Barnsley Hospital NHS
NHS Foundation Trust

Trust Security Policy

May 2021

Document Control

Author / Contact	Lead Healthcare Security Manager Head of Business Security. Ext.1386	
Document Ref		
Equality Impact Assessment	Yes	Date 1st May 2021
Version	V7	
Status	Policy Revision – Update Visitor & I/D Badge measures 1. Keypad codes or other sensitive information not to be affixed to cards 2. Copies of cards not to be posted on social media 3. New Appendix 3 – General Security Guide	
Publication date	May 2021	
Review date	May 2024	
Approval recommended by	Health & Safety Group	Date: June 2021
Approved by	Quality & Governance Committee	Date: June 2021
Distribution	Barnsley Hospital NHS Trust-intranet Please note that the Intranet version of this document is the only version that is maintained. Any printed copies must therefore be viewed as "uncontrolled" and as such, may not necessarily contain the latest updates and amendments	

Table of Contents

1 Introduction

Barnsley Hospital NHS Foundation Trust (the Trust) recognises its responsibility to have effective security measures in place in order to provide a safe environment for its patients, staff and visitors, by the reduction of security hazards and minimisation of crime on the premises under its control. This responsibility needs to be achieved whilst still recognising the need for the site to be easily accessible to patients and visitors.

Operational security on the Barnsley Hospital site is provided by the Site Security Team: 24 hours a day, 365(6) days a year.

Corporate security and strategy are provided by the BFS Business Security Unit under the direction of the Trust nominated Security Management Director (SMD) and managed by the Managing Director of BFS.

Site Security Team

The uniform site security team (SIA licensed security officers) maintain a 24-hour security presence within Barnsley Hospital NHS Foundation Trust, to deal with security emergencies and operational issues, oversee visitor and staff car parking and general traffic on each site. The unit and team objectives are the:

- Protection of all Trust service users and staff from all crime;
- Prevention of loss of Trust assets because of crime or negligence;
- Protection of Trust property against malicious acts, flood, damage and trespass;
- Preservation of good order on the Trust site;
- Maintenance of the prestige and reputation of the Trust;
- Detection and reporting of offenders to the Head of Business Security and/or the local police if crime or misconduct is committed in relation to the above;
- Compliance with the approved Assignment Instructions (AI s).

The uniform team can be contacted on 01226 431837 (Ext.1837) Site Manager on 01226 431836 (Ext.1836). Emergencies contact 3333.

2 Objective

This policy outlines the processes by which the Trust/BFS manages the provision of security services and to encourage all staff to work together, and with external agencies, to minimise risk of security breaches. Its objectives are to:

- Protect patients, staff and visitors from attack
- Prevent loss or damage to the assets of the Trust
- Prevent loss or damage to the property of patients, staff and visitors
- Prevent fraud
- Preserve good order on Trust premises
- Raise the awareness of crime prevention with staff, patients and visitors
- Outline the security surveys and assessments necessary to achieve an effective security agenda

3 Scope of the Policy

This policy applies to all staff of Barnsley Hospital NHS Foundation Trust, Barnsley Facilities Services, the contracted security provider and other parties delivering services on the hospital site, whilst accepting for staff other than those of the Trust their appropriate line management. Whilst the policy outlines how the Trust will manage its security issues, implementation does not replace the personal accountability of all staff in this regard.

'In the event of a serious infection outbreak, flu pandemic, major or critical incident, the Trust recognises that it may not be possible to adhere to all aspects of this document. In such circumstances, staff should take advice from their manager and all possible action must be taken to maintain ongoing patient and staff safety'

.

4 Policy

The Security Team will provide a comprehensive 24-hour security service, 365(6) days per year, which will include but not be limited to the following elements:

- Crime prevention
- Responding to security incidents
- Foot patrols
- Monitoring control of access
- Car parking oversight
- Incident reporting
- Dedicated security to high risk areas/departments
- Surveillance and monitoring systems e.g. closed-circuit television and body worn video.
- Escort duties (critical emergencies only)
- Responding to security/emergency contingency plans
- Responding to medical emergencies and site intruder alarms
- Responding to fire alarms, informing the fire service, initial investigation as to cause, meeting and escorting fire fighters under safe conditions if required.

4.1 Protective/Physical Security

The physical security of buildings:

This is the responsibility of all individuals who work in wards, departments, offices and store areas. This will be achieved by individuals contributing to the protective security of their locality and denying uncontrolled or unauthorised access, except to those who have a valid and legitimate reason to enter. Further advice in respect of visitors is contained in Appendix 3. This is particularly important in areas of high risk to people and property, such as maternity or theatres. Security officers will undertake random (Project Dixon) patrols, around all wards and corridors, paying particular attention to those areas that have medical, computer, television and video equipment. Whilst the majority of offices should be locked, Security Officers will report any breaches of security via the defined procedures which include an escalation process via managers in case of repeated insecurities. In addition, unannounced visits and audits will be carried out by the local Police Community Support Officers, security staff and the BFS Business Security Unit, to check general compliance with security.

The control and issue of keys:

Departmental Keys:

Each Head of Department/Ward Manager holds responsibility for the management of the keys to their areas, other than electronic access control which are considered to be associated with the main entrance to the department. However, close liaison with the security staff, fire officer and estates is of paramount importance, to ensure access for emergencies or essential maintenance. Where departments hold keys, they must be kept in a secure cabinet in a secure location and on sealed, numbered rings with no other means of identification.

