Policy for Surveillance Camera System

Solent NHS Trust policies can only be considered to be valid and up-to-date if viewed on the intranet. Please visit the intranet for the latest version.

Purpose of Agreement	To provide guidance over the use and management of Closed Circuit Television Cameras installed in Solent NHS trust Sites
Document Type	[X] Policy [ ] SOP [ ] Guideline
Reference Number	Solent NHST/Policy/IG08
Version	Version 3
Name of Approving Committees/Groups	Policy Steering Group, Trust Management Team Meeting
Operational Date	March 2020
Document Review Date	March 2023
Document Sponsors (Job Title)	Chief Finance Officer Deputy CEO : Security Management Director (SMD)
Document Manager (Job Title)	Information Governance Lead / Accredited Security Management Specialist (ASMS)
Document developed in consultation with	Health & Safety Committee
Intranet Location	Business Zone / Policies, SOPs and Clinical Guidelines
Website Location	Publication Scheme / Policies and Procedures
Keywords (for website/intranet uploading)	Surveillance Camera System, Security, Closed Circuit Television Camera, (CCTV) Subject Access Request, Policy, IG08

Amendments Summary:

Amend No	Issued	Page(s)	Subject	Action Date
1	01 Mar 16	Title	CCTV will now be known as Surveillance Camera System	01 Mar 16
2	28/11/2019	10	Monitors to be switched off when not in use	March 2020
3	28/11/2019	8	Addition of USB to list of Media types	March 2020
4	28/11/2019	7	Update of the ASMS to list of person for consultation of covert surveillance	March 2020
5	28/11/2019	4	Addition of camera commissioner	March 2020

Review Log

Include details of when the document was last reviewed:

Version Number	Review Date	Lead Name	Ratification Process	Notes
1				
2				
3	28/11/2019	ASMS		

Executive Summary

This policy gives comprehensive guidance to Management and staff trained as Authorized users of any Closed Circuit Surveillance Camera System (CCTV) in use at any Solent site. The policy is an essential part of ensuring the safety and security of CCTV footage recorded of staff, Visitors and patients utilising Solent NHS Trust facilities.

Policy for Surveillance Systems

1. INTRODUCTION & PURPOSE

1.1 Introduction

1.1.1 This policy aims to support staff in the safe implementation and use of Surveillance Cameras in order to protect all staff, patients and public using Trust premises. The Trust acknowledges its responsibility to protect staff, patients and the public who use the services whilst on Trust property while protecting the freedom of all individuals within the standards of the Human Rights Act, GDPR General Data Protection Rules and other guidance which may be issued by the Information Commissioners Office or Surveillance camera commissioner.

1.1.2 As part of our commitment to ensure the delivery of a high quality and safe working environment for our staff, patients and visitors who access our facilities, we will;

- Comply with relevant legislation pertaining to the installation and use of surveillance cameras and recording equipment.
- Establish a surveillance camera management system to correctly identify footage. Store it securely and when required provide continuity of evidence.
- Maintain the surveillance camera system, adopting best practice where possible and strive to continually improve the monitoring control process through monitoring and assessments.
- Provide clear guidance to relevant staff to ensure they understand the reasons, benefits and legal implications of the use of surveillance camera.

1.1.3 Purpose

1.1.4 This policy will assist operators of surveillance camera systems in Solent NHS Trust to understand their legal obligations whilst also reassuring the public and patients using our services about the safeguards in place in relation to compliance with the Data Protection Act 2018 General Data Protection Regulations (GDPR), Human Rights Act 1998, Regulation of Investigatory Powers Act 2000, Surveillance Camera Code of Practise 2014, The Surveillance Camera Commissioner code of practice 2014, The Caldicott Report 1997, Care Quality Commission Using Surveillance 2019 and other relevant legislation and guidance. It is anticipated that compliance with the this Policy & Procedure will ensure that;

- Surveillance Camera systems are not abused or misused
- Surveillance camera is correctly and appropriately installed and operated
- Surveillance camera equipment will only be used by Authorised persons

1.1.5 Surveillance Camera will be used to help prevent and detect crime, including protection of Trust premises and to pursue the prosecution of offenders. In certain clinical situations the use of cameras is forbidden.

