COVERSHEET	
Meeting	Board of Directors' meeting in PUBLIC
Paper Title	Security Annual Report 2019/20
Date of meeting	8 October 2020
Date paper was written	5 May 2020
Responsible Director	Nigel Lee – Chief Operating Officer
Author	Jon Simpson – Local Security Management Specialist
Presenter	Nigel Lee – Chief Operating Officer

EXECUTIVE SUMMARY

SITUATION

Under the provisions of the NHS Standard Contract, Providers are required to have in place and maintain security management arrangements in their organisations. Commissioners are required to review these arrangements to ensure the Provider implements any modifications required by the Commissioner. Aside from publishing this Annual Report, the Trust will also prepare an evidenced based Self-Risk Assessment (SRA) set against 30 previously issued national security standards. We will also complete a mandatory self-assessment in accordance with the provisions of the Premises Assurance Model (PAM).

BACKGROUND

During the reporting period Julia Clarke (Director Corporate Services) was the designated Board level Director responsible for security management matters. Nigel Lee, COO, is now the responsible Director.

Tony Allen is the designated Non-Executive Director responsible for assurance on security management matters.

During the reporting period Violet Redmond was Head of the Trust's Corporate Services Team. Sara Biffen, D/COO is now the responsible Head of Service for security matters affecting the Trust.

Jon Simpson is the Trust Security Manager and NHS accredited Local Security Management Specialist (LSMS) who ensures that the Trust complies with all NHS security guidance and requirements and also oversees day to day implementation of security management across the Trust.

ASSESSMENT

During the reporting period, there has been progress with efforts to manage levels of violence and aggression towards staff from service users and where appropriate seek due sanction and redress for inexcusable behaviour as well as support staff involved in any aggression incident. The report looks at the governance arrangements in place and incidents for the past year. It also reviews the

continuing efforts to protect staff and patients (from user aggression) as well as securing property and assets, which is the largest part of the responsibilities and is covered on pages 9-19 of the attached report.

The Plans for 2020/21 include:

- Supporting future security specifications, architecture and environment as it enters a phase of re-organisation and re-development of both hospitals (Hospitals Transformation Programme (HTP)) and do the same in relation to the refurbishment and/or maintenance of existing areas/new builds not affected by HTP and security risk assessment work.
- Continuing to reinforce the Board's robust approach to abuse of staff and patients and at the same time support staff in reducing harm or injury from clinically aggressive patients.
- Continuing with the work to press the case for additional funding to increase security staff numbers and when such is approved, with our security staff provider to establish, recruit, train and deploy additional security staff resources.

RECOMMENDATION
The Board is asked to:

i) Note and receive the Security Annual Report 2019/20.
ii) Note the outline plans for 2020/21.
iii) Approve the report for publication.

Previously considered by	- Executive Directors 18 May 2020 (for note): No further feedback received. - H&S Committee 27 July 2020 (for note): Support expressed by both the Committee and Staff Side Chairs for an ongoing business case for additional security staffing (to be raised by them at Sustainability Committee and JNCC). - Audit Committee 10 September 2020 (for note & to take assurance): Report commended and recommended for Board of Directors meeting.

The Board is asked to:			
☑ Approve	☑ Receive	☑ Note	☐ Take Assurance
To formally receive and discuss a report and approve its recommendations or a particular course of action	To discuss, in depth, noting the implications for the Board or Trust without formally approving it	For the intelligence of the Board without in-depth discussion required	To assure the Board that effective systems of control are in place

Link to CQC domain:				
☑ Safe	☑ Effective	☐ Caring	☐ Responsive	☑ Well-led

Link to strategic objective(s)	*Select the strategic objective which this paper supports* ☐ PATIENT AND FAMILY Listening to and working with our patients and families to improve healthcare ☑ SAFEST AND KINDEST Our patients and staff will tell us they feel safe and received kind care ☐ HEALTHIEST HALF MILLION Working with our partners to promote 'Healthy Choices' for all our communities ☐ LEADERSHIP Innovative and Inspiration Leadership to deliver our ambitions ☑ OUR PEOPLE Creating a great place to work
Equality Impact Assessment	◉ Stage 1 only (no negative impact identified) ○ Stage 2 recommended (negative impact identified and equality impact assessment attached for Board approval)
Freedom of Information Act (2000) status	◉ This document is for full publication ○ This document includes FOIA exempt information ○ This whole document is exempt under the FOIA

The Shrewsbury and Telford Hospital NHS

NHS Trust

Security Annual Report

2019-20

Foreword

The Shrewsbury and Telford Hospital NHS Trust is committed to ensuring a safe environment for staff and patients so that the highest possible standard of care can be delivered; to this end security remains a key priority within the development and delivery of health services. All of those working within the Trust have a responsibility to assist in preventing security related incidents or losses. This approach underpins and directly links to the Trust's values and objectives.

Julia Clarke (Director of Corporate Services) is the designated Board level Director for security management matters, including tackling violence against NHS staff, and ensuring that there is adequate security management at the Trust.

Tony Allen is the Non-Executive Director responsible for security management at Board level.

Violet Redmond is Head of the Trust's Corporate Services Team.

Jon Simpson is the Trust Security Manager and NHS accredited Local Security Management Specialist (LSMS) who ensures that the Trust complies with all NHS security guidance and requirements and also oversees the implementation of security management across the Trust.

During the reporting period, there has been progress with efforts to reduce and manage levels of violence and aggression towards staff from service users and where appropriate seek due sanction and redress for inexcusable behaviour as well as support staff involved in any aggression incident.

May 2020

Julia Clarke	Tony Allen
Director of Corporate Services	Non-Executive Director

Section	Contents	Page
	Title Page	1
	Foreword	2
	Contents	3
1	Governance, Risk & Assurance	4
2	Security Incident Reporting	8
3	Protecting Staff & Patients (from service user aggression) / Property & Assets	9
4	Communications, Awareness & Training	19
5	Conclusion	20

1 Governance, Risk & Assurance

A sound Governance framework is essential in ensuring a consistent approach to security.

