Bournemouth University	Document Title: Section: Procedure Location: Author: Reviewer: Version Number: Date Created / Last Amended: Amended By: Document Review:	CCTV Policy & Procedures Strategic Documents Estates / Private / Soft Services/Strategic Security Documents Head of FM / Deputy Head of Legal Services Dir Estates Version 1 04/03/2016 Rebecca McPhee January 2018, then annually

BOURNEMOUTH UNIVERSITY
CCTV Policy & Procedures

CONTENTS

Section

Appendices

Bournemouth University
CCTV – Policy and Procedure

1. Introduction

1.1. Overview

1.1.1. This policy is intended to regulate the management, operation and use of closed circuit television (**CCTV**) systems at Bournemouth University (the **University**). It outlines the standards the University expects those responsible for and using CCTV systems to observe. Breach of this CCTV Policy and Procedures may involve breach of the University's Data Protection Policy for Staff and BU Representatives (**BU Data Protection Policy**).

1.1.2. The University operates a number of CCTV systems. The primary CCTV system operates cameras that link to a central control room in Poole House reception for Talbot Campus and to the central control room at Studland House reception for Lansdowne Campus. Secondary systems are operated by faculties and professional services elsewhere within University premises to respond to particular identified needs. These may be security needs, educational needs or other needs identified in accordance with this policy by the person responsible for the system.

1.1.3. This policy does not apply to recording devices, presently the Panopto (previously Echo360) system, used to record lectures or seminars in accordance with the procedures for such lectures or seminars.

1.1.4. Other use by Faculties, for example, use of CCTV systems for general teaching and evaluation is within the scope of this policy. So, within the scope of this policy are TV studio recordings and recordings of practice sessions within the Faculty of Health & Social Sciences. However, staff (and students when with staff) may view recorded footage relating both to them and current teaching and evaluation activity without following the procedures in paragraph 5.3 below: otherwise paragraph 5.3 will apply to any request to view recorded footage.

1.1.5. Nothing in this policy is intended to limit the effect of the BU Data Protection Policy. Failure to comply with the Data Protection Act 1998 can result in criminal liability. In addition, breach of the BU Data Protection Policy, and its associated procedures in force from time to time, may constitute a disciplinary offence for staff.

1.1.6. The Estates department will review this policy annually and, if legislative changes have been introduced, in consultation with the University's Legal Services department. The Estates department will disseminate any update to this policy.

1.1.7. The Head of Facilities Management is accountable for the operation of the primary system. Accountability for the operation of each secondary system rests with the relevant Director of Professional Service or the Director of Operations within faculties (the **Accountable Person**). The secondary systems are administered by the staff identified at Appendix 1.

1.2. Objective

This policy aims to:

1.2.1. Incorporate and build upon the principles of nationally accepted CCTV good practice.

1.2.2. Encompass, where appropriate, the characteristics of both an operating procedure and a code of practice document.

1.2.3. Evolve in line with technological, cultural and legal changes by means of a regular review.

1.3. Systems in operation

1.3.1 Each Accountable Person identified at Section 1.1.7 must provide accurate and up to date information on the location, use and management of all secondary systems to the Soft Services Manager, Estates. This must be done **annually** by 1 December and whenever systems are added to or removed, in each case using the form at Appendix 2.

1.3.1. The **primary system** is operated by:

Bournemouth University (Estates)
PG80 Poole House
Talbot Campus
Fern Barrow
Poole BH12 5BB

Tel: 01202 65001
Email: sbaylis@bournemouth.ac.uk

The primary system is administered by the Soft Services Manager, whose contact details are above. Any comment about the primary system should first be directed to the Soft Services Manager.

1.4. Who is covered by the policy?

1.4.1. This policy covers all staff who operate a CCTV system or process the data captured by it.

1.4.2. Any third parties who have access, on behalf of Bournemouth University, to a CCTV system and data are also required to comply with this policy.

1.5. Purpose and legitimacy of each scheme

1.5.1. The purpose of the primary CCTV system is to:

- help secure a safer environment for staff, students and visitors to Bournemouth University and, in each case their property;
- support the smooth running of the University's properties, including car parks;
- support the University and the Police in preventing and detecting crime and disorder;
- assist in the identification, apprehension and prosecution of offenders; and
- protect the University's assets.

