|  |  |
| --- | --- |
|  **Document name:** | Surveillance Camera Policy (CCTV and Automatic Number Plate Recognition (ANPR), Body Worn Video Cameras (BWV))  |
| **Document type:** | Policy |
| **What does this policy replace?** | Review and update on previous version of policy  |
| **Staff group to whom it applies:** | All staff within the Trust |
| **Distribution:** | The whole of the Trust |
| **How to access:** | Intranet and website |
| **Issue date:** | June 2021 |
| **Next review:** | June 2024 |
| **Approved by:** | Executive Management Team |
| **Developed by:** | Security Adviser  |
| **Director leads:** | Director of Human Resources, Organisational Development and Estates |
| **Contact for advice:** | Security Advisers:Johan CelliersJohn SandersonHead of Estates Operations:Tony Tipton |

**Contents**

1. Introduction.
2. Purpose of the policy.
3. Definitions
4. Roles and Responsibilities
5. Principals of the Policy
6. Purpose of the scheme - recording of Images and Audio
7. Privacy of individuals - recording of Images and Audio
8. Assessment procedure and continued use
9. General Assessment
10. General requirements and responsibilities
11. Complaints
12. Monitoring compliance with the policy
13. References and associated documents

**Appendix A** Application by Authorised Agency

**Appendix B** Application for access to recorded images (subject access request)

**Appendix C** ICO CCTV Notification Template

**Appendix D** Home Office Surveillance Camera Code of Practice 2013

 12 Guiding Principles

**Appendix E** Body Worn Video (BWV) Procedures

**Appendix F** Assessment for new CCTV System and continued use

**Appendix G** Review Checklist

**Appendix H** Maintenance Procedures for CCTV Systems

**Appendix I** Equality Impact Assessment Tool

**Appendix J** Checklist for the Review and Approval of Procedural Document

**Appendix K** Version Control Sheet

**SURVEILLANCE CAMERA POLICY (CCTV AND AUTOMATIC NUMBER PLATE RECOGNITION (ANPR))**

1. **Introduction**

This policy covers the 2018 Data Protection Act (UK GDPR), the CCTV Code of Practice 2008, and the Surveillance Camera Code of Practice 2013 and is aimed at the use of CCTV and similar surveillance equipment that monitor, and record images from, those areas to which the public have largely unrestricted access. In addition, areas which have controlled access will also be monitored by the system, in order to assist in the protection of trust assets, general public**,** patients, visitors and staff.It is also important to note that the Trust manages all data, access to data, and security of the CCTV data is controlled in accordance with the requirements of the 2018 Data Protection Act.

1. **Purpose**

This policy applies to all surveillance camera systems (CCTV, ANPR, Body Worn Video Cameras (BWV)) which are used for the general purpose of crime prevention and detection and public safety. South West Yorkshire NHS Foundation Trust is the responsible owner of various surveillance systems and conforms to the Data Protection Act (UK GDPR), Surveillance Camera Commissioners and Home Office Camera Codes of Practice

By adhering to this policy, the Trust can ensure that CCTV cameras throughout the Trust will be installed and used in compliance with the principles of:

* Data Protection Act 2018 (UK GDPR),
* Human Rights Act 1998,
* Regulation and Investigatory Powers Act 2000 and other UK and EEA relevant legislation.

This policy covers the use of the following types of system:

* Analog and Digital on DVR
* Digital on PC
* Real time viewing

|  |
| --- |
| The Regulation of Investigatory Powers Act 2000 regulates the use of covert/directed surveillance and is subject to a strict code of practice. **The use of CCTV in these circumstances or for any other reason other than that authorised in accordance with this policy is not covered by this policy** and in such circumstances further guidance should be sought from the IG and Records department It is not intended that the surveillance systems should be used by official law enforcement bodies, such as police forces, the security services or HM Revenue and Customs when carrying out specialised and/or surveillance or operations, such use would require the authorisation of the Chief Executive. |

1. **Definitions**

**3.1** A **POLICY** is a high level statement. Each policy should specify its purpose and may also include a procedure setting out how the policy will be achieved. A policy enables management and staff to make correct decisions, deal effectively and comply with legislation, Trust processes and good working practices.

* 1. A **PROCEDURE** is often incorporated into a policy or can be a ‘stand alone’ document. Procedures are the practical way in which a policy is translated into action. They explicitly outline how to accomplish a task or activity, giving detailed instructions. A procedure often allocates specific roles that specific individual must undertake.
	2. **Surveillance Cameras** include systems like Closed Circuit Television (CCTV) and Automatic Number Plate Recognition (ANPR) are deployed extensively across the United Kingdom, and used as valuable tools to contribute to public safety and security and in protection of both people and property.
	3. **Data Protection Impact Assessment** (DPIA) A process for identifying and minimising data protection risks
1. **Roles and Responsibilities**

The following duties apply to this policy.

**4.1 Trust Board**

The Trust Board will ensure, so far as is reasonably practicable, that all steps are taken to ensure secure and safe environments for all stakeholders of the Trust. This will also include persons who are not employees of the Trust, but who use the Trust’s premises. Directors will ensure that adequate training and guidance is given to all their managers and staff on whom this duty devolves.

Responsibility for CCTV systems rests equally with Directors, Managers and individual Employees, not solely with the Local Security Management Specialist, or other competent advisers, Safety & Resilience TAG or Trade Union appointed safety representatives.

**4.2 Executive Management Team (EMT)**

The Executive Management Team is responsible for approving all policies. The EMT will be responsible for ensuring the CCTV policy document has been developed and implemented according to Trust guidance.

**4.3 Directors**

Every Director carries the responsibility for ensuring that within their scope of responsibility, appropriate risk assessments have been undertaken and that there are adequate local working procedures to ensure safe and secure environments.

**4.4 Service Management and Business Delivery Units (BDUs)**

General-, Service- and Line Managers will ensure employees are aware of their rights and responsibilities for the provision and maintenance of a safe and secure environment for staff, patients and visitors. This will be done by providing all employees with information, instruction, training and/or supervision as appropriate to their needs so that they can work safely and understand their obligations under the Health & Safety at Work Act 1974 and associated legislation.

General-, Service- and Line Managers must ensure staff report all breaches of security, criminal activity, security incidents, CCTV systems failure, or suspicions to the relevant security department, in the area where they work immediately. Following an incident, the incident must be reported onto the Trust’s DATIX incident reporting system.

**4.5 Security Adviser (Local Security Management Specialist (LSMS)), and Other Competent Advisers**

The Security Adviser **(**LSMS) is responsible for providing guidance regarding operational requirements for CCTV systems and for managing any application to NHS.

The Security Adviser(LSMS) will, with the help of other advisers, develop the local CCTV procedures to comply with the policy and other guidance referenced for the purpose of this policy.

The Security Adviser **(**LSMS’s) are authorised to support the investigation and detection of crime and security incidents within the Trust’s business areas. These investigations will be carried out in conjunction with the appropriate Senior Management, Internal Audit or where necessary, the Police. Where investigations are being carried out, it is imperative all staff co-operate with the Security Department, Fraud and Internal Audit personnel or Police officers as appropriate.

**4.6 Head of Information Governance**

Ensures that the Trust’s use of CCTV Systems is registered with the Information Commissioner under the terms of the Data Protection Act 2018 (GDPR). They will ensure that the policy and Code of Practice are adhered to and monitors this compliance. Responds to complaints relating to processing under the Data Protection Act. Responds to Subject Access Requests in accordance with Data Protection legislation and trust policy.

**4.7 Estates Department**

The Estates Department are responsible for the general support and maintenance of security and CCTV systems at Trust premises. All heads of department, Directorates and local management teams should co-operate fully with Estates or Security department and ensure they are given all the necessary co-operation to carry out their duties and to allow for appropriate access and maintenance of the CCTV systems. The Estates Department will maintain a register of locations containing repair and maintenance contracts for CCTV. This is not Trust wide and does not include CCTV in PFI sites.