1.1 *Standards for Providers*

Under the provisions of the NHS Standard Contract, Providers are required to have in place and maintain security management arrangements in their organisations. Commissioners are required to review these arrangements to ensure the Provider implements any modifications required by the Commissioner. Aside from publishing this Annual Report, the Trust will also prepare an evidenced based Self-Risk Assessment (SRA) set against 30 previously issued national security standards. Work will commence shortly to prepare our 2020-21 assessment, based on results and outcomes from 2019-20. We will also complete a mandatory self-assessment in accordance with the provisions of the Premises Assurance Model (PAM).

1.2 *Policy*

Prior to publication, any new and/or updated policies are first approved by the Policy Approval Group (PAG). This is a multidisciplinary group that ensures all new and reviewed policies are compliant with Trust standards and that appropriate consultation has been undertaken before recommending them for ratification by the appropriate committee.

During 2019/20, a Patient Search Policy has been developed following the introduction of hand held portable metal detector search wands for security staff (s3.6 refers) and is currently being progressed through the approval process to proactively ensure staff safety, following dangerous weapons being brought in A&E. Procedures and action cards contained in our Trust Lock Down policy have been updated following incident de-brief and review. All other security policies published and available on the intranet are within review dates[1].

1.3 *Security Risks*

All security risks are managed in accordance with the Trust Risk Policy. All risks which have been scored and evaluated as requiring to be placed on a department or Clinical/Corporate Centre register or the Trust Risk register, are entered on to the 4Risk system where they are regularly reviewed. The requirement to regularly review and record progress is initiated by a system generated electronic alert to the risk owner; oversight of this process is undertaken by an Associate Director responsible for Corporate Governance and reported to the Operational Risk Group (ORG). There are currently no recorded security risks scoring 15 or more.

1.4 *Security Risk Assessment*

The following areas of security risk assessment work have been undertaken during the reporting period:

Security Staff Numbers. In the last reporting year concern has been highlighted by a number of key partner agencies that the number of uniformed security staff on duty is not enough. Our intention is to progress the recruitment and deployment of more security staff which should take place in Spring/Summer 2020 (numbers will increase from two to three on duty at each site 24/7).

---

[1]Security Management, Violence & Aggression, CCTV, Lock Down, Counter Terrorism, Hosting of Prisoners On Trust Premises, Lone Working.

Possession of Blades, Knives & Sharps. To increase safety, prevent harm to staff and patients and following discussion at Health & Safety Committee (H&S), hand held metal detectors were issued in December 2019 to security staff to help with the detection of blades, knives and other metal sharp objects (3.6 refers)[2].

General Departmental/Ward Security Risk Assessment and Lock Down. Security risk assessment and/or Lock Down advice/guidance was provided to the following areas during the reporting period:

- Emergency Departments (ED) (both sites) concerning a need for Vulnerable Person rooms;
- IT department concerning generic use and issue of portable iPad devices following concern over numbers of missing/lost devices;
- IT Department (PRH) concerning security of new PC assembly workshop;
- X-Ray department (PRH) concerning Lock Down arrangements;
- Ward 32 (RSH) concerning Lock Down arrangements;
- Ward 33/34 (RSH) concerning Lock Down arrangements.
- Ward 14 (PRH) concerning night time/weekend access control arrangements;
- Ward 35 (RSH) concerning general access control and Lock Down arrangements;
- Chief Information Officer; regarding access to Shrewsbury Business Park (SBP).
- HDU (RSH) Installation of intruder alarm.

Capital Project Risk Assessment & Support. Security risk assessment advice, guidance and documentation were also provided to the Estates Capital Projects Team on the following:

- New build Midwife Led Unit (PRH);
- Vanguard Unit Mobile Operating Theatre (PRH);
- Temporary Cardiac Catheterisation Laboratory (PRH).
- Occupation and transfer of services into the vacated Mytton Oak building (RSH);
- Medical Engineering Section (MES) refurbishment (RSH);
- Off-site medical records storage (Atcham Business Park, Shrewsbury);
- Hamar Centre refurbishment and extension (RSH);
- Improvements to existing access control arrangements (ED RSH).

Areas of Special Interest. Regular and scheduled security risk assessment is undertaken on the following key areas of security:

- Lock Down; every three months our security team supervisors undertake audit and functionality tests of the Lock Down plan for each of our ED. This ensures that paper copies of Lock Down plans are in the place staff expect them to be should they need them, are the correct version and the instructions, systems and facilities referred to in each plan are correctly functioning. Whilst this is being done opportunity is provided for the Sister in Charge and any new or less frequent working A&E staff to walk the department and understand the plan first hand. After the ED check security supervisors then complete a site wide check of the viability, effectiveness and likelihood of each Ward and/or publically accessible department/entrance being able to achieve an emergency Lock Down. Any issues identified are addressed and the check also gives security staff the opportunity to liaise with clinical staff and highlight the procedure and mechanism for securing

[2] A consultation process with senior clinical and operational management in Unscheduled Care and H&S Committee was completed prior to introduction of the devices. Interim instructions on use have been issued to security staff whilst a formal policy on use awaits approval (s1.2 refers).

departments which are not regularly locked and secured because of operational constraints. Records on all these audits are retained by the Trust Security Manager.

- Lone Working (s3.10 refers); Every three months the security team supervisors test and assess lone worker pagers issued to/held by departments to ensure they are available for staff and to ensure equipment functionality by testing them with Switchboards. Records on all these audits are retained by the Trust Security Manager.

- Infant/New Born Security (s3.11 refers); every 3 months to prevent the unauthorised removal of a baby from the hospital the Baby Tagging security systems are tested to ensure system operability and staff knowledge/reactions. Results of each test are fed back to senior Women & Children's management, Director Corporate Services and Head of Corporate Services. Records on all these audits are retained by the Trust Security Manager. The benefit of this constant review and assessment process was noted during the last CQC Inspection[3].

Corporate Services Board. Every month security management activity in relation to acts of intentional/inexcusable aggression by service users towards staff is reviewed by the Director of Corporate Services using specific Key Performance Indicators (KPI).

Restraint Review Group. This group was set up following the last CQC inspection when concern was expressed regarding the completion of entries in patient's medical records following an incident of safe holding/ restraint[4]. All matters and activity concerning the safe holding / restraint of patients are now considered by this group. Chaired by the Patient Safety Lead with oversight from a Deputy Director of Nursing and attended by Lead Nurses for Unscheduled and Scheduled Care, Corporate Nursing and the Trust Security Manager, this group meet monthly. Data on security team interventions is provided on a weekly basis to Corporate Nursing and this data provides a basis for discussion and actions.