2. General Principles

2.1. All BU Systems

2.1.1. The CCTV systems will be operated fairly, lawfully and only for stated purposes. All the data protection principles in Part I of Schedule 1 to the Data Protection Act 1998 will be respected in the operation of CCTV systems and the treatment of data derived from them.

2.1.2. Use of CCTV must always be for one or more specified purposes in pursuit of legitimate aims and necessary to meet that that or them, as applicable.

2.1.3. The CCTV systems will be operated with due regard to the privacy of each individual recorded.

2.1.4. Where individuals might reasonably have a heightened expectation of privacy, cameras will only be used in the most exceptional circumstances and in the least intrusive way consistent with meeting the objective.

2.1.5. The interests of staff, students and visitors will be protected by maintaining the security of data captured and ensuring that appropriate operational procedures are created and followed in accordance with this policy.

2.1.6. Each CCTV operator and person who has access to the recorded data will be issued with a copy of this policy by the relevant Accountable Person. They must become fully conversant with it and comply with its contents. Any query about its requirements it may be referred to the University's Legal Services department: legalservices@bournemouth.ac.uk. All operators for the primary system must be SIA licenced. Training for all people who have access to recorded data is the responsibility of the relevant Accountable Person. Training records are to be retained within departments.

2.1.7. Staff, students and visitors to the University will be informed of CCTV operations by means of prominently displayed signs located at the entrance to and, where appropriate, also inside the surveyed area. The less expected the location of CCTV cameras, the more prominent the sign will be. The system administrator for either the primary or the relevant secondary system must ensure that signage is correctly located and suitable.

2.1.8. As a general rule, the University will not operate sound recording CCTV. Where our CCTV equipment is able to record sound, this facility will usually be disabled. Each installation with sound recording capability will be identified by sign expressly stating this.

2.2 Primary System

2.2.1 For the primary system, operated by Estates, audio recordings must be authorised by the Soft Services Manager and should only be used in exceptional situations such as:

- audio based alert systems, provided that conversations are not recorded and operators are not listening in;
- two-way audio-feeds from designated "help points" activated by the individual requiring assistance;
- where recording is triggered by a particular threat.

In each case signs must make it very clear that audio recording may be carried out.

2.3 Secondary Systems

2.3.1 Each secondary system must have a written procedure for when recording of sound may be undertaken. Where sound recording is not linked to any crime or security purpose, the procedure must set out how those potentially affected by sound recording will be notified that it is active.

2.3.2 Subject to any exceptions expressly noted, the requirements in sections 2 to 6 of this policy apply to the primary and all secondary systems.

2.3.3 Any Accountable Person, system administrator or operator who has any concern about whether their system, or its method of operation, complies with this policy must contact the University's Legal Services department: legalservices@bournemouth.ac.uk for advice.

2.4 Installing new cameras or changing existing ones

2.4.1 Any proposal to install new cameras or change existing cameras must be notified to the Soft Services Manager, whose approval is required before any such installation or change. This is to:

- protect the University against risk of breaching applicable law;
- ensure co-ordination of cameras; and
- so that any necessary associated physical security measures can be discussed.

2.4.2 **Failure to obtain approval may be reported and actioned under the University's disciplinary procedure**.

2.4.3 Any proposal to install new cameras or change exiting ones must explain, consistently with the Surveillance Camera Commissioner's June 2013 Code of Practice and emerging good practice:

- the specific purpose for the installation, consistent with the purposes set out in paragraph 1.5 above;
- why that installation is necessary;
- alternatives, such as door locks, that have been considered, and why they are not sufficient or practicable (or applicable, in the case of educational CCTV installations);
- the specification of the equipment, which must:
  - include face-blurring capability to enable response to subject access requests under the Data Protection Act 1998 (see next section for technical requirements for current systems);
  - produce images and information of suitable quality for the criminal justice system to use without enhancement; and
  - include encryption of any wireless transmission to recording devices;

- how privacy intrusion is minimised, for example, electronic controls over field of view if wider than justifiable area of surveillance;

- proposed signage arrangements consistent with paragraphs 2.1.7 and 2.1.8 above and 3.2 below;

- (secondary systems) who will be responsible for operation of the system, including back-up arrangements to cover leave etc.; and

- (secondary systems) for the recordings:
  a) where they will be kept;
  b) the physical security arrangements to prevent unauthorised access;
  c) access arrangements to the recordings;
  d) incident management procedures (see guidance below); and
  e) the period, together with justification, for which recordings will be kept.