General – Keys:
A number of high-profile keys are held securely at Main Reception or with the Security Team. All keys kept at Main Reception will be signed for on issue and the identity of the signatory checked against the list of those authorised to withdraw the key and against the Trust ID Card of the staff member. Grand Master Keys are held by authorised members of staff and kept at secure locations.

Additional Keys, Locks and Key Pads:
No additional keys for internal or external doors must be cut, locks changed, or key pad installed without the express approval of the BFS Estates Team. The Trust security strategy is to discontinue the use of key pad locks and all requests must be forwarded to the BSU for a security survey and threat assessment.

Door Codes and Key Pad Locks.
All door codes and pin numbers for key pad locks must be communicated to the Security Team and Trust Security Management hold pass keys to these locks. Key pad locks must have a key override facility in case of any urgent entry requirements. Codes must not be affixed to I/D cards.

Departmental Cleaning:
Where domestic staff require access to a department which holds valuable equipment or classified material they must draw the keys from main reception. They will not have uncontrolled access to departmental keys or retain bunches or duplicate keys for their own use. Domestic staff are issued with ID access cards for use within their designated working areas.

Entrance thoroughfares:
All entrance thoroughfares are clearly signposted and designated as such. Emergency fire exit doors that are not designed as thoroughfares are security signed to control unauthorised usage and monitored on the Trust CCTV system.

Intruder alarm systems:
A number of intruder alarms have been introduced across the Trust and have been designed to ensure that inadvertent activation is minimised and protective security increased

The existence of all alarms has been communicated to the switchboard and security office, which are manned 24-hours a day. This will ensure an effective response by security staff, who will be informed immediately by switchboard and, as such, eliminate any delay in preventing intruders and obviate the need for other persons to report a sounding alarm. To assist the switchboard there is an option to site a personal radio for linking with the patrolling Security Officer.

Any additional alarm requirements must be discussed with the Business Security Unit.

4.2 Close circuit television (CCTV), Body Worn Video (BWV) and Drone (UAV) Equipment

CCTV cameras are located at numerous locations within the Trust, as one of the measures to reduce crime levels and ensure the Trust is a safer place for patients, staff and visitors.

The Trust is mindful of human rights and privacy concerns about the use of CCTV and BWV and the Trust ensures it is lawfully licensed and registered. Security Officers are equipped with Body Worn Video (BWV) devices and are fully trained in their use. The Trust complies fully with GDPR and the Data Protection Act and the first principle of the Act requires that personal data shall be obtained and processed fairly and lawfully. To that end, visible notices are sited at appropriate locations throughout the Trust, informing people that CCTV cameras are in operation. Security officers have a strict code of conduct in respect of the use of BWV and should inform anyone present that the device will be activated for recording purposes. The Trust is the first NHS organisation to be accredited under the Biometrics & Surveillance Camera Code of Practice 2013 and also fully complies with all other national advice and guidance. The Trust has a Surveillance Camera Policy and Procedures document which also includes the use and deployment of BWV and UAVs (drones).

External lighting:
All external lighting is in a safe and operational condition. Checks will be made at regular intervals by security staff.

Access to roof areas:
Roof access is made impracticable by ensuring that access doors and other routes of direct access are always locked. Temporary buildings and other structures shall be located such that they do not offer easier access to roofs. All ladders and steps must be locked away. All scaffolding shall be erected with an anti-climb barrier and all access ladders closely checked during the working day and removed during periods of non-activity.

VIP Visits:
The Trust has a full policy and procedures for the visit of VIPs and access to wards and other departments. All visits must be authorised by a Trust Director and coordinated by the Communications and Media Team. All VIP visitors must be accompanied at all times by a Trust senior manager.

4.3 Security of Assets

Assets and equipment:
All assets and equipment will be clearly marked and held on an inventory, in accordance with Standing Financial Instructions. Asset marking may include RFID, ultra-violet and cell-marking (Smart Water) technologies.

IT equipment:
All information technology assets shall be security marked by the IT Department.

Consumables:
All consumables should be controlled and kept in a secure area. Any incidents of theft shall be thoroughly investigated and, where appropriate, the Trust disciplinary procedure invoked.

Cash:
Very precise processes are in place for the Security Team to transfer cash between areas and for emptying cash boxes, such as those in the car parks. Similar processes are in place for the transit and handling of cash by General Office staff. These processes also include clear instructions as to the appropriate subsequent storage of these monies.

Workstations:
Where applicable, staff must ensure that their workstation (desk) is kept clear at the end of the working day: all files should be returned to a filing cabinet or kept in an

orderly fashion in a specific filing tray. If confidential material is left on desks, this must not be left unattended unless the area is secure.

Patient records:
The policy and procedures for the protection, transmission, handling and storage of records on the entire Trust site are contained in the appropriate policies. The Medical Records Manager has direct responsibility for ensuring the correct procedures are followed whilst records are located in the Trust libraries and whilst in transit. It is the responsibility of all staff to ensure the security of records whilst in their departments/wards.

Patient property:
Patient property must be administered in accordance with the Trust Patient Property policy and the necessary disclaimers signed and processes relating to witnessing, storage and transit strictly followed.

Illicit or Indecent property:
This material is not allowed to be kept or stored on Trust premises. This includes illicit drugs, alcohol or any indecent/pornographic media.

Drugs and medicines:
Staff should refer to the Trust's policies for medicine and drugs management and the processes strictly followed.

Reporting Crime & Subsequent Actions:
All crime including theft should be reported as a crime and the security team notified in the first instance, so that appropriate investigation of the theft may be organised and undertaken by the BFS Business Security Unit and/or local police. Trust equipment and assets considered to be 'missing', 'borrowed' or otherwise displaced must be subject of robust checks and investigation. In the event that the equipment is not located a report of crime must be made via a Datix report and call to the police. The police crime number must be added to the Datix report along with any attending police officer's details (name & collar number).

