organisation.

6. Access to, and Security of, Control Room and Associated Equipment

6.1 Only authorised operators who have been certified as appropriately instructed may operate any of the equipment located within the control room. A list of all authorised operators will be maintained in the control room by the Security Operations Manager. An authorised operator must be present at all times when the equipment is in use.

6.2 The control room must be secured at all times. The entrance door to the control room must be fitted with a device to restrict entry from outside, and this must be used by authorised operators to maintain the security of the control room.

Police in the pursuance of their duties

The names of such visitors must be recorded, and visitors must be accompanied at all times by an authorised operator or the Security Manager.

6.4 Public access to the control room will be prohibited except for lawful, proper and sufficient reasons and only then with the personal authority of the Resort Director or Head of Security. Any such visits will be conducted and recorded in accordance with this Procedure.

7. Management of Recorded Material

7.1 For the purposes of this Procedure, “recorded material” means any material recorded by, or as a result of, the technical equipment which forms part of the system, but specifically includes images recorded digitally, or by way of video copying, inclusive of video prints. Every recording obtained using the system has the potential of containing material that may be admitted as evidence in a court of law at some point during its life span.

7.2 It is of the utmost importance that, irrespective of the format of the images obtained from the system, recorded material is treated strictly in accordance with this Procedure from initial recording to date of destruction. All movement and usage of material must be recorded.

7.3 Access to, and the use of, recorded material must be strictly in pursuance of the purposes defined in Cove UK’s CCTV Policy.

7.4 Recorded material may not be copied, sold or otherwise released or used for commercial purposes, personal use, or for the provision of entertainment.

7.5 All material recorded by the system will be retained for 30 days (depending on the system) before being overwritten or erased. Recordings may only be retained beyond this period in the following circumstances:

- Where evidential material exists which is likely to be required by the Police. (This should be kept for duplication and subsequent production in court.)
- Where material is required following a Subject Access Request submitted within 14 days of the incident.
- Where material is required as part of a Freedom of Information Request
- Where the evidence is required under a court order.
- Where the General Manager informs the Resort Director or Head of Security Manager or the Club Group Manager that the maintenance of the material is in the interests of Cove UK, and in accordance with the CCTV Policy.

In these circumstances, the material will be copied to a disc/Memory Stick.

7.6 To ensure the quality of recorded material, only discs/memory sticks that have been specified for the sole use under Cove UK's CCTV system may be used. Each disc/memory stick will have its own unique identity number.

7.7 Each disc will be magnetically erased/wiped/Memory sticks all data deleted –
- Before re-use
- Before destruction
- At the end of its life (12 months or earlier, if necessary)

7.8 Images from every camera will be recorded continuously throughout a 24-hour period. No disc, print or still image may be retained beyond the 30 day period, other than in those special circumstances identified in 7.5 above.

7.9 All recorded images will be identified by camera number, date recorded and time group. Images may only be reviewed by Cove UK Resort Director or Head of Security the Club Group Manager or by such other persons as are authorised by this Policy/Procedure.

7.10 In the event of any recorded material being required for evidential purposes, the procedures outlined in the procedure and manual must be strictly complied with.

8. Request for Information/Release of Data

8.1 Members of Cove UK and the general public who believe their image has been captured by the system have the right to view relevant footage at a time convenient to themselves and to Cove UK. To this end, an individual, and/or his/her legal representative, may request a viewing or a copy of the footage by writing to Cove UK's General Manager.

8.2 Requests for the release of personal data generated by this CCTV system should be directed to:

Operations Director
Cove UK
Warner Lane
Selsey
PO209EL

8.3 Principles of the Data Protection Act 2018(GDPR)(rights of data subjects and others) shall be followed in respect of every request.

8.4 Any person making a request must be able to prove his/her identity and provide sufficient information to enable the data to be located. To this end, the written request should be accompanied by name, address and proof of identify (photocopy of passport ID page, driving license, birth certificate or Team card).

8.5 On receipt of the request Cove UK will make every effort to reply to a request within 40 days. However, there may be some circumstances where Cove UK requires further information, which will be requested within the 40 day period.

8.6 If the request can only be complied with by identifying another individual, permission from all parties must be sought first.