Health & Safety Committee. A quarterly security report is presented to the Trust Health & Safety Committee which is attended by staff side Chairs/representatives, Union representatives and has Centre management representation. The report provides insight on progress with managing violence and aggression by service users (clinical as well as intentional/inexcusable aggression) including reports on sanction and redress and support to staff affected. Traditional security incidents (theft etc.) are also discussed when required. In the fourth quarter, the annual security report is presented which gives feedback and a full account of all security management work in the reporting year.

Operational Risk Group (ORG) meetings. The Trust Security Manager attends this monthly meeting to ensure security management assessment and advice is readily available for all matters discussed.

Local Authority & Police Community Meeting. Chaired by a local Police Inspector, these meetings, attended by the Trust Security Manager, are a multi-agency approach to tackling community issues including anti-social behaviour. Sharing of intelligence on matters of concern to the local community contributes to our own security risk assessment process.

---

[3] "Staff followed the baby abduction policy and undertook baby abduction drills. All babies were electronically tagged, and labels and tags were checked daily. Tags were removed as part of the discharge process. All staff were trained and aware of the baby tagging process". Source: CQC Inspection Report (Evidence Appendix) published 8 April 2020 page 392.

[4] "Only security staff were trained to complete physical restraint and they kept separate records of these interventions outside of the nursing and medical records". Source: CQC Inspection Report (Evidence Appendix) published 8 April 2020 page 50.

Staffordshire & Shropshire Controlled Drugs (CD) Local Intelligence Network (LIN) forum. This forum is attended by the Chief Pharmacist and the Trust Security Manager and enables security assessment and understanding of implications for the organisation on this key area of medicines management.

Staffordshire & Shropshire NHS Local Security Management Specialist (LSMS) Forum. Following the dissolution of NHS Protect in 2016-17 as the national body for coordination of security management in the NHS, this voluntary forum is attended quarterly by the Trust Security Manager. There is representation from all NHS sectors in Shropshire & Staffordshire including Acute, Mental Health and Community services. The forum provides opportunity for briefing and discussion on security issues affecting all NHS interests.

1.5 *Release of Information, Freedom of Information (FOI), Complaints & Challenges*

Release of Information

No releases of CCTV video footage were made to or requested by the public during the reporting period. The Trust released CCTV and/or video footage from Body Worn Video camera equipment 18 times during the reporting period for the following reasons:

- Police Investigation – 14
- Assistance with Trust H&S Investigation - 1
- Assistance with Insurance Claim - 3

The releases to the police concerned criminal and/or suspicious activity or other incident requiring further investigation that occurred on Trust premises. Although some of the releases concerned incidents which did not occur on Trust premises, it was often the case that the original incident subsequently led to other adverse attendance or activity on Trust premises.

Freedom of Information (FOI)

Eleven FOI requests were made regarding other security matters at the Trust. Responses and data were provided to Corporate Services staff that coordinate Trust responses.

Complaints

During the period, five complaints were received citing concern over actions of security staff from both sites. In three instances these concerns formed part of a wider complaint about the clinical care received by patients. On review by the Trust Security Manager, attendant security staff were found to have behaved appropriately and no further action was required. Two further complaints were as a direct result of security team actions. One matter resulted from a clerical error that resulted in a warning letter regarding the behaviour of a patient being sent to the wrong person. The letter accused the recipient of being verbally aggressive and racist towards staff. The complaint was upheld and an unreserved apology made to the (wrong) recipient of the letter[5]. The other matter concerned unsympathetic and inappropriate words said by a relief security guard towards a patient. The complaint was upheld and an unreserved apology made to the patient.

[5]The letter was then sent to the correct recipient.

2 Security Incident Reporting

Security incident reporting remains key to the maintenance of a pro-security culture.

2.1 Comparative figures for 2019-20 are shown in Table 1[6].

Table 1 - Security Incident Reporting

ALL SECURITY INCIDENTS	2017/18	2018/19	2019/20
First quarter: Apr, May, Jun	184	186	170
Second quarter: Jul, Aug, Sep	157	138	182
Third quarter: Oct, Nov, Dec	158	168	166
Fourth quarter: Jan, Feb, Mar	172	155	190
Running Total	**671**	**647**	**708**

2.2 Of the reported 708 incidents in 2019-20, 402 occurred at the RSH, 304 occurred at PRH and 2 off-site.

2.3 Non-aggression incident reporting categories include damage to Trust and non-Trust property, theft of Trust and non-Trust property, trespass and other security[7]. Total incident numbers for these categories are:

- Other Security (205)[8];
- Trespass (26)[9];
- Suspect packages (3);
- Damage to Trust Property (12)[10];
- Damage to non-Trust Property (16)[11];
- Theft/alleged theft of Trust Property (3)[12];
- Theft/alleged theft non-Trust Property (32)[13].

---

[6]Source: Datix. Excludes Cyber Security and security related Information Governance incidents which are managed by IT and Information Governance teams. Figures are as available/recorded with effect 30 April 2019; this applies to all figures contained within this report hereafter. Figures may be subject to increase thereafter due to late reporting and/or incidents being re-coded from other categories during end of year accounting/verification.

[7]For those instances where no pre-selectable code is available.

[8]Examples include building/office insecurities, alarm activations, suspicious behaviour, concern re patient behaviour, undue interest in staff (harassment), nuisance phone calls, possession and/or use of illegal drugs or blades/sharps by service users.

[9]Examples include unwelcome/unnecessary presence of relatives, rough sleepers and/or intoxicated members of public in hospital grounds, unauthorised presence of public in staff only areas, refusal of patients to leave after discharge.

[10]Examples include staff lockers in RSH Theatres (spate of attempted break in), broken window panes other fixtures and a hospital bed (by patients with and without capacity) and 2 vehicles used by Diabetes Eye Screening Program (DESP) (whilst parked off site by persons unknown).

[11]All concerned low speed collision or other damage to motor vehicles aside from 3 incidents which concerned minor damage to a vending machine, a cash point and also a wall in the Theatre department at PRH (caused by a member of staff during an emotional outburst).