It may be necessary because of the circumstances of a theft, other crime or current investigation to ask personnel working or visiting on site to consent to a search of him/her and their outer clothing only, bags/cases and vehicle. The law on this subject is quite clear: no person has any right to search another without that person's consent having been freely given. Searching will only be undertaken as part of a current investigation. The Trust reserves the right to check and search lockers, desks, offices and property spaces. If required these can be forcibly opened and further details are contained in the Trust Locker Policy. In all other cases the following procedure must be followed:

- The person is to be asked for consent to the search of their outer clothing or possessions and their work area, if that is provided by the Trust
- The person must be informed that she/he has the absolute right to refuse consent, without any form of penalty. No persuasion of any nature is to be made to obtain consent and no threats, implied or expressed
- If consent is refused, the proposed search will NOT take place. A refusal may initiate involvement by the police.
- If full and free consent is obtained, the person is to be asked to nominate a witness to be present. If he/she cannot nominate a witness, he/she is to be asked to approve a witness nominated by the searcher. No search must be carried out in the absence of a witness or in the presence of a witness unacceptable to the person being searched.

- Females, their possessions, locker, office and outer clothing must only be searched in the presence of another female.
- In all cases a personal search must be confined to outer clothing: under no circumstances is a body or other intimate search to be made
- Accurate notes must be made, and retained, in respect of the search and the subsequent sequence of events. Dates, times, places, names of those searched, witness etc. must all be recorded in the Manager's and/or Security Officer's notebook
- If articles alleged to have been stolen are found, the facts must be noted and the matter referred to a higher authority for a decision as to whether or not the investigation will continue or the police informed. A list of the articles found in the person's possession is to be given to that person as soon as possible after the search.
- If nothing of an incriminating nature is found, the person is to be issued with a certificate stating that he/she was searched at (time) on (date) in (place) in the presence of (witness) and he/she was not in possession of the allegedly stolen items. The certificate must be signed by the person performing the search.
- It is anticipated that the occasions when searching individuals is considered desirable will be rare and that, generally, a case serious enough to warrant such a search may be referred to the police.

4.4 Security of Personnel

Identification:
Whilst on duty all Trust staff, irrespective of status and including temporary, bank and agency and contracted staff, must wear a Trust identity (ID) card, except in circumstances where it poses a risk to health and safety e.g. in operating theatres. It must be produced when requested by a senior manager or member of the security team/unit. Individuals must report any loss or damage of the ID card on Datix and abide by the reporting conditions accepted under signature. All cards must be returned on termination of employment. Applications for a Trust ID card should be made via the appropriate form available on the Trust Intranet site and signed by their Line Manager. The card remains the property of the Trust and can be withdrawn should the circumstances dictate. ID and Smartcards withdrawn from staff under suspension are to be retained by the line manager and made available on their return to work. Managers must inform the BFS Business Security Unit of the card status to allow it to be disabled and enabled as required. Photographs or copies of any Trust pass cards must not be posted on social media.

Visitors
Staff should stop visitors from entering a ward or department and ask who they are visiting or the location of an appointment. Circumstances in which staff are uncomfortable or concerned should be reported to their line manager or directly to the security team on 1837. Staff should never put themselves at risk and if in any doubt should inform the security team.

Visitors should be escorted by a member of staff to their host and introduced. They should never be left alone or allowed in any office unaccompanied. Prior to this their identity should be verified – Appendix 3 contains further details.

Restricted areas of access:
Enhanced security arrangements are in place for the following areas:

- Maternity areas including NNU
- Children's Wards
- Nuclear Medicine
- Pathology block

- Mortuary building
- Basement
- Roof areas
- Security Office & BSU
- All pharmacy areas

All entrance and exit doors must be secured such that access is only possible through dedicated entrances, via a swipe card, manual keys and/or keypad.

Unauthorised photography and recording:
Unauthorised photography, sound and/or video recording is strictly prohibited on the Trust site and persons found engaged in this activity will be requested to cease immediately and to delete any data obtained or retained. The security team will inform the police of all occurrences.
Authority for photography and/or recording must be requested from a Trust senior manager, senior nurse or the Corporate Communications Department.

4.5 Pre-employment checks

To ensure that the Trust complies with employment legislation and directives laid down by the Department of Health; all new employees will undergo pre-employment checks. As a minimum, this will be confirmation of their identity, the right to work, health clearance and appropriate references and should equate to central government's Baseline Personnel Security Standard (BPSS). There are however other circumstances, when other clearances such as Disclosure and Barring Service (DBS) standard or enhanced checks need to be undertaken prior to (or during) employment. Further advice and guidance on this matter can be found in the Human Resources Department Recruiting and Selection procedures and the Business Security Unit. In the interests of staff and patient safety recruiting managers must check all ID submitted is current, valid and applies to the person being recruited/interviewed.

4.6 Violence and Aggression

Barnsley Hospital's response to violent, aggressive and challenging behaviour incidents;

At any time during a current investigation, the Trust may pursue a civil action on behalf of the member of staff and, in conjunction with the BFS Business Security Unit and/or a criminal action via the Police and may consider pursuing an appropriate action under the Challenging Behaviour procedures or Anti-Social Behaviour legislation.

Training;
Appropriate staff will receive training in customer care and/or violence and aggression management (conflict resolution) and possibly breakaway or physical intervention techniques appropriate to their level of risk. Further information is available in the Trust Violence and Aggression policy.