  By way of guidance, recordings need to be deleted once the purpose for keeping them has been discharged. The University's expectation is that:

  - a local procedure will be in place for relevant incidents to be reported swiftly to the system administrator, and relevant footage then burned to permanent media where likely to be required for future action within the University or by relevant third parties, including the police and the University's insurers;

  - any such permanent footage must be: a) kept securely to prevent unauthorised access; and b) destroyed once the purpose for which it is kept has been discharged. Examples of the latter would be the end of disciplinary proceedings and the end of the retention period for filmed assessments. The Legal Services department are happy to take custody of relevant footage in appropriate cases – contact legalservices@bournemouth.ac.uk;

  - a local procedure will be in place for promptly reporting relevant incidents to the Soft Services Manager, to Legal Services (legalservices@bournemouth.ac.uk) and, if relevant, the Human Resources department and the University's Insurance Officer; and

  - recordings (except those burned to permanent media) will not normally be kept for more than 30 days, although a greater period is acceptable provided it can be justified.

2.4.4 As soon as any secondary system is installed or changed, the form at Appendix 2 is to be completed by the relevant Accountable Person and sent to the Soft Services Manager, Estates.

3 Technical and operational standards

3.1 Cameras

3.1.1 Any new installation must comply with generally accepted standards for CCTV equipment, and, in particular, must offer sufficient resolution of image (and sound, if applicable) to meet the purpose for which it is installed.

3.1.2 Where at 1 June 2016 CCTV systems record images and do not provide for face blurring where disclosure of personal data is sought otherwise than for purposes falling within section 29 of the Data Protection Act 1998 (broadly, policing and allied activity), the operators of the systems must either:

- decommission the systems no later than 31 December 2016 and put in place alternative measures to meet the objectives sought to be achieved by the CCTV installation; or

- create an action plan to migrate to such technology no later than 31 July 2017. This recognises the need for funding requirements for improved technology to be reflected in Delivery Planning arrangements, procurement and installation of new technology.

3.2 Signage

3.2.1 Each CCTV camera sign will clearly set out the purposes for which the camera operates, consistent with the purposes set out in paragraph 1.5 above.

3.2.2 Each CCTV camera sign will clearly identify the operator of the CCTV camera. A telephone number should be provided to enable students, members of staff and visitors to contact the operator directly in relation to the CCTV camera in question.

3.3 Activation period

3.3.1 The CCTV cameras will record for the period needed to meet the purpose(s) for them and no longer. This may be 24-hours per day, or a lesser period. In particular, certain cameras may be set to capture images (and, if applicable, sound) only if activity in unauthorised areas or at unauthorised times is detected.

3.3.2 Every recording must be date and time stamped by the recording device. The accuracy of the date and time stamp must be periodically checked, and appropriate written record of checks kept.

3.4 Storage

3.4.1 No CCTV camera shall record to any cloud-based storage. All storage must be on the University's premises.

3.4.2 Any wireless transmission of CCTV images and sound to permit storage must be suitably encrypted to protect them from interception.

3.5 Access to, and security of, CCTV rooms *(primary system and any applicable secondary system)*

3.5.1 Access to CCTV control rooms will generally be limited to the security team CCTV operators and direct management.

3.5.2 Visitors to the control rooms will only be admitted where:

- directly related to the stated purposes for CCTV capture;
- undertaking work on the equipment, or the room itself;
- providing training or supervision to operators.

3.5.3 All visitors to control rooms will be subject to suitable checks and (except for police visitors) authorisation by the system administrator.

3.5.4 Unless access to the CCTV equipment is physically restricted (e.g. in a locked room, without possibility of observing the equipment from outside), an authorised operator will be present at all times when the CCTV equipment is in use.

3.5.5 Except as required or permitted by law, only those members of staff with responsibility for using the equipment will have access to the CCTV operating controls. Those operators have primacy of controls at all times.

3.6 Audit trail and other operational procedures

3.6.1 **By 31 December 2016, each system (primary and secondary) must have documented information for each camera mirroring paragraph 2.4.3 above**.