**4.8 Employee Responsibilities**

Employees of the Trust have responsibility for: -

* Ensuring that effective measures are taken to ensure that the Trust premises and property are maintained in a secure condition and any shortfalls reported.
* Taking steps to safeguard against loss of the Trust property and the property of individuals as far as reasonable practicable.
* Taking reasonable steps to ensure security of their own personal possessions – the Trust takes no responsibility for personal possessions except in specific circumstances where personal property is handed to staff for safe keeping.
* Report incidents.

Every Trust employee, whilst having the right to a safe working environment, carries responsibility for their own health and safety and the safety of others.

1. **Principals of the Policy**
	1. **Standards for Compliance**

The standards which must be met if the requirements of the Data Protection Act 2018 are to be complied with are based on the Data Protection Principles, which say that data, must be: -

* Fairly and lawfully processed;
* Processed for limited purposes and not in any manner incompatible with those purposes;
* Adequate, relevant and not excessive;
* Accurate;
* Not kept for longer than is necessary;
* Processed in accordance with individual’s rights;
* Secure;
* Not transferred to countries which don’t have adequate protection.

This code also reflects the wider regulatory environment. When using, or intending to use surveillance systems, many organisations also need to consider their obligations in relation to the Freedom of Information Act 2000 (FOIA), the POFA, the Human Rights Act 1998 (HRA) and the [Surveillance Camera Code](https://www.gov.uk/government/publications/surveillance-camera-code-of-practice) of Practice issued under the Protection of Freedoms Act (POFA code).

1. **Purpose of the scheme – Recording of Images and Audio**

The registered purpose of the scheme is for the prevention and detection of crime, the safety and security of public**,** patients, visitors and staff; and for the support of investigations. The CCTV and ANPR systems can only be used for the registered purposes mentioned above and not for any other purpose i.e. monitoring staff movements or directed surveillance.

**Information Commissioner’s (ICO) Registration information (Appendix B)**

* Crime Prevention and Prosecution of Offenders

**Purpose Description:**

* The prevention and detection of crime, and the apprehension and prosecution of offenders.
* Within Trust premises surveillance cameras are used for the following purposes only:
	+ To protect staff, patients and visitors
	+ To protect Trust premises and Trust assets
	+ To increase personal safety and reduce the fear of crime
	+ To reduce incidents of violence and aggression to staff members
	+ To support the Police in reducing and detecting crime
	+ To assist in identifying, apprehending and prosecuting offenders
	+ To provide a deterrent effect and reduce criminal activity
	+ To assist in the traffic management and car parking schemes

**Data Controllers further description of Purpose:**

* The use of surveillance systems for the monitoring and collection of the visual images and sound for the purpose of maintaining security of the premises, for the prevention of crime and for the investigation of crime.

**Data subjects are:**

* Those inside, entering or in the immediate vicinity of the area under surveillance, and members of the public.

**Data classes are:**

* Sound and visual images;
* Offences (Including Alleged Offences);
Criminal Proceedings, Outcomes And Sentences;
* Support of Internal investigations by Trust Departments;
* Personal appearance and behaviour.

**Sources (S) and Disclosures (D)(1984 Act). Recipients (1998 Act):**

* Security organisation;
* Data subjects themselves;
* Business associates and other professional advisers;
* Employees and agents of the data controller;
* Suppliers, providers of goods or services;
* Police forces.

**Transfers:**

* None outside the European Economic Area
1. **Privacy of individual – recording of Images and Audio**

The use of a surveillance system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

The Trust proposed deployment of CCTV systems that includes audio recording in some public places is likely to require a strong justification of necessity to establish its proportionality. However, the surveillance camera system is not installed for the purpose of recording conversations as this is highly intrusive and unlikely to be justified. The purpose is for the deterrence and detection of verbal aggression against trust staff and to use for investigation of these types of incidents. The requirement of audio will be assessed per area and will be reviewed for continued use.

1. **Assessment procedure and continued use**

The Trust surveillance camera systems are strategically administered and managed by the Estates and Facilities Department, in accordance with the principles and objectives expressed in the Data Protection Act 2018, GDPR, Home Office Surveillance Code of Practice, and the Surveillance Commissioner's Codes of Practice.

The Trust realise that using CCTV can be privacy intrusive, as it is capable of putting many law-abiding people under surveillance and recording their movements as they go about their day to day activities. The Trust will carefully consider whether to use it; the fact it is possible, affordable or has public support should not be the primary motivating factor.

The provision of information is the first step in transparency and accountably on the part of the trust. The development and installation of any new CCTV system must include proportionate consolation and engagement with stakeholders to ensure that the new system is an appropriate response to the identified need.

To judge the quality of images that will be necessary, the purpose for which CCTV is used and the level of quality that will be necessary to achieve the purpose will have to be taken into account. The following categories will help with guidance on the type of system required for the proposed purpose of the scheme (Appendix C&D).

* **Monitoring:** To watch the flow of traffic or the movement of people where you do not need to pick out individual figures.
* **Detecting:** To detect the presence of a person in the image, without needing to see their face.
* **Recognising:** To recognise somebody you know, or determine that somebody is not known to you.
* **Identifying:** To record high quality facial images, this can be used in a court of law, to prove someone’s identity beyond reasonable doubt.
1. **General Assessment (Appendix C)**

Before installing and using CCTV and similar surveillance equipment on any SWYPFT owned or occupied site the following assessment procedure must be carried out:

* Establish, and document, who is the person(s) or organisation(s) legally responsible for the proposed scheme and who are/is responsible for the day-to-day compliance with the requirements of the Code of Practice and this policy.
* Assess and document the appropriateness of and reasons for using CCTV or similar surveillance equipment.
* Establish and document the purpose of the scheme.
* Notify the information commissioner of the purpose(s) of the scheme.
* What are the benefits gained from its use?
* Can CCTV technology realistically deliver these benefits? Can less privacy intrusive solutions such achieve the same objectives?
* Will particular system being considered deliver the desired benefits and remain suitable for the future?
	1. **Effective Administration:**
		1. Establishing a clear basis for the handling of any personal information is essential and the handling of images relating to individuals is no different.
		2. Authorisation for the introduction of any new or extended CCTV Scheme must be approved by the Director of Human Resources, Organisational Development and Estates and/or Director of Finance and Resources and reported to the EMT.
		3. Written contracts should be agreed, with clearly defined responsibility for contactors who might do processing and editing of pictures. The contracts should also include guarantees for security and the use of properly trained staff, if required.
		4. Clear operational procedure must be agreed and communicated to those who operate the system.

The use of CCTV systems should be regularly reviewed and justified. This can be done annually with the renewal of the notification to the Office of the Information Commissioner. Individual systems will be reviewed along with the local crime reduction survey completed on a rolling program based on risk associated to the individual service or building.

(It is suggested that reference is made to the CCTV Code of practice 2008 for more in-depth guidance with the Initial Assessment Procedure (**Appendix D** and the Home Office Surveillance Camera Code of Practice 2013 **(Appendix E**).

1. **GENERAL REQUIREMENTS AND RESPONSIBILITIES**
	1. **Siting of cameras and signage**

|  |
| --- |
| **All cameras are located in prominent positions within public and staff view**.  |

It is essential that the location of cameras is carefully considered, because the means by which, and the way in which, images are captured will need to comply with the First Data Protection Principle.