[12]Concerning theft of housekeeping supplies from Wards and allegation by a member of the public concerning theft of Controlled Drugs.

[13]Majority concerned allegations of theft of cash from both staff and patients, in all instances monies had either been left unattended or based on the available information nothing further could be done to investigate. Incidents also included theft of a bicycle and trainers belonging to staff as well as charity collection boxes/jars from a staff room.

3 Protecting Staff & Patients, Property & Assets

A key principle is that staff working at the Trust and patients and visitors using the Trust, have the right to do so in an environment where all feel safe and secure.

3.1 *Intentional/Inexcusable Violence & Aggression*

Figures for reported intentional/inexcusable violence and aggression incidents in 2019-20 are shown in Table 2. Intentional/inexcusable incidents ranged from acts of physical contact (however minor or inconsequential including spitting) to verbally threatening or intimidating behaviour, racial abuse and abusive phone calls. Intentional/inexcusable incidents are those incidents where the perpetrator *was not* deemed to have any reasonable excuse for their behaviour e.g. an underlying medical condition or illness such as dementia or toxic infection.

Legally excess alcohol and/or drug misuse are not seen as mitigating circumstances for adverse behaviour, but as aggravating factors.

Table 2 – *Intentional/Inexcusable Violence & Aggression*[14]

Intentional/Inexcusable Violence & Aggression	**2017/18**	**2018/19**	**2019/20**
First quarter: Apr, May, Jun	29	32	33
Second quarter: Jul, Aug, Sep	23	24	36
Third quarter: Oct, Nov, Dec	42	26	30
Fourth quarter: Jan, Feb, Mar	17	31	29
Total	**111**	**113**	**128**

Of the reported 128 intentional/inexcusable violence and aggression incidents in 2019-20, 72 occurred at the RSH, 55 occurred at PRH and one off-site, but involved staff.

37 involved physical contact (however minor or inconsequential).

- 26 were on staff (25 of these were carried out by patients, 1 involved staff on staff).
- 1 was by patients or relatives (public) on the same.
- 2 were patient on patient incidents.
- 2 were relatives (public) on patient incidents.
- 1 was a staff on patient incident.
- 5 were incidents involving visitors/relatives (public).

None of the intentional/inexcusable physical assault incidents involving Trust staff during 2019-20 resulted in serious injury or triggered RIDDOR[15] reporting to the Health & Safety Executive (HSE).

---

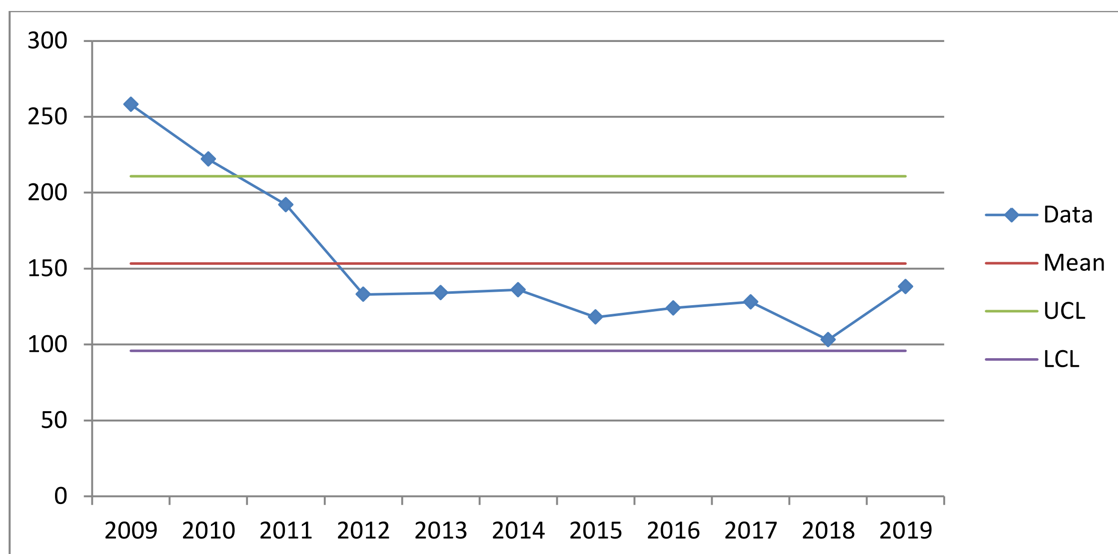
[14]Concerning all staff, patients, visitors and contractors. Source: Datix.

[15]RIDDOR is the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013. These Regulations require employers, the self-employed and those in control of premises to report specified workplace incidents.

There were 91 intentional/inexcusable *non*-physical incidents i.e. incidents of verbal abuse, threatening or other anti-social behaviour by patients, relatives or public, 81 of these were made towards staff and the other 10 towards other patients, relatives or public.

Past investment in security services[16] can be seen to have had positive impact with the number of incidents of intentional/inexcusable aggression reported between 1 January 2009 and 31 December 2019 showing consistent reduction and remaining below the given upper control limit, Figure 1 refers.

Figure 1: The number of incidents of intentional/inexcusable aggression reported between 1 January 2009 and 31 December 2019.



3.2 *Non-intentional / Clinical Aggression*

These are incidents where an individual is deemed to lack capacity and are not therefore held responsible for their actions due to their medical condition, treatment or other underlying medical issue e.g. dementia.

Table 3a - Non-intentional Clinical Violence & Aggression[17].

CLINICAL VIOLENCE & AGGRESSION	Year		
	2017/18	2018/19	2019/20
First quarter: Apr, May, Jun	77	89	62
Second quarter: Jul, Aug, Sep	83	52	62
Third quarter: Oct, Nov, Dec	65	67	71
Fourth quarter: Jan, Feb, Mar	85	74	88
Total	**310**	**282**	**283**

[16] Past investment includes increasing security staff numbers from 1 to 2 on duty; professional and appropriate training of security staff in safe handling and restraint of aggressive service users, investment in CCTV networks and Body Cameras.
[17]Concerning all staff patients, visitors and contractors. Source: Datix.