1.1.6 Surveillance Camera may assist in the robust monitoring of areas that may need observing to maintain levels of safety and security to those people utilising the Trusts facilities.

1.1.7 Surveillance cameras alone will not prevent staff or patients being assaulted or property from being stolen or damaged. However, combined with good local systems and procedures as part of a holistic solution, it can help to prevent and deter security-related incidents, as well as provide evidence to assist investigations of incidents.

2 SCOPE

2.1 This policy applies to all bank, locum, permanent and fixed term contract employees (including apprentices) who hold a contract of employment or engagement with the Trust, and secondees (including students), volunteers (including Associate Hospital Managers), Non-Executive Directors, and those undertaking research working within Solent NHS Trust, in line with Solent NHS Trust's Equality, Diversity and Human Rights Policy. It also applies to external contractors, Agency workers, and other workers who are assigned to Solent NHS Trust.

3. ROLES & RESPONSIBILITIES

3.1 **The Chief Executive** is ultimately responsible for the manner in which the Trust implements the Surveillance Camera policy and adheres to agreed Data Protection requirements.

3.1.1 **Finance Director / Security Management Director (SMD)** responsible for the overall management of the Trusts Surveillance Camera system and ensuring this policy and Codes of Practise issued by Information Commissioner (IC) are complied with.

3.1.2 **Information Governance** is responsible for providing advice to the Accredited Security Management Specialist (ASMS) and systems managers who are designated as the responsible persons on the disclosure of material in response to subject requests. They will also ensure the use of Surveillance Camera equipment on Trust premises has been registered with the Information Commissioner and the notification for the purpose is maintained.

3.1.3 Information Governance is responsible for ensuring that Surveillance Camera arrangements comply with the Data protection Principles and GDPR regulations which state that data must be;

- Fairly and lawfully processed.
- Processed for limited purpose and not in any manner incompatible with those purposes.
- Adequate, relevant and not excessive.
- Accurate
- Not kept any longer than necessary.
- Processed in accordance with individual rights.
- Secure at all times.
- Not transferred to locations without adequate protection.

3.1.4 The system managers and ASMS in liaison with Information Governance will ensure that;

- Appropriate access and reasons for using Surveillance Camera or similar surveillance equipment.
- Documentation of the assessment process and the reasons for installation.

- Ensure documentation the person(s) or organisation (s) responsible for ensuring the day-to-day compliance with requirements of the Code of Practise.
- Establishment and document security and disclosure policies and procedures for Surveillance Camera.

3.1.5 **Accredited Security Management Specialist (ASMS)** is responsible for providing advice on the suitability and provision of access and material to law enforcement agencies including Police, HR as well as advising on the provisions of the Surveillance Camera Code of Practise and the provision of new or additional Surveillance Camera equipment, in association with the Information Governance Manager.

3.1.6 **Staff Trained in Public Space Licence (holder of certificate)** is responsible for the safe operating of Surveillance Camera equipment on behalf of the Trust whilst carrying out their daily duties. The authorised person will be provided with clear instructions and guidance on how to operate the equipment safely and proficiently. They must complete a daily Surveillance Camera log (produced locally) ensuring that the date and time are checked for accuracy, a check that the cameras are working and that the quality of the recorded image is checked. Any faults must be reported immediately, or at the next practicable time, to their line manager.

4. PROCESS / REQUIREMENTS

4.1 Management review using a Surveillance Camera system can be seen as intrusive. It is essential that due consideration is given to the need to maintain privacy and dignity at all times. It is important to remember that Surveillance Camera is not the sole answer to all security and monitoring needs. Due consideration of other means of keeping staff, patients, visitors and property safe should be undertaken prior to settling on installing a new Surveillance Camera system.

4.1.1 Before installing a new Surveillance Camera system it will be necessary to establish the purpose of use for which the equipment is being purchased and installed.

4.1.2 Where people lack the mental capacity to understand, or consent, to the use of surveillance, clinical leads must make decisions in accordance with statutory principles of the Mental Capacity Act 2005.