The Trust has a responsibility to inform people that they are in an area where CCTV surveillance is being carried out. The most effective way of doing this is by using prominently placed signs at the entrance to the CCTV zone. Standards to be met in aid compliance are:

* + 1. Cameras will not be hidden from view and we will inform the public of the presence of the system and its ownership at all times

|  |
| --- |
| * + 1. CCTV cameras within the Trust will not be used for covert surveillance unless authorized.
 |

* + 1. Cameras must be sited in such a way that they only monitor those spaces, which are intended to be covered by the equipment.
		2. If private domestic areas, such as gardens or areas not covered by the scheme, border those spaces, which are intended to be covered by the equipment then the user should consult with the owners of such spaces if images from those spaces might be recorded or these areas can be blanked out, either manually of digitally.
		3. Operators must be aware of the purpose(s) for which the scheme has been established.
		4. If cameras are adjustable by the operators, this should be restricted so that operators cannot adjust or manipulate them to overlook spaces which are not intended to be covered by the scheme.
		5. If it is not possible physically to restrict the equipment to avoid recording images from those spaces not intended to be covered by the scheme, then the operators should be trained in recognising the privacy implications of such spaces being covered.
		6. Operators must be aware that they are only able to use the equipment in order to achieve the purpose(s) for which it has been installed.
		7. Signs should be clearly visible and legible to the members of the public and placed so that the public are aware that they are entering a zone which is covered by surveillance equipment.
		8. The size of signs will vary according to circumstances but they must contain the following information:

**10.1.8.1** Identity of the person or organisation responsible for the scheme.

* + - 1. The purpose of the scheme.
			2. Details of who to contact regarding the scheme.

Where an image of a camera is not used on a sign, the following wording is recommended: “**Images and audio** are being recorded for the prevention of crime and your safety. This scheme is controlled by SWYPFT. For further information contact 01226 644030”.

Where an image of a camera is used on a sign, the following wording is recommended: “This scheme is controlled by SWYPFT. For further information contact 01226 644030”.

* 1. **Quality of the images**

|  |
| --- |
| **All faulty equipment within the CCTV system that could affect picture or recording quality should be repaired or replaced as soon as practically possible**  |

The Third, Fourth and Fifth Data Protection Principle are concerned with the quality of personal data.

It is important that the images produced by the equipment are as clear as possible in order that they are effective for the purpose(s) for which they are intended. For example if a system has been installed to prevent and detect crime, then it is essential that the images are adequate for that purpose.

Recorded material should be stored in a way that maintains the integrity of the image. This is to ensure that the rights of individuals recorded by the CCTV system are protected and that the material can be used as evidence in court.

A record should be kept of how the images are handled if they are likely to be used as evidence on court. Once there is no reason to retain the recorded images any longer, they should be deleted or destroyed. Exactly when to delete images will depend on the purpose for using CCTV.

**Standards to be met to aid compliance with these principles are:**

* + 1. How easy is it to take copies of a recording off your system when asked for by law enforcement agency? Can this be done without interrupting the operation of the system?
		2. Will they find your recorded images straightforward to use?
		3. What will you do when recorded material needs to be taken away for further examination?
		4. Upon installation an initial check should be undertaken to ensure that the equipment performs properly.
		5. The medium on which the images are captured should be cleaned so that images are not recorded on top of images recorded previously.
		6. If the system records features such as the location of the camera and/or date and time reference, these should be accurate.
		7. Cameras should be situated where they will capture images relevant to the purpose for which the scheme has been established. For example, if the purpose of the scheme is the prevention and detection of crime, the cameras should be sited so that images enabling identification of perpetrators are captured.
		8. When installing cameras, account must be taken of the light conditions in which the cameras are located.
		9. Maintenance of the cameras should be undertaken on a regular basis in order to ensure that clear images are recorded.

**10.3** **Processing images**

**Images which are not required for the purpose, for which the equipment is being used, should not be retained for longer than necessary.**

While images are retained it is essential that their integrity be maintained whether it is to ensure their evidential value or to protect the rights of people whose images may have been recorded. It is therefore important that access to and security of the images is controlled in accordance with the requirements of the 2018 Data Protection Act. The Seventh Data Protection Principle sets out the security requirements of the 2018 Data Protection Act. Standards to be met to aid compliance with this principle are:

* + 1. Images should not be retained for longer than 30 days unless they are required for evidential purposes in legal proceedings.
		2. Once the image retention period has expired, the images themselves should be removed or erased. Retention periods will be defined in local protocols and based on local requirements. Images are routinely deleted by being overwritten unless the image is required for evidential purposes then it must be separately retained.

Once the image retention period has expired, the images themselves should be removed or erased. Retention periods will be defined in local protocols and based on local requirements. Images are routinely deleted by being overwritten unless the image is required for evidential purposes then it must be separately retained.

While images are retained, it is essential that their integrity be maintained, whether it is to ensure their evidential value or to protect the rights of people whose images may have been recorded. It is therefore important that access to and security of the images is controlled in accordance with the requirements of the 2018 Act.

* + 1. If images are retained for evidential purposes, they should be removed from the system and retained in a secure place to which access is controlled. The images will stored securely and appropriately by the security team for approximately two years after the invitation has been completed.
		2. The operator removing the images should ensure that they follow the procedure for removal of images, and have documented the footage appropriately.

**10.3.5** Monitors displaying images from areas in which individuals would have an expectation of privacy should not be viewed by anyone other than authorised employees of the user of the equipment.

* + 1. Access to the recorded images is restricted to designated personnel approved by the Director of Human Resources and Workforce Development. Any requests for access by third parties in accordance with the documented disclosure policy must be authorised by the Director of Human Resources, Organisational Development and Estates, or in his absence, by his deputy.
		2. Where CCTV images are required for evidential purposes in legal or Trust disciplinary proceedings, they will be properly processed following consultation with the Head of Information Governance and Data Protection and the Information Governance Manager.
		3. The recording will be placed in a sealed envelope which is signed, dated and then stored securely until the investigation is complete. Viewing of images is controlled by the Local Manager or a person nominated to act on his behalf.
		4. Viewing of the recorded images should take place in a restricted area. Other employees should not be allowed to have access to that area when viewing is taking place.
		5. Removal of the images for viewing should be documented as per Trust CCTV procedures.
		6. All operators and employees with access to images should be aware of the procedures that need to be followed when accessing the recorded images.
		7. The Trust provides training programmes for Trust staff on the Data Protection Act and CCTV Code of Practice. All operators should be trained in their responsibilities under the Code of Practice and this policy. All operators should be aware of:
			1. The SWYPFT Safe and Secure Environments Policy
			2. The Data Protection Act 2018 (GDPR)
			3. Rights of individuals in relation to their recorded images.

**WE MAY NEED TO ALLOW POLICE ACCESS TO DATA OUTSIDE NORMAL HOURS FOR INCIDENTS, ABSCONDINGS OR OTHER EMERGENCIES.**

* 1. **Disclosure of images to third parties**

It is important that access to and disclosure of the images recorded by surveillance systems is restricted or carefully controlled not only to ensurethat the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes. Should copies of images be disclosed, the reason(s) or purpose(s) for the disclosure should be compatible with the reason(s) or purpose(s) for which the images were originally obtained. The second and seventh Data Protection Principles cover these issues.

Standards to be met to aid compliance with these principles are:

* + 1. Access to recorded images should be restricted to those staff who need to have access in order to achieve the purpose(s) of using the equipment.
		2. All access to images should be documented.
		3. Access to images by third parties should only be allowed in limited and prescribed circumstances and must be authorised by Director of Human Resources, Organisational Development and Estates.

If the purpose of the system is the prevention and detection of crime, then disclosure to third parties should be limited to the following:

**10.4.3.1** Law enforcement agencies where the images recorded would assist in a specific criminal enquiry, or where the images are to be used to assist law enforcement agencies in the return of patients who take unauthorised absence under section of the Mental Health Act 1983, or relevant criminal justice legislation.

* + - 1. Prosecution agencies.
			2. Relevant legal representatives.
			3. The media, where it is decided that the public’s assistance is needed in order to assist in the identification of victim, witness or perpetrator in relation to a criminal incident. As part of that assessment, the wishes of the victim of an incident should be taken into account.
			4. People whose images have been recorded and retained (unless disclosure to and individual would prejudice the criminal enquiries or criminal proceedings).
		1. If access to or disclosure of the images is allowed, then the following should be documented.