Terrorist/Bomb Threats and Hoaxes;
Any member of staff who discovers a dangerous substance, bomb or person carrying a suspected biohazard should contact switchboard on 3333 and ask the switchboard staff to activate the Suspicious Packages and Bomb Hoax procedures. Switchboard will immediately contact the security team and/or local police if required. All staff must be aware of the HOT principles contained in those procedures and included in their induction training.

4.7 Security Surveys and Assessments

Undertaking threat and risk reviews;
There are a number of ways in which security surveys and assessments are carried out, to ensure the Trust is doing its reasonable best to manage security issues and provide as safe an environment as possible for its staff, patients and visitors. These include:

- An ongoing review of departmental security assessments by the BFS Business Security Unit
- Local security survey and assessments carried out during the year, by the Trust Security Representatives
- Unannounced assessments by the police including the CTSA or other agencies

Centre for the Protection of National Infrastructure (CPNI):
The CPNI is the national technical authority in respect of protective security and the government authority for providing protective security advice to the UK national infrastructure. Health is a named sector within the UK national infrastructure and the role of CPNI is to protect security by helping reduce the vulnerability to all threats including terrorism. A number of key security strategies adopted by the Trust are based on CPNI advice and guidance.

Action following threat or risk assessments

<u>Annual security assessment and the Protective Security Management System (PSeMS)</u>
The BFS Business Security Unit is responsible for:

- Developing an organisational wide action plan
- Monitoring the implementation of the action plan through receipt of a monthly report from the Site Security Team linked to the regular report by the Unit to the Health & Safety Group
- Ensuring any identified risks and concomitant action plans are included the appropriate risk register or security survey
- The provision of an annual security management assurance via PSeMS.

<u>Local Threat and Risk Reviews carried out during the year</u>
The Trust Security Representatives are responsible for

- Ensuring any identified risks and concomitant action plans are placed on the appropriate risk register and included in the appropriate security survey

<u>Unannounced security surveys and assessments</u>

- Authorised members of multi-agency inspection teams and/or the Police including the CTSA will feedback to the BFS Business Security Unit following unannounced assessments. The Department will then ensure that any identified risks and concomitant action plans are reported to the appropriate committee and SMD and are also placed on the appropriate risk register in accordance with the Trust risk assessment procedures.
- Risks and action plans placed on the risk registers will be monitored by the appropriate Trust Governance Committees

4.8 Incident Reporting

All security incidents must be reported in accordance with the Trust incident reporting procedures and a Datix entry made. The responsibility for reporting sits with the particular ward or department where the incident(s) occurred and not with the uniform security team.

The Specialist in Business Security with the Security Site Manager will review and analyse any reported security incidents, in an effort to ensure that any necessary changes/improvements to security are made and to ensure the environment remains as safe as possible for all service users and staff.

4.9 Lockdown

The Healthcare Security Manager(s) shall ensure that Trust and departmental lockdown risk profiles are completed. It is the responsibility for all departments to have policies and procedures in place to be able to lockdown their department/wards in the event of a critical incident. Guidance and advice is available by contacting the Business Security Unit who will advise.

What could initiate a Lockdown?

- Terrorist attack including Marauding Terrorist Attack (MTA)
- Child/Baby Abduction
- Clinical or Human Disease Outbreak (Flu pandemic) etc.
- Flood or another environmental incident
- Violent attacks/fights in the Emergency Department
- Chemical, Biological, Radiological attack
- Bomb Threats
- Missing or Wandering Patients

The list is not exhaustive or prescriptive

Types of Lockdowns

- Partial Lockdown
- Portable Lockdown
- Progressive Lockdown
- Full Lockdown.

Lockdown is used to ensure the safety and security of all the Trusts personnel, patients and assets in the event of a major incident and by doing so will protect the integrity of the Trust.

Trust Lockdown capability

The Trust’s use of proximity card security access will allow for partial, progressive or full lockdown of the main site and peripheral departments.

The Trust, as part of its business continuity and emergency preparedness, has a full Lockdown and Evacuation Plan

5 Roles & Responsibilities

Health & Safety Group

It is the responsibility of the Health & Safety Group to monitor adverse violence and aggression incidents and near misses at their regular meetings and to identify any emerging threat trends. In addition, the Committee will monitor risk registers and will escalate any appropriate threats or risks appropriately where identified as a result of security related incidents for inclusion in either the Trust Risk Registers or proactive action planning and response by the security teams.

Quality & Governance Committee
The Quality & Governance Committee have the delegated responsibility to approve all Trust Security and Emergency Resilience policies, procedures, surveys and plans. The Committee will assure that the structures and processes are in place to provide the frameworks to support and ensure that non-clinical risks are mitigated and assured appropriately. The Committee will further assure that any issue that threatens the Trust's ability to do this is managed and escalated appropriately and actioned planned accordingly. That new policy documents are reviewed and recommendations made to the Trust Board and to approve amended policies and procedures. The assurance is provided to the Trust Board in respect of controls to mitigate security risks and that all the relevant assurance programmes are in place and operating correctly.

The Security Management Director (SMD) has delegated and financial responsibility for security management. The SMD's remit also includes emphasising the security management needs of the Trust to the Board to ensure that responsibilities are taken seriously at the highest level. The Trust Director of Operations or the Managing Director of BFS have the authority to act for and on behalf of the SMD in all matters related to security management.