3.6.2 CCTV systems may be subject to internal audit in due course.

3.7 Incidents

3.7.1 For the primary system, incidents observed by the CCTV operator and judged potentially useful for investigative and evidential purposes or for future CCTV system assessment and evaluation **must be notified promptly** to the Soft Services Manager, who will then determine whether they should be burned to permanent media. These will include any instances where there appears to be threat or harm to person or property, including cases of tripping or slipping.

Please note that primary systems are not continually monitored, but an operator may be directed to look at live or recorded CCTV if an incident is known to be occurring or has been notified.

3.7.2 The police should be contacted (via 222) if the CCTV operator notes any 'live' incident that may need their assistance. The CCTV operator must alert the Soft Services Manager to such incidents as soon as possible thereafter.

3.7.3 The Soft Services Manager will report any such incidents promptly to Legal Services (legalservices@bournemouth.ac.uk) and, as relevant, the Head of Student Services, Assistant Director of Human Resources and the University's Insurance Officer. Any of these may require the relevant recording to be burned to permanent media.

3.7.4 Any such permanent media must be kept securely to prevent unauthorised access. The Legal Services department are happy to take custody of relevant footage in appropriate cases.

4. Civil liberties

4.1 Civil liberties must not be breached by the operation of the CCTV scheme. To that end systems must be operated:

- with utmost integrity;
- only in accordance with the stated purposes; and
- specifically not in any way that may be perceived as being motivated by personal prejudice.

4.1.2 The University may require any manager, administrator or operator of a CCTV system to justify their interest in, and recording of, any particular individual, group of individuals or property at any time. The University reminds relevant parties in that respect both of its Dignity and Respect (Harassment) Policy and Procedures and that harassment may amount to a criminal offence.

5. The Data Protection Act 1998

5.1 Personal Data

5.1.1 CCTV recordings are covered by the Act, as is information about individuals which is derived from the images – for example, vehicle registration numbers.

5.1.1. As data controller, the University must comply with the Act when processing personal data. This includes capturing, transmitting, storing and any disclosure. This applies equally to the primary system and to each secondary system.

5.1.2. Each system, and its operation, must comply with the following eight principles. This policy has been written to try to address these. Subject to the transitional provision above for face-blurring technology, each Accountable Person is accountable within the University for any non-compliance of their system with the Act.

The principles are set out in more detail here: https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/ but, for summary:

- personal data shall be processed fairly and lawfully, and with the appropriate conditions for processing (set out in Schedules to the Act) being met;
- personal data shall be obtained (CCTV capture in this context) only for one or more specified and lawful purposes (the purposes for the rest of this summary), and shall not be further processed in any manner incompatible with the purposes;
- personal data shall be adequate, relevant and not excessive (for example, no unjustified recording of sound in addition to image) in relation to the purposes for which they are processed;
- personal data shall be accurate (for example, accurate time stamps on recordings);
- personal data shall not be kept for longer than needed for the purposes;
- personal data shall be processed in accordance with the data subject's rights under the Act;
- appropriate technical and organisational measures shall be taken against unauthorised or unlawful personal data processing and against accidental loss or destruction of, or damage to, personal data; and
- personal data shall not be transferred outside the European Economic Area unless the place to which the transfer takes place ensures adequate protection for the rights and freedoms of data subjects in relation to the processing of personal data.

5.2 Requests for imagery from data subjects

5.2.1 Where operators or system administrators receive a request from a member of staff, a student or a visitor in relation to their personal data (images or sound recordings of them or associated with them, for example, of their car) recorded on a CCTV system, they should refer the matter to the Information Office, c/o Legal Services.

5.2.2 The contact details for paragraph 5.2.1 are:

E: freedomofinformation@bournemouth.ac.uk

T: 01202 961211

Information Officer
Legal Services
Bournemouth University
2nd Floor, Melbury House
1-3 Oxford Road
Bournemouth
BH8 8ES

5.2.3 BU's Data Protection Policy applies equally to CCTV recordings as it does to other personal data.

5.3 Internal requests for imagery that is not own personal data

5.3.1 Any staff member who wishes to review a CCTV recording, for example, to investigate an incident, must approach the system administrator. System administrator details are set out in Paragraph 1.3 above and Appendix 1.