4.2 LOCATION of SURVEILLANCE CAMERAS

4.2.1 There are three main areas of consideration when positioning Surveillance Camera;

- Public areas – These are areas around Trust property to which the public have unrestricted access e.g grounds, car park, main entrance etc. There should be valid reasons to position cameras at these locations such as staff and visitor safety and vehicle security but due consideration of the risk posed needs to take place.
- Communal Areas – These are shared areas on the Trust buildings foot print. They can include dayrooms, dining areas or corridors. Cameras can be placed in communal patient areas where safety of either people who use the services, staff or visitors justifies the positioning. It is central to any decision that, in line with the requirements of the Information Commissioners Office (ICO), a clear reason for installation is available. This could be in the form of a Risk Assessment highlighting incidents that have occurred within a specific area.

- Private Areas – Cameras should NEVER be installed within private areas such as any clinical areas, toilets, bathrooms or shower rooms.

4.2 2 Prior to any surveillance cameras being fitted within seclusion rooms/136 suite, the Operations Manager of the relevant department, in liaison with the ASMS, is to seek legal advice in regards to the impact of cameras within these areas under Article 8 of the Human Rights Act 1998 and, complete a Privacy Impact Assessment form and submit it to the head of Information Governance for approval.

4.3 COVERT RECORDING

4.3.1 Covert recording utilising a Surveillance Camera system, or additional cameras, will not be undertaken without any consultation through.

- ASMS
- Chief Finance Officer / Deputy CEO (SMD)
- Head of Risk and Litigation
- People Services (**HR**)

Any requests will be undertaken in accordance with the laws and legislation stipulated within the Regulation of Investigatory Powers Act 2000 (RIPA). Any covert surveillance will only be considered as a last resort.

4.3.2 In accordance with the Human Rights Act 1998, Article 8 states that 'All persons have a right to a private life' and, under the Mental Health Act 1983, Section 8.4 states 'Hospital staff should make a conscious effort to respect the privacy and dignity of patients as far as possible while maintaining safety, including enabling a patient to wash and dress in private'.

4.4 POSITIONING of CAMERAS

4.4.1 Cameras should not be hidden from view but positioned in locations where they are secure and protected from vandalism. Where practicable, cameras must be having the ability to set Privacy filters so that areas where cameras are covering neighbouring spaces are prevented from any visual intrusion.

4.4.2 CCTV Signs must be displayed informing staff, patients and visitors of the presence of a Surveillance Camera system.

4.4.3 Viewing monitors must be sited out of public/staff view, where the images can only be seen by the authorised staff.

4.5 SIGNAGE

4.5.1 All signage placed within the Trust premises and property must be placed so that the public can clearly see the signage and are immediately aware that they are entering a location that is covered by surveillance camera equipment. The signage must contain the following information;

- Identify the organisation responsible for the system i.e. Solent NHS Trust.
- The purpose of the system and why it will be recording images.
- Details of whom to contact regarding the system (e.g. Information Governance.)

4.5.2 The following wording is recommended on all signage;

These NHS premises are under CCTV Surveillance.
Images are being recorded and monitored for the Purposes
Of the prevention and detection of crime and for Public Safety

The scheme is operated by Solent NHS Trust and for Subject Access Requests
Or Queries please contact the:

Data Controller Via email On InformationGovernanceTeam@solent.nhs.uk
Or Call 0300 123 3919

Quoting Scheme ID on the sign: (add Hospital / Location)

4.6 QUALITY of IMAGES

4.6 .1 It is vital for a system that the images produced are of a sufficient quality to enable the recognition and identification of persons suspected of committing acts of unlawful intention.

4.6.2 All systems must be installed and maintained by appropriately certificated contractors. Upon installation all equipment is to be tested to ensure that only designated areas are covered by the cameras and high quality images are available in live and play back modes. All Surveillance Camera equipment should be serviced annually and maintained when required.

4.7 STORAGE & RETENTION of IMAGES

4.7.1 All recordings, whether CDR, DVDR, hard disc or Encrypted USB, must be traceable. There are several elements to this:

- All recordings must be logged and traceable. For Digital Video Recorders (hard disc) systems, this means ensuring the system is set up to record with a camera number, date and time stamp.

- All incidents requiring provision of images must be logged within the daily occurrence book and a signature gained from the authorised person receiving the recording.

- The ASMS or Information Governance Team must be contacted before any images are released to any third party.

4.7.2 A daily Surveillance Camera log must be completed by an authorised person, the date and time of the system should be checked for accuracy and a check that all cameras are functioning correctly.