The Business Security Unit (Head & Specialist) are the Trust Healthcare Security Managers and are the accredited officers for managing both security and resilience issues in line with other Trust policies and procedures and the security team's assignment instructions (AI's). They are also responsible for providing specialist investigative expertise and for working with the Trust to provide an environment that is safe and secure for all users. The BSU staff are licensed by the SIA and hold National Security Vetting – SC Level Clearance.

The BSU will receive reports on any offences in connection with crime or misconduct on Trust premises and lead with any investigation that is required as a result of alleged unlawful or criminal activities and assist in aspects relating to fraud, whilst ensuring the involvement of the police or local counter fraud specialist as and when necessary. In addition, and in collaboration with the Centre for the Protection of National Infrastructure (CPNI), Counter-Terrorist Security Advisor (CTSA) and Designing Out Crime Officer (DOCO) provide advice on the planning and commissioning elements of any future hospital development. This advice should be sought at the earliest possible stage to ensure the external and internal assets of the Trust are adequately safeguarded.

The Uniform Security Site Manager has responsibility for the operational and day-to-day implementation of this policy.

The Security Team
The Site Security Team (SIA licensed Security Officers) will maintain a 24-hour security presence on the hospital site to deal with security emergencies and scheduled issues, visitor and staff car parking and general traffic. The Department objectives are the:

- Protection of life from malicious criminal activity
- Prevention of loss of Trust assets because of crime
- Protection of Trust property against malicious acts, flood, damage and trespass
- Preservation of good order in Trust property
- Maintenance of the prestige of the Trust
- Detection and reporting of offenders to the Security Manager if crime or misconduct is committed in relation to the above
- Compliance with the working and assignment instructions.

Managers and Heads of Department
Ward Managers and Heads of Department are responsible for ensuring:

- The security of their areas, their staff and of any patients, visitors and contractors within their ward or department.
- That all unused areas are locked and windows closed when not in use; particularly at night and at weekends. Areas containing items of expensive equipment must, where practicable, be kept locked at all times when not occupied. Confidential documents, particularly patient records, must be locked away, wherever possible, when a room or area is left unattended
- That, where computer equipment is used, the Trust policy is followed to ensure compliance with the requirements of the Data Protection Act.
- That their staff advise all new patients to be cautious with regard to the security of any valuables that may have been brought into hospital. Property must be recorded on admittance and all patients must be advised to give large amounts of money and any valuables to a relative or, should this not be possible, such items must be handed over to the Trust for safe-keeping. Reference must be made to the relevant policies relating to patient and staff property and that the Trust will not accept responsibility for lost or stolen personal property.
- That staff are security conscious and do not bring large amounts of money or valuables into the work place.

Security Representatives
Security & Resilience Representatives (CBU Managers) are linked to the site security team via regular briefings, Security and Emergency Resilience meetings and support network and have responsibility for actively pursuing any identified security issues within their area of responsibility.

All Staff
All staff, irrespective of status, are responsible for:

- Their personal security whilst at work within the Trust
- Wearing the Trust ID badge when in the workplace, except when it may pose an ongoing operational risk to health and safety (e.g. operating theatres).
- Producing the Trust ID card issued to them on the request of an identified Trust manager, Healthcare Security Manager or security officer.
- Not posting copies or photographs of I/D cards on social media
- Maintaining a secure environment for their fellow employees, patients and visitors and ensure, where possible, the protection of their property.
- Maintaining a secure environment for property and all assets belonging to the Trust
- Ensuring they are aware of this Security Policy and that they follow its requirements within their workplace
- Politely challenging anyone in their area that they do not recognise, providing it is safe to do so. If a member of staff sees anyone acting suspiciously, behaving unusually, smoking or is an area that they should not be, they should politely challenge and then must inform security on Ext 1837 or 1836 immediately and their line manager as soon as possible
- Ensuring that their office doors and windows are shut and locked when they leave work or when they leave their place of work for a period of time
- Ensuring that when they leave their place of work, expensive equipment and confidential papers, particularly patient records, are locked away and out of sight.

6 Associated Documentation and References.

Internal
Violence & Aggression Policy
Lone Worker Policy
Surveillance Camera Policy
Locker Policy
ID Card Policy
Unacceptable Behaviour Procedures.
Security Department Assignment Instructions (AI's)
Security Staff Toolbox Training
Patient Property Policy
Suspicious Packages & Bomb Hoax Procedures
Baby/Child Abduction Policy
Access Control Procedures
VIP Visitors Policy

External
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*
Surveillance Camera Commissioner – *Code of practice. A guide to the 12 principles*
Home Office Scientific Development Branch – *Is your CCTV system fit for purpose?*
Centre for the Protection of National Infrastructure (CPNI) – *Embedding Security Behaviours: using the 5Es*
Centre for the Protection of National Infrastructure (CPNI) – *Guide to Producing Operational Requirements for Security Measures*
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) – *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) – *Protective Security Management Systems (PSeMS). Guidance, Checklist and Case Studies.*
Data Protection, Information Commissioner's Office – *CCTV code of practice*
NHS England - *NHS National Standard Contract 2019/20*

7 Training & Resources.

Site Security Team training matrix and toolbox talks

A mandatory induction security awareness programme and information can be accessed via the Trust Intranet for all staff.

Let Us Know (LUK) confidential reporting line (1111)

General security awareness and crime reduction advice is available on the BFS Business Security Unit e-learning programme that is assessed and also accesses on the Trust induction programme

‘Not on My Watch’ and ‘It’s OK to Say’ videos accessible by staff on the Trust Intranet.

Conflict Resolution and Customer Care training are available based on training needs.

The BFS Business Security Unit will provide bespoke security management training to all Trust departments and staff on request.