5.3.2 The staff member must explain the reason for the request, and must provide the reason in writing if required by the system administrator. The system administrator will decide whether the request is consistent with the purposes for which the CCTV system was operated. If satisfied on this front, the staff member will be permitted to view (and, if applicable, listen to) the recording.

5.3.3 Any dispute on access will be referred to the Legal Services department (legalservices@bournemouth.ac.uk) for advice. The requesting staff member and system administrator may be required to put their reasons in writing.

5.4 CCTV recording on permanent media

5.4.1 Other than system administrators, and operators under their direction, the only persons authorised to receive CCTV recordings on permanent media are:

- members of the Human Resources department authorised for these purposes by the Assistant Director of Human Resources;
- (recordings relating to students only) members of the Student Services and Student Administration departments responsible for student complaints and authorised for these purposes by, as the case may be, the Head of Student Services or Head of Student Administration;
- the Director of Estates, the Head of Facilities Management, the Soft Services Manager and any other members of the Estates department authorised for those purposes by the Director of Estates;

- members of the Legal Services department and others authorised for those purposes by them, for example solicitors acting for the University's insurers;

- the University's Insurance Officer; and

- the police (where procedures below have been followed).

5.4.2 System administrators will comply with directions from any of the above for supply of relevant recordings. Any dispute over supply will be referred to Legal Services for resolution; and Legal Services will liaise with the University Executive Team as necessary.

5.5 Requests from the police to either see recordings or be supplied with recordings on permanent media

5.5.1 Unless there is a statutory duty to disclose, the University doesn't have to disclose information without a court order. Members of staff should not be bullied into disclosing personal data if there is any doubt as to the validity of the request. It is, however, the University's expectation that it will be able to work co-operatively with the police to promptly help them in the execution of their duty.

5.5.2 The police have standard forms (commonly known as section 28 or section 29 forms) for requesting personal data in accordance with guidance issued by the Association of Chief Police Officers.

5.5.3 The form should certify that the information is required for an investigation concerning national security (a section 28 form), the prevention or detection of crime or the apprehension or prosecution of offenders (a section 29 form) and that the investigation would be prejudiced by a failure to disclose the information.

5.5.4 Subject to the emergency procedure discussed below, unless the request is in person (not over the telephone) from a member of the University's Safer Neighbourhood Team known personally to the system administrator or CCTV operator to be a member of that team, all police requests should be in writing.

5.5.5 Check any written request purporting to be from the police for authenticity. In particular, check any sending email address, and seek to verify via an alternative source if possible. For example, if possible check the switchboard telephone number and calling the relevant officer via that route.

5.5.6 Whether or not the request is from the University's Safer Neighbourhood Team, check the basis for disclosure. In particular:

- be clear why not releasing the information sought would be likely to prejudice (that is, significantly harm) any attempt by the requester to prevent crime or catch a suspect; and

- you should only release the minimum data required to for the requester to be able to do their job.

5.5.7 If there is any doubt about the validity of a request you should not disclose the personal data and should contact Legal Services urgently for advice (legalservices@bournemouth.ac.uk).

5.5.8 As soon as possible after the disclosure, make and retain a record of any disclosure made. Keep the request or court order received alongside this.

- Keep the record securely, by scanning and placing in the collaborative folder in the I-Drive under Estates/CCTV (Administrative support will be provided by the Soft Services Manager). Delete any other local copy of the record once lodged in the collaborative folder.

- The record should state the:
  - name of member of staff authorising the disclosure;
  - the recipient's name, serial number and force;
  - the time, date and reason for the disclosure (why the information was required and the grounds on which the information was disclosed);
  - any advice sought and received;
  - if known, name(s) of the affected staff or student(s);
  - details of the information that was disclosed.

5.6 How to deal with emergency situations involving the police

5.6.1 An emergency situation is one where there is a reasonable belief that there is a life or death situation or a significant risk of serious harm (either to a staff member, student or any other person).

5.6.2 Where information is required in an emergency, unless the request has come from an individual you are used to dealing with (such as a member of BU's Safer Neighbourhood Team), ask the caller to provide a switchboard number and call them back through the organisation's switchboard before providing any personal data.

5.6.3 Where personal data is disclosed, you should make a record of the enquiry and the information disclosed. You may find it helpful to run through the points at paragraph 5.5.8 above when making a record of the disclosure. The record should be retained as for a normal police request (see paragraph 5.5.8 above).