8.7 In complying with the national standard for the release of data to third parties, Cove UK will, as far as is reasonably practicable, safeguard the individual's right to privacy, and will give effect to the following principles:

- Recorded material shall be processed lawfully and fairly, and should be used only for the purposes defined in this code
- Access to recorded material will only take place upon completion of a declaration of confidentiality.
- The release or disclosure of data for commercial or entertainment is specifically prohibited.

8.8 Members of the police service, or other agency having a statutory authority to investigate and/or prosecute offenders, may release to the media details recorded by Cove UK only in an effort to identify alleged offenders or potential witnesses, and only in accordance with their responsibilities as the new controller of the data.

8.9 If material is to be shown to witnesses, including police officers, for the purpose of obtaining identification evidence, it must only be shown after prior approval for disclosure is granted by the General Manager or person of equivalent status.

9. Responsibilities

9.1 Security Manager

The Resort Director or Head of Security will:

- Ensure that the Policy and Procedure are adhered to.
- Ensure that there is no breach of Security.
- Ensure that the functions of the CCTV system are implemented.
- Ensure that operators are supervised and developed.
- Ensure that the interests of Cove UK are upheld in accordance with the terms of the Policy, Procedure and Code of Practice.
- Ensure that all faults relating to the system and any associated equipment forming part of the CCTV system are reported and adequately maintained and developed.
- Consider reports from the operators detailing the state of readiness of the equipment and the day-to-day and long-term operation of the system.
- In consultation with the operators and other relevant individuals, investigate and propose alterations, additions or amendments to the system.
- Liaise with relevant Team to ensure that CCTV Policy and Procedure remains compliant with legislation.
- Facilitate viewing requests, including making arrangements to copy footage for potential viewings, as requested by the GM
- Ensure that operators and other relevant Team are regularly reminded about the contents of the Policy and Procedure, and any updates.
- Ensure destruction of images, in accordance with protocols.
- Monitor and supervise the daily procedural instructions, security of data and confidentiality.
- Ensure that at all times operators of the CCTV system carry out their duties in an efficient and responsible manner. This will include regular checks and audit trails to ensure that any documentation is relevant and up to date.

9.2 **Operators**

Operators are responsible for taking appropriate action to deal with incidents detected through use of the system, and for keeping records, as required by this Handbook.

Operators must:

- Carry out their duties in accordance with the Policy, the Procedure, and managerial instructions.
- Control and operate the cameras and equipment forming part of the system with proficiency.
- Ensure that information recorded by the system or operator (spot recording) is accurate, adequate, and relevant and does not exceed that necessary to fulfil the purpose of the system.
- Justify decisions to view or record any particular individual, group of individuals or property, when requested by the supervisor or manager.
- Regularly refresh their knowledge of the contents of the CCTV Policy and Procedure, and manuals.

10. Discipline

10.1 Team who impede implementation of the CCTV Policy may be subject to disciplinary proceedings.

10.2 Breach of the CCTV Policy, Procedure or any aspect of confidentiality by individuals with specific responsibilities under the terms of the CCTV Policy and Procedure may be subject to Cove UK's Team Disciplinary Policy.

10.3 Any unauthorised use or abandonment of the control room, its systems and/or equipment, for any purpose whatsoever, (apart from evacuation in an emergency) may amount to gross misconduct under Cove UK's Team Disciplinary Procedure.

11. Complaints

11.1 Any member of Team or the general public wishing to register a complaint with regard to any aspect of the system may do so by contacting the Resort Director or Head of Security in the first instance. Data Protection concerns may be referred to the General Manager.

1.2 Should the matter remain unresolved, a formal complaint may be submitted to the Resort Director.

Annex B

Declaration of Confidentiality

Cove UK CCTV System

I, (……..……..…….... D.O.B ……...……...) am employed by (..... ……..……) in the capacity of ……..…… to perform the duty of CCTV Control Room Operator /Supervisor/Manager. I have received a copy of the Code of Practice and/or the CCTV Procedural Manual in respect of the operation and management of that CCTV System.

I hereby declare that:

I am fully conversant with the content of that CCTV Code of Practice/Procedural Manual and understand that all duties which I undertake in connection with my employment must not contravene any part of the current code of practice, or any future amendments of which I am made aware. If now, or in the future, I am or become unclear of any aspect of the operation of the system or the content of the code of practice, I undertake to seek clarification of any such uncertainties.