4.7.3 If the cameras are not functioning correctly they must be immediately reported to the Trust approved specialist for repair or replacement.

4.8 MANAGEMENT of HARD DISC SYSTEMS

4.8.1 Images must not be retained for any longer than necessary, normally 28 days. Each site that has Surveillance Camera in situ must adhere to the Information Commissioners Code of Practice and the Department of Health Code of Practice for Record Management which

states that images can only be kept on a recording system for a maximum of 31 days. Once this time frame has expired the images must be erased. On most modern systems this will automatically be completed.

4.9. DISCLOSURE of IMAGES TO THE MEDIA

4.9 .1 The decision to release Surveillance Camera footage to the media in a non-Police situation can only be taken by the Chief Executive after consultation with the SMD/ASMS, Media Operations Team and Information Governance Team.

4.9.2 If it is decided that images will be disclosed to the media, images of those persons not involved in the incident must be disguised or blurred so that identification is impossible. If the system does not have this facility than an editing company will need to be established that will perform this function.

4.10 ACCESS BY DATA SUBJECTS

4.10.1 The Data Protection Act provides Data Subjects (persons to whom 'personal data' relates) with the right to access data concerning them, including images obtained by Surveillance Camera.

4.10.2 Requests for Data Subject Access should be made on the appropriate application form (Available from Information Governance and on this policy at ***(Annex B***) and submitted to the Trusts Information Security Manager.

4.10.3 Access and disclosure to images is only permitted if it supports the purpose of an investigation. Under these conditions the request should be made through the ASMS or Information Governance Team. In a time critical situation authorised staff can issue a copy of Surveillance Camera footage to the Police or other Government agency. The request form would then be submitted retrospectively.

4.11 SURVEILLANCE FOOTAGE FOR DISCIPLINARY PURPOSES

4.11.1 Only in the event that Surveillance Camera footage shows activity that gives rise to concern may it be considered during the investigatory stages of a formal disciplinary procedure. It may only be used in formal disciplinary hearings when relevant to the allegations against the staff member and can be shown to prove, or disprove, the accusations.

4.11.2 Activity where Surveillance Camera can be provided to a Human Resource investigation may include;

- Acts which constitute Gross Misconduct in accordance with Trust policy.
- Practices that seriously jeopardise the health and safety of other staff, patients or visitors.
- Inappropriate treatment of patients.

4.11.3 In cases where Surveillance Camera footage is used in a disciplinary hearing, the accused will be given the opportunity to review the Surveillance Camera footage and explain, or challenge its content.

4.11.4 If the Trust identifies Surveillance Camera footage/images relevant to formal proceedings, then the timescale (28 days) for the retention of Surveillance Camera footage/images shall

not apply. Footage/images retained for such purposes will be held for three (3) years following the completion of all disciplinary procedures, including any appeals process.

4.12 ACCESS, DISCLOSURE AND VIEWING OF SURVEILLANCE FOOTAGE BY THIRD PARTIES

4.12.1 Disclosure of recorded material will only be made to a third party in strict compliance with the Data Protection Act 2018 (GDPR) and any other relevant legislation, after authorised and served appropriate documentation is received by the Trusts ASMS or Information Governance Lead. (***Found at Annex C***)

4.12.2 All access by Third Parties, and the medium on which it's recorded, must be documented on the relevant forms (*found at Annex D*). Likewise, if access is refused this must also be documented.

4.12.3 Information on the documentation of issue must include:

- Date and time of request
- Description of incident
- Camera identifying incident
- Date and time on the image
- The reason why recorded medium was removed and/or crime/incident number
- Full details of person receiving the recording e.g Police number and home station
- Signature
- Date, location and method of destruction
- Details of person carrying out the destruction

4.13 VIEWING OF LIVE IMAGES

4.13.1 Viewing of live images must be restricted to authorised operators only, unless specifically authorised by the ASMS or Information Governance Manager. (In the case of an emergency, Police/Government Agencies can view without specific authorisation.)

4.13.2 Surveillance Camera monitors must be switched off when not in use and positioned when in use in a way that the general public, or unauthorised staff members, cannot view the images indiscreetly or inadvertently when passing.

4.13.5 Police or Government officials requesting access to images must complete Form (Annex D) or provide a DP2 form before images can be released.