6.0 Staff training

6.1 General

6.1.1 The University offered training in 2015 to all staff known to be administrating a system or operating it.

6.1.2 The Estates team will provide an initial induction to all new staff allowed access to the primary system.

6.1.3 The Estates team will provide regular training to all staff operating the primary CCTV system to ensure that they comply with this policy, the law and the ICO's CCTV Code of Practice 2015 (the **Code**). The Code is available here: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

6.1.4 For secondary systems, the relevant Accountable Person through the respective nominated administrators identified at 1.1.7 and Appendix 1 is responsible and accountable for sourcing appropriate training for all staff using their CCTV systems. The University expects the training for secondary systems to be no less than offered by Estates to those administrating and operating the primary system.

6.1.5 The level of training required will vary depending upon skills and knowledge already acquired, the nature of the system and its operation and the working environment (how secure, etc.).

6.1.6 System administrators will ensure that for themselves and each operator they:

- assess the particular training needs.
- explain the training objectives, as set out in paragraph 6.1.3 above and 6.2 below as a minimum;
- establish the training content;
- choose an appropriate delivery method and monitor and evaluate delivery; and
- oversee the provision of continuous development and refreshment.

6.1.7 Training records must be kept and made available for inspection by internal audit as needed.

6.2 Training programme content

6.2.1 As noted in paragraph 6.1.3 above, training needs to ensure system compliance with this policy, the law and the Code. This is likely to include, without limitation:

- the necessary justifications for each camera, and associated audit trail;
- general arrangements for accessing CCTV recordings;
- what to do if requests for access come from the police;
- the BU Data Protection Policy;
- the Data Act 1998 as it applies to CCTV systems; and the Code.

Appendix 1

BOURNEMOUTH UNIVERSITY CCTV Policy & Procedures 2016

Details of Secondary Systems

Faculty / Professional Service	Accountable Person	Address	Administrator	Contact Details (Phone & e-mail)	Remarks / Number of secondary CCTV assets in use?
Faculty of Media & Communication	*School Director Of Operations*	*Faculty of Media & Communication Bournemouth University Weymouth House Talbot Campus Fern Barrow Poole BH12 5BB*	*Support Group Manager*	*Tel: 01202 961293 kheyward@bournemouth.ac.uk*	*20 cameras for security & safety management*
Faculty of Science and Technology	*School Director Of Operations*	*Faculty of Science & Technology Bournemouth University Poole House Talbot Campus Fern Barrow Poole BH12 5BB*	*Technical Support Manager*	*Tel: 01202 965497 gtoms@bournemouth.ac.uk*	*28 cameras for security & safety management*
Faculty of Management	*School Director Of Operations*	*Faculty of Management Bournemouth University Poole House Talbot Campus Fern Barrow Poole BH12 5BB*	*Resource Planning Manager*	*Tel: 01202 965156 lbrooks@bournemouth.ac.uk*	*To be confirmed by Faculty*
Faculty of Health & Social Sciences	*Faculty Director of Operations*	*Faculty of Health & Social Sciences Bournemouth University Royal London House Christchurch Road Bournemouth BH1 3LT*			*20 cameras for educational purposes*

The Student Union Bournemouth University is not covered by this CCTV policy, however, details of known systems that they operate are listed below					
The Old Fire Station	*General Manager*	*Student Centre* *Bournemouth University* *Poole House* *Talbot Campus* *Fern Barrow* *Poole* *BH12 5BB*	*Venue Manager*	*Tel: 01202 963889* *scox@bournemouth.ac.uk*	*To be confirmed by SUBU*

Appendix 2

BOURNEMOUTH UNIVERSITY CCTV Policy & Procedures

To be completed by each Accountable Person (one per Faculty and Professional Service) as specified in the CCTV Policy & Procedures and **returned to the Soft Services Manager, Estates annually by 1 December** and when any changes occur

Nil responses are required

Faculty / Professional Service:				
Accountable Person	**Name:**		**Post:**	
	Telephone		**E-mail:**	

Camera Name & Location (room number)	**Coverage**	**Purpose**	**Date Installed / Removed**	**CCTV Administrator (name and contact detail)**	**Where is CCTV data stored?**	**Who has access to the data?**	**Remarks**

Signed…….. **Dated……..**
Accountable Person