**10.4.5.1** The date and time at which access was allowed or the date on which disclosure was made.

* + - 1. The identification of the third party who was allowed access or to whom disclosure was made.
			2. The reason for allowing access or disclosure.
			3. The extent of the information to which access was allowed or which was disclosed.
		1. Recorded images should not be made more widely available – for example they should not be routinely made available to the media or placed on the Internet.
		2. If it is intended that images will be made more widely available, authorisation is required from either the Chief Executive, Director of Human Resources, Organisational Development and Estates. The reason for that decision should be documented.
		3. If it is decided that images will be disclosed to the media (other than in the circumstances outlined above) the images of individuals will need to be disguised or blurred so that they are not readily identifiable.
		4. If the system does not have the facilities to carry out the type or editing required as described, above an editing company may be hired to carry out that editing.
	1. **Freedom of Information**

Public Authorities may receive requests under the Freedom of Information Act 2000 (FOIA) or Freedom of Information (Scotland) Act 2002 (FOISA).

**Procedure for dealing with requests which may be covered by the Act**

* The Trust maintains a publication scheme which makes a range of information about the organisation routinely available via the Trust’s website.
* Requests for information under the Freedom of Information Act are dealt with by the Trust’s Customer Services Team.
* Requests for information under the general right of access must be made in writing; requests received by email are valid.
* All requests must be referred to the Customer Services Team, who will authorise and action all requests.
* For further information reference Trust’s Freedom of Information policy and procedure
	1. **Access Request by Data Subject**

The 2018 Data Protection Act provides individuals with a number of rights in relation to the processing of their personal data. An example of these rights is, the right to be provided with a copy of the information constituting the personal data held about them, in appropriate cases. A further example is the right to seek compensation for damages and distress suffered as a result of any contravention of any requirements of the Act.

The Subject Access Officer is the designated person in each locality to whom all requests must be directed.

Written request for access must be directed to:

The Subject Access Officer.

South West Yorkshire Partnership Foundation Trust

Oaks Building

Kendray Hospital

Doncaster Road

Barnsley

S70 3RD

The Subject Access Officer has responsibility for the receiving and processing all subject access requests. If such a request is received the Subject Access Officer will log the request and forward the request to the Security Adviser(LSMS) who will forward the Application form to the data subject. For more information regarding the application process and trust data, reference the Trust’s Information Governance Policy and Data Protection Policy.

All requests from data subjects for access or disclosure of recorded images must be made in writing on this form (Appendix B). A fee of £10 will be required by SWYPFT to carry out the search for the images requested. If no fee is paid, the search will not be conducted. The fee is not refundable if no images are found.

The Trust will only accept applications from the data subject, not persons acting on their behalf, except in cases where an application is made on behalf of a child under 16 years of age by someone with parental responsibility for the child or an application is made by a Legal Representative and the express consent of the data subject accompanies the request. Care must be taken when dealing with requests for recorded images of children from someone with parental responsibility for the child. Where children have the capacity to understand the implications, and make an informed decision, about access to their recorded image, it would be appropriate to seek their consent in addition to that of the person with parental responsibility.

Further info about the applications process can be obtained from the Information Governance Team. This section must be read in conjunction with the Trust’s Service User Access to Personal Identifiable Information.

[Subject access requests (swyt.nhs.uk)](http://nww.swyt.nhs.uk/it/information-governance/Pages/Subject-access-requests.aspx)

1. **Complaints**

Any complaints arising from the management and operation of CCTV surveillance will be dealt with under the Trust’s normal complaints procedures. All complaints will be acknowledged in writing and the complainant will be advised that they may also refer the matter to the Information Commissioner either whilst the Trust is investigating the complaint or if they are dissatisfied with the outcome of the Trust’s investigation.

1. **Monitoring compliance with the policy**

12.1The Safety & Resilience Trust Action Group (TAG) will monitor the effectiveness of this policy by periodically reviewing non clinical accidents and incidents and also training attendance.

12.2 All departments will fully participate in the annual health and safety monitoring programme. A report will be provided to the Safety & Resilience Trust Action Group on an annual basis by the Head of Security & Emergency Preparedness and/or the Health & Safety Manager of the request received/not received.

12.3 The Security Department will carry out periodic quality checks of all premises risk assessments and provide feedback to Managers.

12.4 The Security Adviser(LSMS) will ensure that the surveillance systems comply with this policy and Information Commissioner’s Office (ICO) Code of Practice.

1. **References and associated documents**

This document has been developed in line with guidance issued by the ICO’s CCTV Code of Practice 2008 and Home Office’s Surveillance Camera Code of Practise 2013.

It should be read in conjunction with

**Internal**

* Management of Violence & Aggression Policy
* Lone Worker Policy
* Safe and Secure Environments Policy
* SWYPFT Estates and Facilities Operations Manual
* Patient Property Policy
* Suspicious Packages & Bomb Hoax Procedures

**External**

* Surveillance Camera Code of Practice: A guide to the 12 principles <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/368115/Leaflet_v6_WEB.pdf>
* Surveillance Camera Code of Practice:Steps to complying with the 12 principles

<https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409290/12_principles_diagram_v3.pdf>

* Home Office Scientific Development Branch, CCTV Operational Requirements Manual, 2009.
* Home Office – *Surveillance Camera Code of Conduct*
* Home Office – *Surveillance and counter-terrorism*
* Information Commissioners Office - *In the picture: A data protection code of practice for surveillance cameras and personal information*
* Information Commissioners Office – *Conducting privacy impact assessments code of practice*
* Information Commissioners Office – Privacy notices code of practice
* Joint Commissioners *– Surveillance Road Map. A shared approach to the regulation of surveillance in the United Kingdom*
* Ann Cavoukian, PhD *– Privacy by Design. The 7 Foundational Principles*
* Information Commissioners Office – *Big data and data protection*
* Information Commissioners Office – *The Guide to Data Protection*
* Information Commissioners Office – *Data sharing code of practice*
* Information Commissioners Office – *Subject access code of practice*
* Information Commissioners Office – *The Guide to the Freedom of Information*
* Home Office Scientific Development Branch – *Is your CCTV system fit for purpose?*
* Surveillance Camera Commissioner – *Self Assessment Tools for CCTV, BWV and UAVs*
* Centre for the Protection of National Infrastructure (CPNI) – *Guide to Producing Operational Requirements for Security Measures*
* Centre for the Protection of National Infrastructure (CPNI) – *Embedding Security Behaviours: using the 5Es*
* Centre for the Protection of National Infrastructure (CPNI) – *Marauding Terrorist Attacks, Making your organisation ready.*
* Centre for the Protection of National Infrastructure (CPNI) – *Passport to Good Security for Senior Executives*
* Centre for the Protection of National Infrastructure (CPNI) – *Protective Security Management Systems (PSeMS). Guidance, Checklist and Case Studies.*
* Centre for the Protection of National Infrastructure (CPNI) – *CCTV within the workplace. A guidance document.*
* Centre for the Protection of National Infrastructure (CPNI) – *CCTV within the perimeter of a site. A guidance document*
* Centre for the Protection of National Infrastructure (CPNI) – *Human Factors in CCTV control rooms: A best practice guide*
* Centre for the Protection of National Infrastructure (CPNI) – *Storage of Recorded CCTV Images.*
* CAP 722 – *Civil Aviation Publication 722 - Unmanned Aircraft System Operations in UK Airspace*
* NACOSS Code of Practice NACP 20 *– Code of Practice for CCTV Systems.*
* BS EN 50132 Series of Standards *– European Standards for CCTV Systems*
* Home Office *– UK Police Requirements for Digital CCTV Systems*
* Data Protection, Information Commissioner’s Office *– CCTV code of practice*

**Appendix A**

**Application by Authorised Agency**

**Releasing information to the police**

Information should not normally be given to anyone, including the police, about a patient without their consent. The police may know the patients name, address and date of birth, but without consent no information can be given except in certain situations:

**Serious incidents**
If the police are investigating a serious incident, such as an assault, robbery or murder they may ask for information regarding individuals fitting a certain description.

Information should not be given unless the police provide us with a section 29 request form. You can give police a [section 29 form](http://nww.swyt.nhs.uk/it/information-governance/Documents/s.29%20form.docx) to complete in this circumstance (Or see below).