Further details of the processes for dealing with security and counter-terrorist issues including VIP visits etc. are retained with the BFS Business Security Unit

- Daily C/T briefing
- Security Service, Military CPNI and CTU contacts
- Projects Argus-Health, Revise and Artemis.
- Action Counters Terrorism (ACT) and See, Check and Notify (SCaN) training
- NaCTSO and ‘Prevent’ advice

8 Monitoring and Audit

The Trust SMD and Managing Director of BFS will monitor the implementation of this policy.

Where monitoring has identified deficiencies, recommendations and action plans will be developed and changes implemented accordingly. Progress on these will be reported to the Quality & Governance Committee via the Health & Safety Group.

The BFS Business Security Unit will carry out an annual audit by sending questionnaires to a number staff on a random basis, to encompass a wide range of staff groups. A number of semi-structured interviews will also take place with staff members along with a full audit of requested data and information.

Annual review of security strategy against PSeMS submissions

Compliance will be reported to the Health & Safety Group and relayed to the Quality & Governance Committee.

Any subsequent actions required following the audit will be developed by the BFS Business Security Unit

Progress on the implementation of corrective actions required will be reported to the Health & Safety Group, annually until all corrective actions are completed.

9 Equality and Diversity

The Trust is committed to an environment that promotes equality and embraces diversity in its performance as an employer and service provider. It will adhere to legal and performance requirements and will mainstream equality and diversity principles through its policies, procedures and processes. This policy should be implemented with due regard to this commitment.

To ensure that the implementation of this policy does not have an adverse impact in response to the requirements of the Equality Act 2010 this policy has been screened for relevance during the policy development process and a full equality impact analysis conducted where necessary prior to consultation. The Trust will take remedial action when necessary to address any unexpected or unwarranted disparities and monitor practice to ensure that this policy is fairly implemented.

This policy and procedure can be made available in alternative formats on request including large print, Braille, moon, audio, and different languages. To arrange this please refer to the Trust translation and interpretation policy in the first instance.

The Trust will endeavor to make reasonable adjustments to accommodate any employee/patient with particular equality and diversity requirements in implementing this policy and procedure. This may include accessibility of meeting/appointment venues, providing translation, arranging an interpreter to attend appointments/meetings, extending policy timeframes to enable translation to be undertaken, or assistance with formulating any written statements.

9.1 Recording and Monitoring of Equality and Diversity

The Trust understands the business case for equality and diversity and will make sure that this is translated into practice. Accordingly, all policies and procedures will be monitored to ensure their effectiveness.

Monitoring information will be collated, analysed and published on an annual basis as part Equality Delivery System. The monitoring will cover the nine protected characteristics and will meet statutory duties under the Equality Act 2010. Where adverse impact is identified through the monitoring process the Trust will investigate and take corrective action to mitigate and prevent any negative impact.

The information collected for monitoring and reporting purposes will be treated as confidential and it will not be used for any other purpose.

Barnsley Hospital NHS
NHS Foundation Trust

Appendix 1

Equality Impact Assessment

Security Policy

May 2021

INITIAL ASSESSMENT STAGE 1 (part 1)

<table>
<tr><td>**Department:**</td><td colspan="3">Business Security Unit</td><td>**Division:**</td><td>Barnsley Facilities Services</td></tr>
<tr><td>**Title of Person(s) completing this form:**</td><td colspan="3">Head of Business Security</td><td>**New or Existing Policy/Service**</td><td>Existing</td></tr>
<tr><td>**Title of Policy/Service/Strategy being assessed:**</td><td colspan="3">Trust Security Policy</td><td>**Implementation Date:**</td><td>Review – May 2021</td></tr>
<tr><td>**What is the main purpose (aims/objectives) of this policy/service?**</td><td colspan="5">To combine legislation and guidance establishing a framework for proactive security management within the Trust.</td></tr>
<tr><td rowspan="5">**Will patients, carers, the public or staff be affected by this service?**
Please tick as appropriate.</td><td></td><td>Yes</td><td>No</td><td colspan="2" rowspan="5">If staff, how many individuals/which groups of staff are likely to be affected?
Safer working environments for Estates, Facilities and Estates staff.</td></tr>
<tr><td>Patients</td><td>X</td><td></td></tr>
<tr><td>Carers</td><td>X</td><td></td></tr>
<tr><td>Public</td><td>X</td><td></td></tr>
<tr><td>Staff</td><td>X</td><td></td></tr>
<tr><td rowspan="5">**Have patients, carers, the public or staff been involved in the development of this service?**
Please tick as appropriate.</td><td>Patients</td><td>X</td><td></td><td colspan="2" rowspan="5">If yes, who did you engage with? Please state below:
• Business Security Unit
• BFS Estates Management
• BFS Facilities Management
• Trust Security Team
• G4S Secure Solutions
• All Trust staff including volunteers, non-executive directors and governing body
• Trust Members
• Trust Service Users (Patients, Visitors, Relatives)
• All staff side organisations
• Barnsley Hospital Charity
• Contracted staff and service providers
• NHS Barnsley Clinical Commissioning Group
• NHS England
• South Yorkshire Police
• Yorkshire Ambulance Service
• Barnsley Metropolitan Borough Council including elected members
• Partners and Community Together (PACT – CSG)
• Ward Alliance Group
• Pogmoor Residents Association
• Old Town Residents Association</td></tr>
<tr><td>Carers</td><td>X</td><td></td></tr>
<tr><td>Public</td><td>X</td><td></td></tr>
<tr><td>Staff</td><td>X</td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

What consultation method(s) did you use?	Each section of the policy will be circulated internally and externally to appropriate partners and stakeholders to form part of the security, surveillance and ID card policies. Consultation is part of the induction and awareness programmes to staff and the policy is available via the Trust internet and intranet sites. All security procedures are outlined during exercises and during Projects SCaN, Revise, Artemis and ACT awareness programmes. Bespoke security briefings can be requested by any member of staff and all local community forums contribute to the awareness programme.