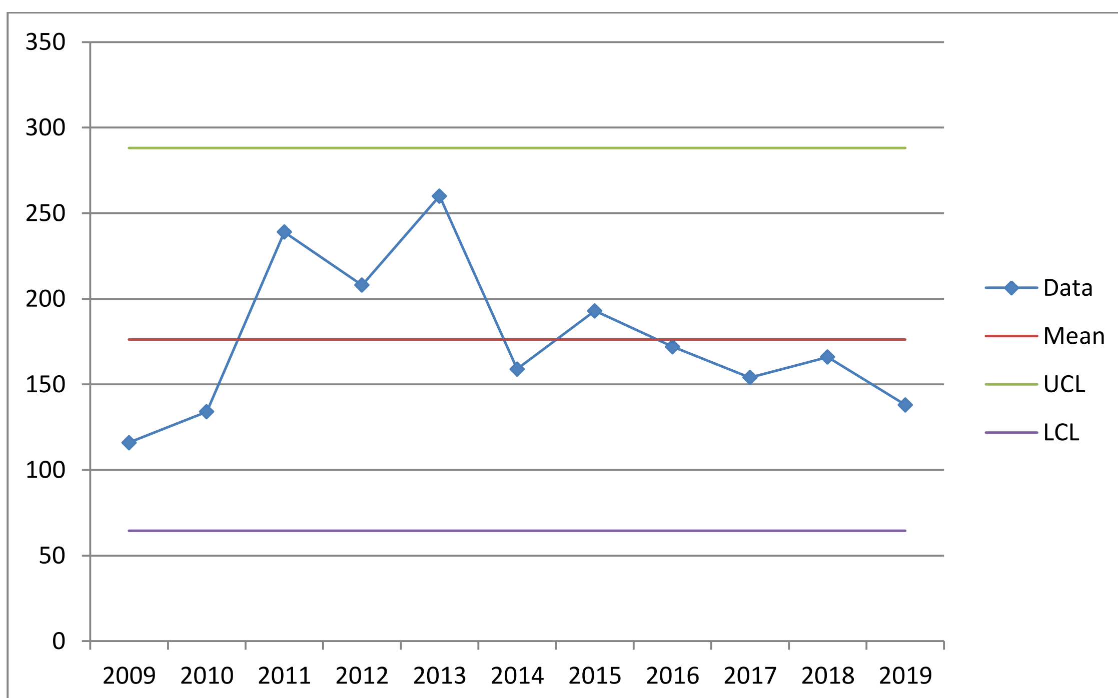
Of the reported 283 non-intentional clinical aggression incidents in 2019-20, 167 occurred at the RSH, 115 occurred at PRH and 1 off-site[18]. 151 involved physical contact (Table 3b refers), 137 of these involved staff. 1 of these non-intentional physical assault incidents triggered RIDDOR reporting to the Health & Safety Executive (HSE)[19].

Table 3b - Non-intentional / Clinical Physical Aggression

CLINICAL VIOLENCE & AGGRESSION – PHYSICAL	**Year**		
	2017/18	**2018/19**	**2019/20**
First quarter: Apr, May, Jun	47	57	31
Second quarter: Jul, Aug, Sep	49	31	38
Third quarter: Oct, Nov, Dec	35	39	34
Fourth quarter: Jan, Feb, Mar	53	48	48
Running Total	**184**	**175**	**151**

The number of incidents of non-intentional clinical aggression resulting in physical contact, harm or injury to staff reported between 1 January 2009 and 31 December 2019 shows consistent reduction and remains below the given upper control limit, Figure 2 refers.

Figure 2: The number of non-intentional/clinical aggression resulting in physical contact, harm or injury reported between 1 January 2009 and 31 December 2019.



[18]Datix id: 172014 concerning a member of Audiology staff working at Whitchurch Community Hospital.
[19]Datix id: 177621.

3.3 *Immediate Response to Violence & Aggression*

In line with our published policy on dealing with violence and aggression an escalated approach is used to deal with all violent and aggressive incidents, namely:

Step 1 – Using by all staff of conflict resolution techniques to diffuse situations (4.3 refers).

Step 2 – Calling for emergency assistance from hospital Security Officers. Security Officers provide emergency response and support to all staff facing threats of violence and aggression from service users, intentional or not (3.5 refers). As well as being backed up by an extensive CCTV network (3.8 refers) all Security Officers carry Body Worn Video camera[20].

Step 3 – Enlisting emergency assistance from the police.

3.4 *Post Incident Action, Sanction & Redress*

All reported security incidents from either hospital staff or the security teams are individually reviewed by the Trust Security Manager. This includes liaison with staff affected by more serious incident and/or their line management. The Director of Corporate Services acknowledges reported incidents of violence and aggression by writing to all members of staff who may have been injured, harmed or significantly affected by an incident, offering support through line management or occupational health/counselling services and advising of the Trust's response to incidents. During the reporting period 181 letters offering support and/or feedback to staff were sent to staff and/or department managers whose staff were involved or affected by incidents (intentional or not)[21].

Where an assailant's actions were deemed to have been intentional, an entry is made on our electronic violence and aggression register. Linked to a patient's electronic SEMA record this allows staff in future to be warned of the potential for adverse behaviour from a patient[22]. A warning letter, signed by the Chief Executive, is sent to the perpetrator of the adverse behaviour and copied to the victim and police, advising that non-emergency treatment could be withdrawn if there are any further episodes and support for police action or civil action by the Trust[23]. In the reporting period 39 SEMA alerts and 70 warning letters and/or letters of concern were issued. Only 8 of those receiving a warning letter in this period have come to further attention despite further hospital attendances, thereby giving some assurance as to the effectiveness of warning letters.

The Trust supports all police and Court actions when taken and every effort is made to enable partnership working and achieve rightful sanction and redress for unacceptable behaviour. This often includes provision of supporting CCTV, Body Worn Video (BWV) recordings or other documentary evidence. The following are some (but not all) examples of effort to see rightful outcome to incidents of aggressive and/or anti-social behaviour in 2019-20[24]:

---

[20] A statement on how the equipment is used and controlled is included within our published CCTV policy.

[21] In line with the strategy outlined for dealing with violence and aggression a resulting outcome is that much adverse behaviour is diverted away from medical and nursing staff by the intervention of security staff before the behaviour escalates and so medical and nursing staff can avoid injury or unnecessary involvement; by virtue of their involvement security staff, based on their early involvement become responsible for reporting on the incident with medical/nursing staff being identified as witnesses as opposed to victims. This explains in some way the disparity between numbers of support letters issued to Trust/NHS staff and all reported incidents (Tables 2 and 3 refer).