Requests may be made by the police, or any agency with the ability to bring forward a prosecution under section 29 of the Data Protection Act 1998.  This asks that the Data Controller (The Trust) considers release of the requested information, without informing the Data Subject (who the information was about). The form outlines that the police require information in the prevention and detection of a crime, and must be countersigned by a senior officer (for the police this is usually an Inspector or above).

If you are unsure about how to deal with a section 29 request please contact the Information Governance team

|  |
| --- |
| **PLEASE STATE THE LEGISLATION UNDER WHICH YOU ARE MAKING THIS APPLICATION** |
| **Application under Section 29(3) of The Data Protection Act 1998** |

|  |
| --- |
| **YOUR DETAILS** |
| Name |  | Department |  |
| Position |  |  |
| Telephone |  | Agency |  |
| E-mail |  |  |
| A signature, or co-signature of a senior person within your organisation is required for your request to be considered e.g. The Police Force – Inspector or above |
| Name |  |  |  |
| Position |  |  |  |
| Telephone |  |  |  |
| **ENTER SUBJECT DETAILS BELOW** |
| Full Name |  | Male/Female |  |
| Date of Birth |  |
| Last known address |  |
| Any known alias/other information which may assist  |  |
| Reply Required by (Date) |  | Your Reference |  |

|  |  |
| --- | --- |
| **Nature of Enquiry** | **State details of the criminal investigation or proceedings to which this request relates.**These details must show how the individual named is linked to the investigation and state what criminal offences they are suspected of (please state Act or Statutory Instrument) also include in this area Justification, Proportionality and Necessity.  |
|  |

|  |  |  |  |
| --- | --- | --- | --- |
| Specify time period i.e. last 6 months. 12 months or 2 years (Select time period) | 6 MonthsOther (please state) | 12 Months | 24 Months |

|  |
| --- |
| Please give brief details to show that: -* the requested information cannot be obtained by other means or from other sources
* the requested information will be of substantial value to the investigation or proceedings
* the lack of access to the requested information will prejudice the investigation or proceedings
 |
|  |

|  |
| --- |
| **ENQUIRY RESPONSE** |
| Officer Dealing |  | FIN |  | Date |  |
|  |

|  |
| --- |
| **HANDLING CONDITIONS – Imposed by**  |
| * Any information supplied by South West Yorkshire Partnership NHS Foundation Trust is to be used only for the purpose for which it was requested.
* It is to be stored securely in accordance with the Government Protective Marking Scheme and destroyed when no longer required for the purpose for which it was provided.
* Receiving agency to apply appropriate measures commensurate with requirements of principle 7 of The Data Protection Act e.g. accidental loss or compromise.
* The information shared must not be disclosed to any third party without written consent of the originating agency, unless it is disclosed under a statutory obligation.
 |

**FLOWCHART - APPLICATION FOR ACCESS TO CCTV IMAGES**

1. Contact Security team / Security Adviser (LSMS) and Request

Application form for Access to CCTV

2. Complete and return application form

3. CCTV checked for appropriate footage by security team

4. Application approved by SMD

5. CCTV footage released

**Appendix B:**

**Application for access to recorded images (subject access request)**

**APPLICATION FOR ACCESS TO RECORDED IMAGES (subject access request)**

The Information requested below is to help South West Yorkshire Partnership NHS Foundation Trust to:

1. Satisfy itself as to your identity and
2. Find any relevant data held

|  |
| --- |
| SECTON 1 ABOUT YOU |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Title (tick box) | Mr |  | Mrs |  | Miss |  | Ms |  |
| Other title (e.g. Dr) |  |  |  |  |  |  |  |  |
| Surname/family name |  |  |  |  |  |  |  |  |
| First name(s) |  |  |  |  |  |  |  |  |
| Maiden name / former name |  |  |  |  |  |  |  |  |
| Sex (tick box) | Male |  | Female |  |
| Height |  |
| Date of Birth |  |
| Place of Birth | Town County |

|  |  |
| --- | --- |
| Your current home address (to which we will reply)A telephone number will be helpful in case we need to contact you |  |
|  |
|  |
| Post Code |
| Tel No. |

If you have lived at the above address for less than 10 years, please give your previous address(es) for this period.

|  |  |
| --- | --- |
| Previous Address(es) |  |
|  |  |
| Dates of Occupancy | From  | To |
|  |  |
| Dates of Occupancy | From  | To |
|  |  |

|  |
| --- |
| SECTION 2 PROOF OF IDENTITY |

|  |
| --- |
| To help establish your identity, your application must be accompanied by TWO official documents that between them, show your name, date of birth and current addressFor example, birth/adoption certificate, driving licence, medical card, passport or other official document that shows your name and addressAlso TWO recent photographs of yourself, one of which is full face and the other a side perspective**Failure to provide this proof of identity may delay your application** |

|  |
| --- |
| SECTION 3 SUPPLY OF INFORMATION |

|  |
| --- |
| You have a right, subject to certain exceptions, to receive a copy of the information in a permanent form. Do you wish to:1. view the information and receive a permanent copy?
2. only view the information?

**Delete as appropriate** |

|  |
| --- |
| SECTION 4 DECLARATION |

|  |
| --- |
| **DECLARATION** (To be signed by the applicant) |
| I have read and understood the accompanying information explaining South West Yorkshire Partnership NHS Foundation Trust’s policy in relation to the purpose of the CCTV surveillance and the arrangements for access to recorded images.I certify that the information that I have supplied in this application is true and accurate and that I am the person to whom it relates.I understand that it is necessary for South West Yorkshire Partnership NHS Foundation Trust to confirm my identity and that it may be necessary to obtain more detailed information in order to locate the correct information.I enclose a non-refundable payment of £10 for the search to be completed. |
| Signed by |  | Date |  |
| **WARNING: A PERSON WHO IMPERSONATES OR ATTEMPTS TO IMPERSONATE ANOTHER, MAY BE GUILTY OF AN OFFENCE** |
| **Please ensure that all Sections are completed before returning the form** |

|  |
| --- |
| SECTION 5 TO HELP US FIND THE INFORMATION |

|  |
| --- |
| **Were you** (tick box) |
| A person reporting and (alleged) offence or incident? |  |
| A witness to an (alleged) offence or incident? |  |
| A victim of an (alleged) offence or incident? |  |
| A person accused or convicted of an offence? |  |
| Other – please explain |  |

|  |  |
| --- | --- |
| Date(s) and time(s) of incident |  |
| Place incident happened(e.g. Fieldhead, Dales unit) |  |
| Vehicle Registration Number (if you believe that your image was captured whilst you were there travelling in your vehicle) |  |
| Brief details of incident |  |

**Use separate sheets if required**

|  |  |
| --- | --- |
| Before returning this form please check: | * Have you enclosed TWO identification documents?
* Have you enclosed TWO recent photographs?
* Have you signed and dated the form?
* Have you enclosed the £10.00 (ten pounds) fee?
* Have you included a stamped addressed envelope for the return of proof of identity/authority documents where appropriate?
 |

**NOTE:** South West Yorkshire Mental Health Partnership NHS Foundation Trust reserves the right to obscure or suppress information relating to other third parties (under the terms of the Data Protection Act 2018).

|  |  |  |  |
| --- | --- | --- | --- |
| SIGNED |  | DATE |  |

**A written response to your application will be made within 21 days.**

Further information and advice may be obtained from:

http://www.ico.org.uk/

**Appendix C**

**ICO CCTV Notification Template**

From the information Commissioner’s website:

**‘N865 – CCTV only’ TEMPLATE**

Purposes:

 **Crime prevention and prosecution of offenders (including CCTV)**

Includes use of Closed-Circuit television for the monitoring of visual images for the purpose of maintaining the security of premises, for preventing crime and investigating crime.