Equality Impact Assessment Stage 1 PART 2

Based on the data you have obtained during the consultation what does this data tell you about each of the above protected characteristics? Are there any trends/inequalities?

Barnsley Hospital NHS Foundation Trust has a duty to protect, secure and promote the health of the community at all times. The Trust strategy focuses on reducing health inequalities and the treatment of all members of the community including the most vulnerable and ensuring they are safe during this care. The purpose of the sections of the policy is to ensure appropriate, legal and necessary procedures for protecting patients, staff and Trust assets. Also, to combine legislation and guidance establishing a policy & procedures for investigations and support for outside agencies for use within the Trust and where required to provide evidence for further investigation thereby minimising any impact on the health of the Barnsley community irrespective of Race, Disability or Gender etc.

No trends or inequalities identified

What other evidence have you considered? Such as a ‘Process Map’ of your service (assessment of patient’s journey through service) / analysis of complaints/ analysis of patient satisfaction surveys and feedback from focus groups/consultations/national & local statistics and audits etc.

The Trust Security Policy ensures that actions and responses are proportionate, legitimate, necessary and justifiable. In addition, it will ensure that the use satisfies the requirement of addressing a pressing staff and patient security requirements described in Trust policy, the assignment instructions and NHS national advice and guidance. At all stages it will comply with the Data Protection Act and other legislation. In the case of the Human Rights Act 1998, there will be adherence to the requirements of Article 6 (Right to a fair trial) and in respect of Article 8 (Right to respect for private and family life, home and correspondence) since this is a qualified right, information will only be captured and processed to achieve a legitimate aim as detailed earlier. UAV assets will only be deployed strictly for aerial safety and survey purposes and are not considered either a surveillance or security resource.
The policy has been reviewed by the relevant Trust governance committees prior to being enacted and has undergone a rigorous privacy impact assessment.

The Trust 'Hospital Eyes' website fully explains security asset use and privacy and dignity aspects and translations can be freely provided if required. The policy outlines the full and comprehensive consultation process.

Equality Impact Assessment Stage 1 PART 3

ACCESS TO SERVICES

What are your standard methods of communication with service users?

Please tick as appropriate.

Communication Methods	Yes	No
Face to Face Verbal Communication	X	
Telephone	X	
Printed Information (E.g. leaflets/posters)	X	
Written Correspondence	X	
E-mail	X	
Other (Please specify) – Training and dedicated webpage	X	

If you provide written correspondence is a statement included at the bottom of the letter acknowledging that other formats can be made available on request?

Please tick as appropriate.

Yes	No
	X

But this service is provided on the Trust web links where the Framework is located.

Are your staff aware how to access Interpreter and translation services?

Interpreter & Translation Services	Yes	No
Telephone Interpreters (Other Languages)	X	
Face to Face Interpreters (Other Languages)	X	
British Sign Language Interpreters	X	
Information/Letters translated into audio/braille/larger print/other languages?	X	

EQUALITY IMPACT ASSESSMENT – STAGE 1 (PART 4)

Protected Characteristic	Positive Impact	Negative Impact	Neutral Impact	Reason/comments for positive or negative Impact Why it could benefit or disadvantage any of the protected characteristics
Men	Low	Low	Low	Ensure the security and safety of all users and staff
Women	Low	Low	Low	Ensure the security and safety of all users and staff
Younger People (17 – 25) and Children	Low	Low	Low	Ensure the security and safety of all users and staff
Older people (60+)	Low	Low	Low	Ensure the security and safety of all users and staff
Race or Ethnicity	Low	Low	Low	Ensure the security and safety of all users and staff
Learning Disabilities	Low	Low	Low	Ensure the security and safety of all users and staff
Hearing impairment	Low	Low	Low	Ensure the security and safety of all users and staff
Visual impairment	Low	Low	Low	Ensure the security and safety of all users and staff
Physical Disability	Low	Low	Low	Ensure the security and safety of all users and staff
Mental Health Need	Low	Low	Low	Ensure the security and safety of all users and staff
Gay/Lesbian/Bi sexual	Low	Low	Low	Ensure the security and safety of all users and staff
Trans	Low	Low	Low	Ensure the security and safety of all users and staff
Faith Groups (please specify)	Low	Low	Low	Ensure the security and safety of all users and staff
Marriage & Civil Partnership	Low	Low	Low	Ensure the security and safety of all users and staff
Pregnancy & Maternity	Low	Low	Low	Ensure the security and safety of all users and staff
Carer Status	Low	Low	Low	Ensure the security and safety of all users and staff
Other Group (please specify)				

INITIAL ASSESSMENT (PART 5)

Have you identified any issues that you consider could have an adverse (negative) impact on people from the following protected groups?

IF 'NO IMPACT' IS IDENTIFIED Action: No further documentation is required.

IF 'HIGH YES IMPACT' IS IDENTIFIED Action: Full Equality Impact Assessment Stage 2 Form must be completed.

(c) Following completion of the Stage 1 Assessment, is Stage 2 (a Full Assessment)
Necessary? NO

Assessment Completed By: Mike Lees **Date Completed:** 5 May 2021

Line Manager: Marianne Betts Date: 5 May 2021

Head of Department: Mike Lees Date: 5 May 2021

When is the next review? Please note review should be immediately on any amendments to your policy/procedure/strategy/service.