4.14 REQUEST TO PREVENT PROCESSING

4.14 .1 An individual has the right to request a Prevention of Processing where not doing so is likely to cause substantial and unwarranted damage to the individual.

4.14.2 All such requests should be addressed to the Information Governance Manager who must provide a written response within 20 days of the initial request, setting out their decision on the request and the reasons why.

4.15 DISPOSAL of DOCUMENTATION

4.15.1 All documentation relating to the management and operation of a Surveillance Camera system, together with all request forms must be retained by the system manager for a

minimum of three (3) years after which destruction can only be authorised by the Information Governance Manager. All documentation must be disposed of as CONFIDENTIAL waste and be either incinerated or shredded by an authorised provider.

5. TRAINING

5.1 Training in CCTV will only be given to authorised persons who have a genuine need to have access to CCTV footage these authorised persons will be:

- Accredited Security Management Specialist (ASMS)
- Premises and Line Managers authorised by the ASMS to view
- Administration and other reception staff who are required to have access (assessed and authorised by the ASMS)
- Security Officers
- IG Lead

5.1.1 Any Training in the use of CCTV and Public Space Licence must be renewed every three (3) years to ensure that knowledge and ability is maintained.

5.1.2 Training will also be provided in any new CCTV software that has been installed as part of a Trust Programme to renew or update CCTV systems. This training will be undertaken by the company installing the software

5.1.2 Alerts when received must be shared with the trained staff so that they can ensure that their knowledge of the use of current devices is kept up to date.

6. EQUALITY IMPACT ASSESSMENT AND MENTAL CAPCITY

6.1 This policy has not identified any significant equality or diversity issues,

Equality impact assessment can be found at (Annex A)

7. SUCCESS CRITERIA / MONITORING EFFECTIVENESS

7.1 A review of the policy and procedures will be conducted every 3 years or when changes force an earlier review.

7.2 Premises Managers are to review local procedures to comply with all relevant policies involving suspect packages/devices.

7.3 The ASMS will continue to monitor ICO (information commissioner Office) and Camera Commissioner Guidelines as well as any changes to the GDPR and data protection rules.

7.3 All non-compliance of this policy must be reported to the ASMS via Ulysses stating when and where the non-compliance occurred so that it can be satisfactorily investigated

8. REVIEW

8.1 This document may be reviewed at any time at the request of either at staff side or management, but will automatically be reviewed 3 years from initial approval and thereafter on a triennial basis unless organisational changes, legislation, guidance or non-compliance prompt an earlier review.

9. REFERENCES AND LINKS TO OTHER DOCUMENTS & WEB SITES

9.1 The following items of legislation are relevant to this policy;

- Crime & Disorder Act 1998
- Criminal Justice & Public Order Act 1994
- Criminal Procedure & Investigation Act 1996
- Data Protection Act 2018 (GDPR)
- Human Rights Act 1998
- Private Security Industry Act 2001
- Police & Criminal Evidence Act 1984
- Regulation of Investigatory Powers Act 2000

9.1.1 The following external publications have helped the development of this policy;

- NHS Guidance on CCTV Systems
- Home Office CCTV Operational Requirement Manual 2009 (Publication 28/29)
- Information Commissioners Office
- Camera Commissioner 12 Guiding Principles

10. Glossary

10.1 **CCTV:** Closed Circuit Tele-vision
ASMS: Accredited Security Management Specialist
SMD: Security Management Director
GDPR: General Data Protection Regulations

Annex A

Equality Analysis and Equality Impact Assessment

Equality Analysis is a way of considering the potential impact on different groups protected from discrimination by the Equality Act 2010. It is a legal requirement that places a duty on public sector organisations (The Public Sector Equality Duty) to integrate consideration of Equality, Diversity and Inclusion into their day-to-day business. The Equality Duty has 3 aims, it requires public bodies to have due regard to the need to:

- **eliminate unlawful discrimination**, harassment, victimisation and other conduct prohibited by the Equality Act of 2010;
- **advance equality of opportunity** between people who share a protected characteristic and people who do not;
- **foster good relations** between people who share a protected characteristic and people who do not.