**Subjects**

Customers and clients

Members of the public

Offenders and suspected offenders

Those inside, entering or in the immediate vicinity of the area under surveillance

**Classes**

Criminal proceedings, outcomes and sentences

Goods or services provided

Offences (including alleged offenders)

Personal details

Sound and/or visual images

**Recipients**

Business associates and other professional advisers

Data subjects themselves

Employees and agents of the data controller

 Persons making an enquiry or complaint

 Police forces

 Security organisations

 Suppliers, providers of goods or services

 **Transfers**

 None outside the EEA

**It is the responsibility of the Data Controller to ensure their notification is accurate.**

**Appendix D**

**Home Office Surveillance Camera Code of Practice 2013**

**12 Guiding Principles**

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

2. The use of a surveillance camera must take into account its effects on individuals and their privacy, with regular reviews to ensure its use remains justified.

3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

4. There must be clear responsibility and accountability for all surveillance system activities including images and information collected, held and used.

5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted: the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to the system and its purpose and work to meet and maintain those standards.

9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

12. Any information used to support a surveillance system which compares against a reference database for matching purposes should be accurate and up to date.

**Appendix E**

**Body Worn Video (BWV) Procedures**

1.Only trained and accredited security staff and specialists carrying a SIA CCTV licence will be authorised to operate on Trust premises. Police Officers and accredited officers of the Local Authority must inform the Trust security management team of any operation of their BWV systems on Trust premises.

2. The terms of reference and objectives of the Trust CCTV system apply to the Trust BWV equipment

3. Person’s subject of any operation of the system (when practical) will be informed and warned clearly that the system is to be deployed and this will be repeated upon activation. Any other persons (including staff and patients) in the immediate vicinity will also be informed even though they may not be the active subjects of surveillance.

4. The use of BWV for continuous recording will not be authorised although officers are encouraged to activate the screen when responding to an incident.

5. BWV will only be used on ward and office areas where there is an immediate danger or threat to personnel or property. It will be activated in every case of restraint or the physical handling of patients or other service users.

6. BWV footage will only be handled and stored in strict accordance with the Data Protection Act, ICO & SCCO guidance, Trust and NHS retention schedules. All data will be encrypted and access limited to authorised persons only.

7. All Trust security systems including CCTV, BWV and access control are subject of Privacy Impact Assessments and Privacy Notices.

8. Operational guidance has been issued to security staff and specialists in the use of BWV. This will be strictly adhered to and regularly monitored.

BWV records not only the actions and speech of an individual but can also record an individuals’ associations with others within the recording range, including friends, family members, bystanders, victims and suspects. This policy recognises that the recording of individuals must be necessary, proportionate and effective and only when all other alternatives have been considered. There must be an operational need for its deployment. It raises a significant risk to individual privacy, and the Trust must be committed to only using the system to the degree and manner that respects and protects staff, patient and general public’s right to personal privacy.

**Appendix F**

**Assessment for new CCTV System and continued use**

|  |
| --- |
| 1. **Organisation and Site:**
 |
| **2. Person Requesting CCTV**(The person requesting the CCTV system will be the responsible person for the system). |
| **3. Position:** |
| 1. **Reason and appropriateness of installation:**
 |
| **5. Purpose of the Scheme:** |
| **6. Has the information commissioner been informed of the new system? YES/NO** |
| **7. Are there agreed procedures in place for operational use and repairs to system:** |
| **8. Date & Signature:** |
| Please make sure all policy installation requirements are met. Any questions must be directed to Johan Celliers, Facilities, Fieldhead Hospital, Wakefield, tel: 01924 316000 |

**Authorisation:**

|  |
| --- |
| **Authorised by:** |
| **Position:** |
| **Date & Signature:** |

**New CCTV system installation procedure**

1. Requirement identified – Incidents / Assessment

2. Application made by Assessment for new CCTV system (Appendix C)

3. Application presented to H&S TAG / Estates TAG

4. Consultation with appropriate stake holders

5. Application approved by SMD

6. Order raised in line with system requirements

7. New system installed

8. New system signed off

**Appendix G**

**Review Checklist**

**CCTV and the Data Protection Act 2018**

 CCTV Code of Practice 2008

(Use a separate form for each CCTV System)

**TRUST: ………………………………………………………………………**

**SITE: ………………………………………………………………………………………..**

**Section One:** general details about the CCTV system

|  |
| --- |
| **1. Responsibility** |
| Who is responsible for the operation of the CCTV System? |
| Further details: |

|  |
| --- |
| **2. Contact Details** |
| Name: |  |
| Designation: |  |
| Telephone Number: |  |

|  |
| --- |
| **3. Purpose** |
| What is the purpose of the CCTV System? (e.g. prevention of crime & detection) |
| Has this purpose been registered with the Information Commissioner? | YES | NO |

**Section Two:** you should complete the checks specified under headings 4 to 7 for each camera operating as part of the CCTV system.

|  |
| --- |
| **4. Location** |
| Where is the camera/s sited? |
| What area(s) is this intended to monitor? |
| Does it monitor any other area not intended? (e.g. private gardens) | YES | NO |
| If yes, has consultation taken place with owners etc.? | YES | NO |
| Is the monitoring compatible with the registered purpose? | YES | NO |

|  |
| --- |
| **5. Signage** |
| Are there clear signs in place to inform the public they are entering a zone covered by CCTV? | YES | NO |
| If no, provide reason(s) for this: |
| If yes, are these signs clearly visible and legible? | YES | NO |
| Does the sign state the purpose of the scheme? | YES | NO |
| Does the sign identify who is responsible for the system? | YES | NO |
| Does the sign provide a telephone number? | YES | NO |
| Does the sign depict a camera?(\*If yes, the purpose of the monitoring does not require to be stated) | YES | NO |

|  |
| --- |
| **6. Quality of Images** |
| The following standards should be met to comply with the Data Protection Code of Practice: - |
| Equipment should be in good working order, well maintained and serviced on a regular basis | YES | NO |
| If tapes are used, these should be of good quality | YES | NO |
| The medium on which images are captured should be cleaned to ensure they are not recorded on top of images recorded previously | YES | NO |
| The medium should not be used if the quality of the images recorded has deteriorated | YES | NO |
| If the system records feature such as date, time etc. these must be accurate | YES | NO |
| Cameras should be protected from any physical/environmental risks (e.g. vandalism) | YES | NO |
| If an automatic facial recognition system is used to match images captured against a database of images, both sets of images should be clear to ensure an accurate match. The match should also be verified by a human operator | YES | NO |
| Clear written procedures should be in place to ensure damaged equipment is fixed within a specific time period | YES | NO |

|  |
| --- |
| **7. Processing of Images** |
| The following standards should be met to comply with the Data Protection’s Code of Practice:- |
| A Retention Policy should be in place identifying the length of time recorded images require to be kept | YES | NO |
| Images kept during the retention period or for evidential purposes, should be retained in a secure place to which access is controlled | YES | NO |
| Once the retention period has expired, images should be removed or erased | YES | NO |
| The Data Protection’s Code of Practice should be referred to when removing the medium on which images have been recorded for use in legal proceedings | YES | NO |
| Monitors displaying images should be viewed by authorised staff only | YES | NO |
| Viewing of recorded images should take place in a restricted area and on a strict ‘need to know basis’ | YES | NO |
| Access to recorded images should be restricted to authorised staff only | YES | NO |

**Appendix H**

**Maintenance Procedures for CCTV Systems**

**CCTV systems failure** must be reported ASAP to the department manager. An Incident form must also be completed.

All unexpected damage and repairs to the CCTV systems should be reported to the Facilities Hotline, on 01226 644030 or on [Log a job (swyt.nhs.uk)](http://nww.swyt.nhs.uk/facilities/Pages/planet-fm.aspx)

For further advice and support please contact:

Johan Celliers: 07771345275

John Sanderson: 07920535209

Tony Tipton: 07775220773

All unexpected repairs and maintenance will need a purchase order raised under the local departmental budget.

The Estates department will then assess and repair or contact individual contractors and request repairs to be completed.

**Maintenance Log must be completed for all works carried out.**

**Appendix I**

**Equality Impact Assessment template to be completed for all policies, procedures, and strategies**

***Appendix 4* Date of Assessment: 7th April 2021**

As a trust wide policy, the assessment includes demographics’ for the four areas covered by the trust as below.