I understand that it is a condition of my employment that I do not disclose or divulge to any individual, firm, company, authority, agency or other organisation any information which I may have acquired in the course of, or for the purposes of, my position within the CCTV control Room. I also understand this undertaking will apply for a period of one year after the cessation of my employment in connection with the CCTV control room.

In appending my signature to this declaration, I agree to abide by the Code of Practice/Procedure Manual at all times. I also understand and agree to maintain confidentiality in respect of all information gained during the course of my duties, whether received verbally, in writing or any other media format - now or in the future.

Signed: .....

Print Name: .....

Witnessed: ..... Position: .....

Dated the ..... day of .....

Maintenance Log – External CCTV Cameras

Camera 1			
Camera Type		**Camera Location**	

Date of Fault	Description	Security Ref	Date of Repair	Remarks

Security Control Room CCTV Equipment – General

Date of Fault	Description	Security Ref	Date of Repair	Remarks

Maintenance Log – Control Room Recording Equipment

Equipment		Function	
Serial Number			
Date of Fault	Description	Sec Ref	Date of Repair

Maintenance Log – Internal Recording Equipment

Equipment		**Function**	
Serial Number		**Cameras**	
System Owner			

Date of Fault	Description	Date of Repair	Remarks

DIGITAL CCTV EVIDENCE REGISTER Sheet Ser No_____

MASTER	Serial No	
COPY	Serial No	

DVD PRODUCTION	
Date Produced	
Produced By	
Signature	

ISSUE DETAILS			
Issued By		Issued To	
Date		Date	
Signature		Signature	

Both Master & Working Copies to be Issued.

RECORDING DETAILS			
Recorder Location			
Camera No(s)		Date & Time of Incident	
Incident No/Reference			
Brief Details			

Notes:

- Data Destruction Register is to be completed when the DVD's/Memory Sticks are returned to Security and no longer required for evidential purposes.
- All DVDs/Memory Sticks that fail to record should be recorded in the Data Destruction Register and then destroyed
- **No DVD/Memory Stick is to leave the Control room unless it is signed for.**

DATA DESTRUCTION REGISTER

DESTRUCTION NOTES

1. **DVD/CD/Memory Stick**

a Data Destruction Register is to be completed when the DVDs/CD/Memory Sticks are returned to Security and no longer required for evidential purposes.

b Details of all DVDs/CD/Memory Sticks that fail to record, are to be recorded in the Data Destruction Register and then destroyed .

c No DVD/CD/Memory Stick is to leave the Control Room unless it is signed for.

d Score the disk with an abrasive; the disk should then be snapped/bent in half to prevent use. Render the Memory stick unusable.

2. PRINTED MEDIA

a Data Destruction Register is to be completed when printed media (Images) are returned to Security and no longer required for evidential purposes.

b Details of all Still Images that are not required or are poor quality, are to be recorded in the Data Destruction Register and then destroyed.

c No Image is to leave the Control room unless it is signed for.

d All printed media (still images/reports etc) are to be destroyed by shredding.

Sheet No……..

DATA DESTRUCTION REGISTER				
Ser	Date	Data Type/Serial No	Destroyed By	Signature

Annex D

SECURITY CONTROL ROOM –EVACUATION PROCEDURE

In the event that the Security Control Room is to be evacuated in an emergency the following guidelines are to be followed by the Control Room Officer.

SHORT TERM EMERGENCY EVACUATION

1. Inform all radio call signs on Channels 1 that you are evacuating the control room.
2. Collect two (2) radios and the Emergency Log Book. This will maintain radio communications and a written record of events.
3. If time allows, secure all windows.
4. If time allows, log off desktop PC and switch off all monitors.
5. Leave control room ensuring the door is locked to prevent unauthorised access.

LONG TERM EVACUATION

1. Inform all radio call signs on Channels 1 hat you are evacuating the control room and moving to …(alternate location?) confirmed by Resort Director or Head of Security Manager/Supervisor.
2. Transfer forward telephones to temporary Ext number.
3. Collect all available radios/chargers and the Emergency Log Book. This will maintain radio communications and a written record of events.
4. If time allows, secure all windows.
5. If time allows, log off desktop PC and switch off all monitors.
6. Leave control room ensuring the door is locked to prevent unauthorised access.

In the event access is required to the Control Room by the Emergency Services, they should be accompanied by a Security Officer unless the situation is deemed too dangerous. If that is the case then the Emergency Services should be allowed unaccompanied access.