1 Year	**2 year**	**3Year X**

Title of Service/Policy being assessed:	Trust Security Policy
Assessment Date:	22 January 2020
Is the service/policy aimed at a specific group of users?	No

STAGE 2 – FULL ASSESSMENT & IMPROVEMENT PLAN

MUST be completed if any negative issues have been identified at stage 1

Protected Characteristic	**What adverse (negative) impacts were identified in Stage 1 and which groups were affected?**	**What changes or actions do you recommend to improve the service to eradicate or minimise the negative impacts on the specific groups identified?**	**Lead**	**Time-scale**
Men Younger People (17-25) and Children Older People (50+) Race or Ethnicity Learning Disability Hearing Impairment Visual Impairment Physical Disability Mental Health Need Gay/Lesbian/Bisexual Transgender Faith Groups (please specify) Marriage & Civil Partnership Pregnancy & Maternity Carers Other Group (please specify) Applies to ALL Groups				

How will actions and proposals be monitored to ensure their success? Which Committee will you report to? (i.e. Divisional DQEC / Governance Meeting).	
Who will be responsible for monitoring these actions?	

Appendix 2

Glossary of Terms used within the Policy

Security: the protection of people, information, material activities, reputation and all assets against harm, loss or unauthorised disclosure.

Lockdown is the process for controlling movement and access – both entry and exit – of people (NHS staff, patients and visitors) around a trust site or other specific trust building/area in response to an identified risk, threat or hazard. A lockdown is achieved through a combination of physical and electronic security measures and the deployment of security and other Trust personnel.

Lockdown risk profile a risk assessment of each site to determine its capability of either partial or full lockdown.

Trust Identification (ID) Card is the photographic proximity card issued for use with the access control system and is only issued on the completion of the requisite form signed by the member of staff and line manager.

Trust Name Badge is the 'patient friendly' badge issued to staff and cannot be used to gain access and does not display the staff members photograph.

There is an administration charge for the loss or damage to any card issued by the Trust.

Centre for the Protection of National Infrastructure	**CPNI**
Barnsley Facilities Services	**BFS**
Assignment Instructions	**AIs**
Security Management Director	**SMD**
National Counter Terrorism Security Office	**NaCTSO**
Security Industry Authority	**SIA**
Conflict Resolution Training	**CRT**
Counter Terrorist Security Advisor	**CTSA**
Counter Terrorist Unit	**CTU**
Designing Out Crime Officer	**DOCO**
Unmanned Aerial Vehicle (Drone)	**UAV**
Training Needs Analysis	**TNA**
Radio Frequency Identification	**RFID**

Appendix 3

General Security Advice – All Staff

Workplace:

- Ensure security training is refreshed – security and cyber threats change regularly, make sure you are aware of these.
- Do not add stickers or write keypad lock number onto the rear of I/D cards.
- Lock rooms when not in use and/or keep a clear desk process. Medical records and sensitive documents should be secured and kept out of sight.
- Sensitive or personal information including passwords must not be written on office whiteboards. Consider a pulldown screen to conceal less sensitive information.
- Supervisors and managers should regularly check their workplace areas to review security measures – 'walk the floor'.

Visitors:

- Verify the identity of all visitors and consider:
    - A physical check of I/D card – is it just paper or card? NHS lanyards and card holders can by purchased via Amazon and other public suppliers.
    - Does the photograph match and is it current? Has the I/D card expired?
    - If in doubt request secondary identification – driving licence or credit card
    - Stethoscopes and high-visibility (yellow) jackets on their own are **not** accepted forms of identification. A current I/D card is also required.
    - Contact the visitor's department or company to verify identity. Legitimate visitors will understand any short delay while you confirm.
    - Consider escorting any visitor to their destination or arrange for them to be met at reception.
    - Be prepared to politely challenge and call security if you are suspicious.

Security of IT Equipment:

- Any equipment, particularly computers and laptops must be kept secure:
    - Do not allow ANY equipment to be removed unless you can verify the reason and the identity of the person taking.
    - Be prepared to politely challenge and call security if you are suspicious.
    - Never disclose any passwords or other sensitive/personal information.
    - Lock rooms when not in use and/or keep a clear desk process. Laptops and sensitive documents should be secured and kept out of sight.
    - Desktop and laptop computers should be logged off when not in use.
    - Ensure you refresh your security training – security and cyber threats change regularly, make sure you are aware of these

Appendix 4

Policy Version Control

Version	Date	Comments	Author
4	1/7/16	Minor Revisions Only	Mike Lees
5	1/2/18	Update – Minor Revisions Only	Mike Lees
6	1/2/2020	Update – See Document Control	Mike Lees
7	1/5/2021	Update – See Document Control	Mike Lees

Review Process Prior to Ratification:

Name of Group/Department/Committee	Date
Commercial Director - BFS	May 2021
Security Management Director (SMD)	May 2021
Security Site Manager	May 2021
Security Contract Group (including Security Provider)	May 2021
Surveillance Camera Commissioner & SSAIB	May 2021
Domestic Services Manager for all Domestic Staff	May 2021
Matrons & Lead Nurses	May 2021
Designing Out Crime Officer	February 2021
Counter Terrorist Security Advisor (NaCTSO)	February 2021
Surveillance Camera Group & SSAIB	June 2021
Staff Side Representatives (H&SG)	June 2021
Equality & Diversity Manager (HR)	May 2021
Policy Review Committee	June 2021
Health & Safety Group	June 2021