Assessment of the SURVEILLANCE SYSTEMS Policy & Guidance has not highlighted any Equality Impact issues

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | White | Asian | Black | Mixed | Chinese & Other |
| England % av. | 85.5 | 5.1 | 3.4 | 2.2 | 1.7 |
| **Kirklees** |  |  |  |  |  |
| % average | 79.1 | 15.7 | 1.9 | 2.3 | 0.7 |
| **Barnsley** |  |  |  |  |  |
| % average | 97.9 | 0.7 | 0.5 | 0.7 | 0.2 |
| **Calderdale** |  |  |  |  |  |
| % average | 89.6 | 7 | 0.9 | 1.3 | 0.6 |
| **Wakefield** |  |  |  |  |  |
| % average | 95.4 | 2.6 | 0.77 | 0.9 | 0.29 |

*Taken from Census 2011 data*

|  |  |  |
| --- | --- | --- |
|  | **Equality Impact Assessment Questions:** | **Evidence based Answers & Actions:** |
| **1** | **Name of the document that you are Equality Impact Assessing** | SURVEILLANCE SYSTEMS Policy |
| **2** | **Describe the overall aim of your document and context?****Who will benefit from this policy/procedure/strategy?** | This policy applies to all surveillance camera systems (CCTV, ANPR, Body Worn Video Cameras (BWV)) which are used for the general purpose of crime prevention and detection and public safety. South West Yorkshire NHS Foundation Trust is the responsible owner of various surveillance systems and conforms to the Data Protection Act (UK GDPR), Surveillance Camera Commissioners and Home Office Camera Codes of Practice.All identifiable subjects |
| **3** | **Who is the overall lead for this assessment?** | Johan Celliers – Security Adviser  |
| **4** | **Who else was involved in conducting this assessment?** | Equality and Engagement Leads |
| **5** | **Have you involved and consulted service users, carers, and staff in developing this policy/procedure/strategy?****What did you find out and how have you used this information?** | No – not applicable, as the SURVEILLANCE SYSTEMS Policy & Guidance primarily covers staff related injuries, diseases or organisational near misses. |
| **6** | **What equality data have you used to inform this equality impact assessment?** | **Workforce data**As per workforce annual report 2020 * The Trust currently employs 4,328 staff delivering a range of services including mental health, learning disability, forensic, physical health and an extensive range of community services.
* The Trust split of 77.9% female to 22.1% male is reflected approximately across most areas, except for Medical Staff (36%/64%). ***As in previous years, female staff make up over three quarters of Trust staff***
* As in previous years, the highest number of Trust staff fall in the age bands ***40-49*** and ***50-59*** with over 55% of the total staff being between 40 and 59. Just over 42% of medical staff are between 40 and 49. Support Services have the highest percentage of staff in the 60-69 age bands with 14% (102) being 60 or over
* The data shows that **6.1%** of our staff consider themselves to have a **disability,** the same figure as last year. The total number of staff is 266, this is an increase of 11 since last year.
* The Trusts staff profile has a larger White British representation than the local demographic of the people that it serves collectively. Trust wide, 90% of the total staff in post are white British which is similar to previous years and equates to an over-representation of 1.3% (last year 1.1%). Mixed race staff are underrepresented by 0.2%, Chinese staff are over-represented by 0.2%, Black staff are over-represented by 1.6% and South Asian staff are under-represented by 3.2%. However, the Trust’s local demographic has large variation in BAME representation and there is a significant under-representation of South Asian staff in Kirklees/Calderdale (exact figures not available due to mixed teams)
* The number of staff who have not stated their religious belief (Unknown) has decreased slightly from 2018 (23%) to just below 21% currently. Staff reported as 48% Christianity, 3%Islam, 12% other and 17% Atheism.
* There has been a significant increase in the number of staff reporting their religion and sexual orientation. Currently 83% of staff have provided data indicating their sexual orientation, which is a slight improvement on last year’s figures.
 |
| **7** | **What does this data say?** | This data confirms that the Trust workforce has a diverse make up and that we should be aware of any obvious trends involving over seven day injuries involving any particular strand of the workforce, i.e. Race, Disability, Gender, Age or sexual orientation |
| **8** | **Taking into account the information gathered above, could this policy /procedure/strategy affect any of the following equality group unfavourably:** | **No** | Far more likely that a person’s job role will impact on their risk factor of being affected by a reportable over seven day injury |
| **8.1** | **Race** | **No** | ***Race***Taken from Census 2011 for each areaAs above, it is far more likely that a person’s job role will impact on their risk factor of being affected by a reportable over seven day injuryPeople who may not read or speak English as their 1st Language can via Trust commissioned serviceAccess easy read/pictorial symbols. |
| **8.2** | **Disability** | **Noted** | ***Disability groups***

|  |  |
| --- | --- |
|  | **Day to day activities limited by disability** |
|  | Not at all | A little | A lot |
| England % av. | 47.2 | 13.2 | 4.2 |
| **Kirklees** |  |  |  |
| % average | 45.5 | 12.5 | 13.7 |
| **Barnsley** |  |  |  |
| % average | 76.1 | 11.3 | 12.6 |
| **Calderdale** |  |  |  |
| % average | 56.5 | 12.2 | 13.8 |
| **Wakefield** |  |  |  |
| % average | 77.93 | 9.33 | 8.31 |

*Taken from Census 2011 for each area*The Trust will be aware of any obvious trends involving over seven day injuries involving any group of staff reporting a disability |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **8.3** | **Gender** | Noted | ***Gender***

|  |  |  |
| --- | --- | --- |
|  | **Male** | **Female** |
| England % av. | 49.2 | 50.8 |
| **Kirklees** |  |  |
| % average | 49.4 | 50.6 |
| **Barnsley** |  |  |
| % average | 49.1 | 50.9 |
| **Calderdale** |  |  |
| % average | 48.9 | 51.1 |
| **Wakefield** |  |  |
| % average | 49 | 51 |

*Taken from Census 2011 data*Gender equality is reported as part of the Trust workforce approach. In terms of over seven day injuries, risks are more likely to be determined by job role. |
| **8.4** | **Age** | **Noted** | ***Age***It is far more likely that a person’s job role, rather than their age will impact on their risk factor of being affected by a reportable over seven day injuryAdditionally, young workers should and must also be covered by the Trust ***Work Environment Risk Assessment for a Workplace/Work Shadowing Placement*** risk assessment, that will reduce the risk of an over seven day injury – link below<http://nww.swyt.nhs.uk/health-safety/Documents/Young%20Workers%20Risk%20Assessment.doc>  |
| **8.5** | **Sexual orientation** | **Noted** | ***Sexual orientation***It is far more likely that a person’s job role, rather than their Sexual orientation will impact on their risk factor of being affected by a reportable over seven day injury |
| **8.6** | **Religion or belief** | **Noted** | ***Religion or belief***

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Christian** | **Buddhist** | **Hindu** | **Jewish** | **Sikh** | **Muslim** | **Other** | **No religion** |
| England % av. | 71.8 | 0.3 | 1 | 0.5 | 0.7 | 10.1 | 0.2 | 15.1 |
| **Kirklees** |  |  |  |  |  |  |  |  |
| % average | 67.2 | 0.2 | 0.3 | 0.1 | 0.7 | 10.1 | 0.2 | 14 |
| **Barnsley**   |  |  |  |  |  |  |  |  |
| % average | 59.4 | 0.5 | 1.5 | 0.5 | 0.8 | 5 | 0.4 | 24.7 |
| **Calderdale** |  |  |  |  |  |  |  |  |
| % average | 60.6 | 0.3 | 0.3 | 0.1 | 0.2 | 7.8 | 0.4 | 30.2 |
| **Wakefield** |  |  |  |  |  |  |  |  |
| % average | 66.4 | 0.16 | 0.25 | 0.04 | 0.12 | 2.0 | 0.3 | 24.4 |