[22] A recommendation for an alert on a patient's SEMA record and the issue of a warning letter is made by the Trust Security Manager. However, prior to this action being undertaken the recommendation has to be approved and supported by an ED Consultant; this ensures that patients who may have lacked capacity at the time of the incident and whose circumstances may not have been accurately reflected in the incident reporting process are not unnecessarily sanctioned.

[23] It should be noted that it is not always possible or appropriate to issue a warning regarding unacceptable behaviour because the individual may not have been identified or the circumstances of the individual deem it inappropriate.

[24] For a criminal prosecution and/or other form of police sanction to take place an individual personal complaint is required; it is not always the case that staffs feel able or willing to make such.

- On 26 June 2019, an intoxicated and abusive man seen at the RSH was told by security staff to leave. Earlier discharged from ED he reacted aggressively, threatening security staff with a broken bottle. His removal from premises followed during which two Security Officers were assaulted and then threatened with a broken bottle. He then endangered members of the public by stepping into moving traffic, forcibly stopping a motorcyclist and attempting to take control of the motor cycle. He repeated this with a female Doctor in a car on her way to work. Both were threatened with the broken bottle. The individual was later sentenced at Crown Court to 9 months in prison. Body Worn Video camera footage of the incident was used in evidence.

- On 6 July 2019, a male patient was brought into the RSH ED by ambulance intoxicated. He behaved very aggressively towards staff, after leaving the department and entering other parts of the hospital a female nurse and a member of the security team were assaulted as attempts were made to prevent him throwing a wheelchair at a door. A pane of glass in the door was smashed. The individual pleaded guilty at Magistrates Court on 15 January 2020 to assault by beating of emergency service worker(s) and damage to property. He was given a Conditional Discharge for 2 years[25]. Recorded CCTV footage of the incident was used in evidence.

- At the RSH ED on 21 December 2019 an intoxicated male patient, was reported as being aggressive with ambulance staff as he was being prepared for handover. His behaviour quickly escalated to threats of physical violence and threatening to kill nurse staff. A security intervention with police support was needed to control his behaviour. The individual pleaded guilty at Magistrates Court on 11 February 2020 to being drunk and disorderly and was given a Community Order for 3 offences which included his behaviour in the ED. The order included a requirement for him to be electronically tagged for its duration.

- At the RSH ED on 15 February 2020, a young female patient was arrested by police after a significant disturbance that involved the assault of security staff that were kicked several times in various places as clinical staff tried to treat her and prevent her injuring herself. The patient subsequently admitted to common assault and was given a police caution[26].

- At the PRH ED on 3 February 2020, a male patient was arrested by police after a significant disturbance that involved abuse and threats towards a number of ED staff. One member of the security staff was spat on. On 4th March 2020 at Magistrates Court, the individual admitted to common assault was sentenced to an 18 month Community Order (40 days rehabilitation activity) £60 fine and £100 compensation to the staff member he spat on.

- At the PRH ED on 13 February 2020, assigned care workers were unable to control the escalating behaviour of a male patient in his twenties. His behaviour escalated and resulted in a smashed a window pane on a door in the department. The patient, who was deemed by medical staff to have full capacity later admitted during police interview to causing criminal damage. On review of the patient’s circumstances by the police and the Trust

---

[25]A Conditional Discharge means that the offender is released but the offence is placed on their criminal record, at the same time the Court have the power to review sentencing for the offence if the offender commits any further offence within a time period set by them (in this case 6 months). If the offender does commit a further offence within that time period, they may be recalled and resentenced for the original matter as well as the new matter.

[26] Cautions are given to anyone aged 10 or over for minor crimes - for example writing graffiti on a bus shelter. You have to admit an offence and agree to be cautioned. You can be arrested and charged if you don’t agree. A caution is not a criminal conviction, but it could be used as evidence of bad character if you go to court for another crime. Cautions show on standard and enhanced Disclosure and Barring Service (DBS) checks.

Security Manager agreement was reached that the matter could be dealt with by way of a Community Resolution Order[27].

3.5 *Principle Role of Security Officers*

Although security staff at both sites are provided by a parent company, they are very much seen as part of the hospital team and relied upon for support across all areas of both hospital sites. All of the core team staff only work at the hospital and are not employed on other contracts. There are two officers on duty 24/7 at each hospital with an assigned supervisor to each site[28].

With any aggression incident security staff are called to help provide reassurance and assistance in seeing the safe closure of the incident or prevent further escalation, as well as providing pre-arranged preventative support to staff to stop a foreseeable incident escalation[29]. Often staff may note a SEMA warning alert for aggression on a patient's electronic record, this triggers a request for security staff presence when they attend. All Security Officers carry portable Body Worn Video camera equipment[30] which is compatible with police equipment and acceptable as prima facie evidence in any subsequent prosecution.

Our regular core team security staffs are trained to make physical interventions by way of safe holding / restraining those service users whose behaviour has escalated to the point that the safety of staff, the service user or others is being endangered. To provide security staff with the skills and confidence to do this, specialist training is delivered over a one week training course to security teams by accredited NHS training staff from the Midlands Partnership NHS Foundation Trust (FT) (4.1 refers)[31].

270 safe hold / restraint interventions were undertaken across both sites by security staff during the reporting year. Not all 'safe holds / restraints' were undertaken as a result of actual aggression towards staff. Some were undertaken due to concern about potential aggression due to:

- Concern by medical/nursing staff about safety during a planned invasive procedure where the patients mental or physical state, whilst not aggressive, suggested that harm or injury to the patient or staff would have occurred had an intervention not been undertaken;

- A need to prevent patients in personal crisis from attempting/carrying out acts of self-harm;

- High risk confused and/or agitated patients who had or were attempting to leave the hospital buildings and/or their ward/bed spaces and refusing to return.