Equality Impact Assessment (EIA) is a tool for examining the main functions and policies of an organisation to see whether they have the potential to affect people differently. Their purpose is to identify and address existing or potential inequalities, resulting from policy and practice development. Ideally, EIAs should cover all the strands of diversity and Inclusion. It will help us better understand its functions and the way decisions are made by:

- **considering the current situation**
- **deciding the aims and intended outcomes of a function or policy**
- **considering what evidence there is to support the decision and identifying any gaps**
- **ensuring it is an informed decision**

Equality Impact Assessment (EIA) *see supporting guidance on pg 3*

Step 1: Scoping and Identifying the Aims

Service Line / Department	All Employees, Patients, Visitors	
Title of Change:		
What are you completing this EIA for? (Please select):	Policy	*(If other please specify here)*
What are the main aims / objectives of the changes	Reduction in Financial Loss, Improved management of Challenging behaviour, Reduction of Severity of Incidents of aggression directed as staff.	

Step 2: Assessing the Impact

Please use the drop-down feature to detail any positive or negative impacts of this document /policy on patients in the drop-down box below:

Protected Characteristic	Positive Impact(s)	Negative Impact(s)	Action to address negative impact: *(e.g. adjustment to the policy)*
Sex			This Policy does not have a positive or Negative impact on any protected characteristic such as Sexual Orientation

Gender reassignment			This Policy does not have a positive or Negative impact on any protected characteristic such as Gender Reassignment.
Disability		Y	This policy could have a negative impact on the determination of whether a sanction is appropriate for persons suffering from Mental Health implications or Learning Disabilities but the law and legislation attached to the policy and the policy itself will ensure it is fair and balanced and won't affect diversity and equality.
Age			This Policy does not have a positive or Negative impact on any protected characteristic such as Age
Sexual Orientation			This Policy does not have a positive or Negative impact on any protected characteristic such as a persons Sexual Orientation
Pregnancy and maternity			This Policy does not have a positive or Negative impact on any protected characteristic such as Pregnancy or Maternity
Marriage and civil partnership			This Policy does not have a positive or Negative impact on any protected characteristic such as Marriage or any Civil Partnership
Religion or belief			This Policy does not have a positive or Negative impact on any protected characteristic such as Religion or Belief
Race			This Policy does not have a positive or Negative impact on any protected characteristic such as Race

If you answer yes to any of the following, you MUST complete the evidence column explaining what information you have considered which has led you to reach this decision.

Assessment Questions	Yes / No	Please document evidence / any mitigations
In consideration of your document development, did you consult with others, for example, external organisations, service users, carers or other voluntary sector groups?)	Yes	LSMS from other trusts EPRR Lead H&S Manager Local Police
Have you taken into consideration any regulations, professional standards?	Yes	ICO guidelines and Camera Commissioner guidelines as well as Data Protection act and GDPR principles will be followed to ensure fairness impartiality and equality.

		RIPA 2000 will always be adhered too with regards to privacy and equality during any surveillance
In drafting your document have you identified any discrimination issues, and if so how have they been mitigated?	No	

Step 3: Review, Risk and Action Plans

How would you rate the overall level of impact / risk to the organisation?	Low	Medium	High
	■	☐	☐
What action needs to be taken to reduce or eliminate the negative impact?	Each case where Surveillance is used that might be likely to affect someone with a mental health issue or disability will be individually assessed to ensure that the person's dignity and diversity Is considered at all times. All incidents where a crime is committed will be dealt with to keep collateral intrusion to a minimum and all ICO and CC guidelines will be followed.		
Who will be responsible for monitoring and regular review of the document / policy?	The policy will be reviewed by the ASMS as well as the H&S manager where this policy falls upon both areas covered by each of those roles.		

Step 4: Authorisation and sign off

I am satisfied that all available evidence has been accurately assessed for any potential impact on patients and groups with protected characteristics in the scope of this project / change / policy / procedure / practice / activity. Mitigation, where appropriate has been identified and dealt with accordingly.