*Taken from 2011 Census data*It is far more likely that a person’s job role, rather than their Religion or belief will impact on their risk factor of being affected by a reportable over seven day injury |
| **8.7** | **Transgender** | **Noted** | ***Transgender***It is far more likely that a person’s job role, rather than being Transgender will impact on their risk factor of being affected by a reportable over seven day injury |
| **8.8** | **Maternity & Pregnancy** | **Noted** | ***Maternity & Pregnancy***<http://nww.swyt.nhs.uk/health-safety/Documents/Pregnancy%20Risk%20Assessment%202019.doc> All pregnant, and new mothers should, and must be covered through the Trust ***Health and Wellbeing for Pregnant Workers and New Mothers Risk assessment & action plan*** (link above)As such, the risks of an over seven day injury are greatly reduced. |
| **8.9** | **Marriage & Civil partnerships** | **Noted** | ***Marriage & Civil partnerships***Marriage and civil partnerships are not considered to be a factor in staff suffering an over seven day reportable injury whilst in the work environment |
| **8.10** | **Carers\*Our Trust requirement\*** | **Noted** | EASY to Navigate site maps that shows key Trust Locations at FHH/KH sites and other larger sites Folly Hall/Drury Lane can be found in the Trust’s website: [Buildings Archive | South West Yorkshire Partnership NHS Foundation Trust](https://www.southwestyorkshire.nhs.uk/buildings/)It’s likely that every one of us will have caring responsibilities at some time in our lives with the challenges faced by carers taking many forms. Many carers juggle their caring responsibilities with work, study and other family commitments. Some, younger carers, are not known to be carers and this means that the sort of roles and responsibilities that carers must provide varies widely.Within the local footprint of South West Yorkshire Partnership NHS Foundation Trust, there is an estimated **160,000 unpaid carers** |
| **9** | **What monitoring arrangements are you implementing or already have in place to ensure that this policy/procedure/strategy:-** | Regular discussions around SURVEILLANCE SYSTEMS notifications are undertaken at Safety & Resilience TAG & RRPI TAG meetings. Over the course of the policy lifetime there will be robust evaluation undertaken with regard to potential themes from an Equality perspective that could emerge such as HCA, Gender - Female and Age – Young etcAny difficulties related to an impact of equality will be addressed. |
| **9a** | **Promotes equality of opportunity for people who share the above protected characteristics;** | All Health & Safety Policies provide equality of opportunity, and promote personal responsibilities for everyone, including anyone with a protected characteristic or particular workforce strand. |
| **9b** | **Eliminates discrimination, harassment and bullying for people who share the above protected characteristics;** | All Health & Safety Policies contribute to the elimination, discrimination, harassment and bullying for everyone including anyone with a protected characteristics or particular workforce strand. |
| **9c** | **Promotes good relations between different equality groups;** | All Health & Safety Policies contribute to good relations between different equality groups |
| **9d** | **Public Sector Equality Duty – “Due Regard”** | We are confident that the Trust Health & Safety approach contributes to the effectivePublic Sector Equality Duty – “Due Regard” |
| **10** | **Have you developed an Action Plan arising from this assessment?** | To keep the Safety & Resilience and RRPI appraised of over seven day injury incidents |
| **11** | **Assessment/Action Plan approved by** | Alan Davis, Director of Human Resources, OD and Estates  |
|  |  | **Signed:** **Date:** **Title:**  |
| **12** | ***Once approved, you must forward a copy of this Assessment/Action Plan to Equality & Engagement Managers - Aboo Bhana (******Aboobaker.Bhana@swyt.nhs.uk******) and Zahida Mallard (******Zahida.Mallard@swyt.nhs.uk******)*** **Please note that the EIA is a public document and will be published on the web.****Failing to complete an EIA could expose the Trust to future legal challenge.** |  |

*If you have identified a potential discriminatory impact of this policy, please refer it to the Equality & Engagement Development Managers together with any suggestions as to the action required to avoid/reduce this impact.*

*For advice in respect of answering the above questions, please contact the Equality & Engagement Managers.*

**Appendix H - Checklist for the Review and Approval of Procedural Document**

*To be completed and attached to any policy document when submitted to EMT for consideration and approval.*

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Title of document being reviewed:** | **Yes/No/Unsure** | **Comments** |
| **1.** | **Title** |  |  |
|  | Is the title clear and unambiguous? | YES |  |
|  | Is it clear whether the document is a guideline, policy, protocol or standard? | YES |  |
|  | Is it clear in the introduction whether this document replaces or supersedes a previous document? | YES |  |
| **2.** | **Rationale** |  |  |
|  | Are reasons for development of the document stated? | YES |  |
| **3.** | **Development Process** |  |  |
|  | Is the method described in brief? | YES |  |
|  | Are people involved in the development identified? | YES |  |
|  | Do you feel a reasonable attempt has been made to ensure relevant expertise has been used? | YES |  |
|  | Is there evidence of consultation with stakeholders and users? | YES | EMT, Safety and Resilience TAG, Police.  |
| **4.** | **Content** |  |  |
|  | Is the objective of the document clear? | YES |  |
|  | Is the target population clear and unambiguous? | YES |  |
|  | Are the intended outcomes described?  | YES |  |
|  | Are the statements clear and unambiguous? | YES |  |
| **5.** | **Evidence Base** |  |  |
|  | Is the type of evidence to support the document identified explicitly? | YES |  |
|  | Are key references cited? | YES |  |
|  | Are the references cited in full? | YES |  |
|  | Are supporting documents referenced? | YES |  |
| **6.** | **Approval** |  |  |
|  | Does the document identify which committee/group will approve it?  | YES |  |
|  | If appropriate have the joint Human Resources/staff side committee (or equivalent) approved the document? | YES |  |
| **7.** | **Dissemination and Implementation** |  |  |
|  | Is there an outline/plan to identify how this will be done? | YES |  |
|  | Does the plan include the necessary training/support to ensure compliance? | YES | Estates and Security staff |
| **8.** | **Document Control** |  |  |
|  | Does the document identify where it will be held? | YES |  |
|  | Have archiving arrangements for superseded documents been addressed? | YES |  |
| **9.** | **Process to Monitor Compliance and Effectiveness** |  |  |
|  | Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document? | YES |  |
|  | Is there a plan to review or audit compliance with the document? | YES |  |
| **10.** | **Review Date** |  |  |
|  | Is the review date identified? | YES |  |
|  | Is the frequency of review identified? If so is it acceptable? | YES |  |
| **11.** | **Overall Responsibility for the Document** |  |  |
|  | Is it clear who will be responsible implementation and review of the document? | YES |  |

**Appendix J - Version Control Sheet**

*This sheet should provide a history of previous versions of the policy and changes made*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Status** | **Comment / changes** |
| 3.1 | 09/13  | Johan Celliers | Draft | Updated and revised policy in line with NHSLA requirements and Revised CCTV Code of Practice 2008. |
| 3.2 | 10/13 | Johan Celliers | Draft | Included comments from various colleagues after draft circulated on 22/09/13 |
| 3.3 | 05/14 | Johan Celliers | Draft | Included recommendations after consultation with union representatives. |
| 3.4 | 08/14 | Johan Celliers | Draft | Included comments from last circulation |
| 3.5 | 09/14 | Johan Celliers | Draft | Include final comments from H&S Trust Action Group. |
| 3.6 | 01/18 | Johan Celliers | Draft | Scheduled revision, incorporating comments from Safety & Resilience and Sub Group members |
| 3.7 | 02/18 | Johan Celliers | Draft | Incorporate and update references to statutory guidance and good practice.  |
| 3.8 | 05/21 | Johan Celliers  | Draft  | Policy Revision: 1. Include Data Protection Act 2018 and GDPR 2. Replace - term LSMS with Security Adviser 3. Remove - references to NHS Protect and include Centre for the Protection of National Infrastructure (CPNI) as national technical authority. 4. Full revision of reference documents 5. Introduce - PSeMS as annual assurance model 6. Use of BWV in handling security incidents |
| 3.9 | 06/21 | Johan Celliers | Draft |  |