---

[27] A Community Resolution is an alternative way of dealing with less serious crimes, allowing officers to use their professional judgement when dealing with offenders. It can be used for offences such as low level public order, criminal damage, theft, and minor assaults. At the same time they still allow victims a say in how the matter is dealt with. In this instance it was agreed that the patient would apologise in writing to the Trust. Community resolutions do not constitute a criminal record and are not recorded on the Police National Computer. They are however recorded on police information systems and can be accessed for intelligence purposes. A previous Community Resolution is taken into consideration if further offences are committed.

[28] All Security Officers are licensed in accordance with the Private Security Industry Act (PSIA) by the Security Industry Association (SIA) for Door Steward Duties & Public Surveillance CCTV Monitoring.

[29] "Staff we spoke with were positive about the responsiveness of security staff within the hospital" and "nursing staff told us that the security team were often called if a patient's behaviour was challenging and they were skilled in dealing with these challenges in a sensitive manner". Source: CQC Inspection Report (Evidence Appendix) published 8 April 2020 page 270 & page 91 respectively.

[30] A statement on how the equipment is used and controlled is included within our published CCTV policy.

[31] "Restraint consisted of the use of a number of specialist holds that were completed by security staff who had received appropriate training" Source: CQC Inspection Report (Evidence Appendix) published 8 April 2020 page 45.

3.6 *Increasing Severity of Incidents*

Whilst the decreases in reported incidents of service user aggression is welcomed (page 10 & 11 refer) the severity and intensity of many remaining incidents is increasing. The incidents summary on page 13 illustrate what can be weekly occurrences as regards intentional/inexcusable aggression. The number of intentional/inexcusable incidents of aggression against staff resulting in prosecution and awarded prison sentences has increased in recent years[32].

It is also recognised that the risk of clinically related aggressive behaviour will always be present in an acute hospital, not least due to consistent pressures from an ageing population in Shropshire which is above the national average and increasing levels of dementia. Security staff are the only trained resource at the Trust for the safe handling and restraint of physically violent or aggressive patients. There is a risk in terms of continuity and consistency of service when multiple demands for security support puts pressure on security teams, not least in terms of availability of trained officers versus compliance with the numbers of trained officers required to undertake safe holds / restraints[33].

In the reporting period, there have been significant increases in numbers of blades, knives and sharps being removed from patients/service users[34]. In July 2019 alone, there were five occasions at ED where bladed items were removed from disturbed, in-crisis or vulnerable patients[35].

Datix web138218: "A mental health patient self-presented with suicidal thoughts and expressed serious thoughts of harming others. Patient sat in the relative's room. A Security Officer then came to me showing me a large black handled knife with a *14 inch* blade he had removed from the patient. Police subsequently carried out a further search of the patient, a hidden compartment in his bag contained another knife".

Following risk assessment (s1.4 refers) to increase safety hand held metal detectors were issued in December 2019 to security staff[36]. Between January and March 2020, 9 patients were searched for possession of blades, knives or sharps. 7 searches revealed concealed/undisclosed blades, knives or sharps. 4 were only confirmed after use of metal detectors.

Following risk assessment of security staff numbers (s1.4 refers), Pre-Business and Full Business Cases to increase the number of security staff on duty at each site to 3 at all times have been submitted and accepted in principle by Exec's and await budget setting (2020-21) outcome.

---

[32] This equated to 3 years of sentences in 2018-19 and 1 year in 2019-20.
[33] "We saw evidence in one record that only one security guard was trained in restraint. (Where) restraints were level three with only two security guards carrying out these restraints (there was) no record of third person". Source: CQC Inspection Report (Evidence Appendix) published 8 April 2020 page 269.
[34] Concerning patients both with and without capacity.
[35] Knife crime/possession in 2018-19 rose 18% on the previous year in the West Mercia Police area and 44% in Dyfed-Powys.
Source: https://www.shropshirestar.com/news/crime/2019/07/18/west-mercia-and-mid-wales-knife-crime-hits-record-high/
[36] A consultation process with senior clinical and operational management in Unscheduled Care and H&S Committee was completed prior to introduction of the devices. Interim instructions on use have been issued to security staff whilst a formal policy on use awaits approval (s1.2 refers).

3.7 *Other Duties*

Security staff also contribute to a wide range of tasks which are not specifically recorded as security incidents, but occur on a daily basis, these include:

- Help with preventing or locating absconded/missing patients or patients in crisis deemed to be vulnerable and/or at high risk of self-harm or may/are intending to take flight (patient safety);

- Fire alarm activations and other fire incident related activity (fire safety incidents);

- Attendance at Air Ambulance arrival/departure (operational task);

- Emergency resuscitation team calls to victims in public areas of the hospitals to ensure resuscitation teams can work without disruption or oversight of victims and ensure safe passage for patient evacuation etc. (medical emergency task);

- Escort of General Office staff carrying out cash transfer and filling/emptying of change machines and collection of valuables from night safes (cash security).

3.8 *Closed Circuit Television (CCTV)*

Each main hospital site has a dedicated CCTV camera control room which forms an operating base for Security Officers. Output from security cameras on our main hospital sites is fed back to these camera control rooms. As well as addressing a wide range of security issues and requirements these facilities prove very helpful with the rapid investigation of missing patients, some of whom have either inadvertently or intentionally left the hospital buildings. For the safety and security of staff, we have also installed in recent years our own CCTV facilities at a number of satellite sites, namely the Midwife Led Unit at Ludlow Community Hospital, our Therapy Services Centre on the NHS William Farr House site in Shrewsbury and our Sterile Services Decontamination facility at Queensway Business Park, Telford.

Images recorded on all systems are stored and controlled in accordance with our CCTV operating policy (s1.2 refers). CCTV equipment at all our sites is covered by 24/7 maintenance support contracts from an approved contractor.

During the reporting period, opportunity was taken at both sites to replace 4 of our oldest recording units which, whilst still functioning, had significantly past their intended useful working life. These replacement systems offer much improved clarity for both live and played back/recorded footage as well as increased functionality and will assist greatly when urgent searches are being undertaken for missing or absconded patients.

On specialist advice, investment was also made to replace and re-configure the recording unit/ network cabinet in the security camera office at PRH to avoid overheating and damage to recording units as well as a potential electrical overload on the cabinet.

CCTV equipment was included in the design specification of the new build MLU at the PRH completed in March 2020. The equipment is configured to work in partnership with the building door access control and baby tag systems with images recorded in the main security CCTV room, but viewable in the MLU at 3 locations as well as the main security camera room.