Equality Assessor:		*Date:*	

This section is to be agreed and signed by the Head of Diversity and Inclusion in agreement with the Diversity and Inclusion Strategy Lead:

Diversity and Inclusion authoriser name:	
Date:	

Additional guidance

Protected characteristic		Who to Consider	Example issues to consider	Further guidance
1.	**Disability**	A person has a disability if they have a physical or mental impairment which has a substantial and long term effect on that person's ability to carry out normal day today activities. Includes mobility, sight, speech and language, mental health, HIV, multiple sclerosis, cancer	• Accessibility • Communication formats (visual & auditory) • Reasonable adjustments. • Vulnerable to harassment and hate crime.	Further guidance can be sought from: Solent Disability Resource Group
2.	**Sex**	A man or woman	• Caring responsibilities • Domestic Violence • Equal pay • Under (over) representation	Further guidance can be sought from: Solent HR Team
3	**Race**	Refers to an individual or group of people defined by their race, colour, and nationality (including citizenship) ethnic or national origins.	• Communication • Language • Cultural traditions • Customs • Harassment and hate crime • "Romany Gypsies and Irish Travellers", are protected from discrimination under the 'Race' protected characteristic	Further guidance can be sought from: BAME Resource Group
4	**Age**	Refers to a person belonging to a particular age range of ages (eg, 18-30 year olds) Equality Act legislation defines age as 18 years and above	• Assumptions based on the age range • Capabilities & experience • Access to services technology skills/knowledge	Further guidance can be sought from: Solent HR Team
5	**Gender Reassignment**	" The expression of gender characteristics that are not stereotypically associated with ones sex at birth" World Professional Association Transgender Health 2011	• Tran's people should be accommodated according to their presentation, the way they dress, the name or pronouns that they currently use.	Further guidance can be sought from: Solent LGBT+ Resource Group
6	**Sexual Orientation**	Whether a person's attraction is towards their own sex, the opposite sex or both sexes.	• Lifestyle • Family • Partners • Vulnerable to harassment and hate crime	Further guidance can be sought from: Solent LGBT+ Resource Group
7	**Religion and/or belief**	Religion has the meaning usually given to it but belief includes religious and philosophical beliefs, including lack of belief (e.g Atheism). Generally, a belief should affect your life choices or the way you live for it to be included in the definition. (Excludes political beliefs)	• Disrespect and lack of awareness • Religious significance dates/events • Space for worship or reflection	Further guidance can be sought from: Solent Multi-Faith Resource Group Solent Chaplain
8	**Marriage**	Marriage has the same effect in relation to same sex couples as it has in relation to opposite sex couples under English law.	• Pensions • Childcare • Flexible working • Adoption leave	Further guidance can be sought from: Solent HR Team
9	**Pregnancy and Maternity**	Pregnancy is the condition of being pregnant or expecting a baby. Maternity refers to the period after the birth and is linked to maternity leave in the employment context. In non-work context, protection against maternity discrimination is for 26 weeks after giving birth.	• Employment rights during pregnancy and post pregnancy • Treating a woman unfavourably because she is breastfeeding • Childcare responsibilities • Flexibility	Further guidance can be sought from: Solent HR team

Annex B

Application to Access Surveillance Camera Images

Applicants Details

Surname: …… Forenames: ……..

Company/Address: ……

Telephone Number: ……

Details of Images Required

Date: ……..

Time: ……

Camera Location: ……

Camera Number: ……..

Tick as Appropriate

I require viewing the images only ☐

I require a hard copy of the images ☐

Data Protection Declaration

I declare that the information given is correct to the best of my knowledge and that I am entitled to apply for access to surveillance camera images.

Records referred to above under the terms of the Data Protection Act 1998

Name: ……

Signature: ……

Date: ……

Annex C

Viewing of Surveillance Camera Images

Date & Time Viewed	Camera Number	Operator

Reason for Viewing:
Authorised By : Name: Signature:

Details of Person Viewing:

Name:

Appointment:

Signature:

Annex D

PROVISION OF IMAGES TO POLICE/ 3rd PARTY FOR INVESTIGATION/ LEGAL PROCEEDINGS

Name of Applicant……

Company……

Telephone Number……..

Date of Incident……..

Time of Incident……

Camera No…….

Location……

Crime/Incident Number……..

Brief Description of Incident:
……
……
……
……
……
……

Signature……..

Date……..

Date of Destruction……

Method of Destruction……

Name of Person Carrying Out Destruction……..

Signature…….

Annex E

Surveillance Camera Daily Check Sheet

Date	Time	Operator	Signature	Camera Date/Time Check	Picture Quality	Maintenance Contacted
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						
29						
30						
31						