3.9 *Networked Swipe Card Door Access Control*

Continued restrictions in capital funding/investment have restricted any opportunity for realising security (capital) aspirations to see expansion of the Trust networked swipe card door access system to departments at both sites[37]. This is set to change as plans are developed for the Hospitals Transformation Program (HTP).

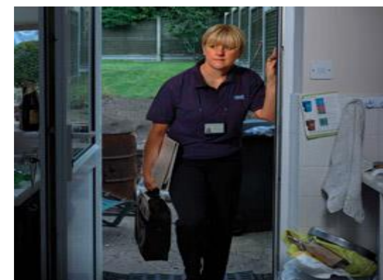
In the interim networked swipe card access control is included in any new build or major refurbishment programs. To this end it was included in the PRH MLU new build and is being included in the final phase of the move of Ophthalmology Services into Ward 20 of the Copthorne Building at the RSH and the planned extension to RSH ED.

3.10 *Lone Working*

The Trust has a two-track strategy, one for off-site lone workers or those out in the community and one for those working alone on-site.

(i) Off-Site Strategy

The lone worker device used is in the form of an identity badge holder worn around the neck or clipped to a belt or tunic. It includes a panic alarm that can be discreetly activated and which automatically opens a line of communication (via roaming mobile phone signal) to a national Alarm Receiving Centre (ARC), thereby allowing situation assessment and immediate response/escalation, as well as recording of evidence. In very extreme instances ARC staff are able to directly provide information from the staff member's device including pre-recorded information on where the staff member is located, to the nearest police control room. The advantage here is that police response is quicker because the information being received by them is from an accredited source as opposed to an anonymous cold call to police from public.



The device is not seen as a risk eliminator, rather as a risk reducer designed to work with and complement other safe systems of work. The use of this system was noted during the last CQC Inspection[38]. 238 staff are currently trained and have access to a live device.

---

[37] 4Risk Register No 75.
[38] "New mobile phones, lone worker security devices and maternity grab bags with standardised equipment had been provided for each community midwife". Source: CQC Inspection Report (Evidence Appendix) published 8 April 2020 page 429.

(ii) On-Site Strategy

In this system upgraded hospital pagers allow a lone worker to send a discreet emergency alert to security staff pagers and hospital switchboards. As well as being used on a daily basis in departments whose task requires continual support e.g. overnight Pathology Laboratory staff, devices have also been used to provide immediate short term reassurance to staff who through no fault of their own have become the victim of undue interest from patients/public.

As well as regular checks by our security team supervisors (s1.4 refers) a maintenance and support contract with the supplying company is in place to ensure specialist technical support and equipment repair is available.

3.11 *Baby Tagging*

This facility is in operation at the Shropshire Women and Children's Centre at the PRH on the Post-Natal Ward and Ante-Natal Wards (standby facility should Post-Natal overspill). It is also installed on our Midwife Led Unit at the RSH. Each new born has a tag fitted after delivery. Should the infant then be taken towards a doorway, including a fire exit, the tag will alarm and send doors into Lock Down mode whilst discreetly alerting staff at the nurse base via a PC type console so they can investigate. If doors are physically forced, breached or someone manages to tail-gate out, the system will immediately alarm in a very loud and audible manner. In the Women & Children's Centre should the alarms at the doors fail, a second layer of sensors will activate in the main foyer and each external entrance to the building. If the tag is forcibly removed or cut off the system automatically goes into alarm. The same occurs if the system detects an inability to communicate with a tag e.g. if the infant were wrapped in coverings or placed in a bag to enable unauthorised removal.

The system has also been included in the new build MLU at the PRH, construction of which was completed in March 2020.

As part of our security management assurance program, checks and testing of the system and staff reactions are carried out every 3 months by Ward Managers and the Trust Security Manager with feedback provided to senior management on the outcome from each test. A maintenance and support contract with the supplying company is in place to ensure system continuity and reliability. A 24/7 emergency telephone help line is included within the support element of the contract so staff have constant access to specialist technical support.

4 Communication, Awareness & Training

Efforts continue to raise staff awareness on security matters and encourage a proactive security culture. When appropriate, global e-mail alerts as well as screen messages can be sent out to all IT account users in the Trust.

4.1 *De-Escalation & Management Intervention (DMI) for Security Staff*

Security staff are the only trained resource at the Trust for the safe handling and restraint of physically violent or aggressive patients. To provide security staff with the skills and confidence to do this, specialist DMI training is delivered by accredited NHS training staff from the Midlands Partnership NHS FT.

The training, which consists of a 5 day foundation course and annual refresher days thereafter, has been accredited by the British Institute for Learning & Development (BILD) and the Institute of Conflict Management. A syllabus ordinarily delivered to NHS Mental Health professionals working at Midlands Partnership NHS FT is followed, but with additional bespoke content aimed at recognising the role of our security staff and the varied and different circumstances and settings experienced in a busy acute hospital environment.

In the reporting period 7 of our security staff undertook whole day annual refresher training whilst 4 new staff members completed the 5 day foundation course.

4.2 *Public Space CCTV Surveillance Training*

All of our security staff are licensed and trained in accordance with Security Industry Act requirements for use of CCTV equipment. During the period, 3 Security Officers undertook and successfully completed this training.

4.3 *Conflict Resolution Training (CRT)*

Learning & Development colleagues provide CRT for staff based on a previously issued DH national syllabus. CRT was delivered to 1368 frontline staff via 3 hour face to face sessions, 14 junior medical staff via e-learning induction and 753 other staff via e-learning[39].

4.4 *Lone Workers*

During the reporting period 5 members of staff who work alone in the community (regularly and/or occasionally) were trained on lone worker device usage and personal security. All staff using lone worker devices for use under the off-site strategy are given training by the service provider prior to a device being enabled. The training not only informs on how to use the device in terms of practicalities like switching on and off and battery charging, but also informs on the risks to lone workers identifying vulnerabilities and risk assessment.

4.5 *Corporate Induction*

During the period, 1094 staff members were given security and fraud awareness briefings and training at Corporate Induction by the Trust Security Manager[40].

[39]Figures from Learning Development 27 Apr 2020. These figures resulted in 87% compliance, just off the Trusts self-imposed target of 90% compliance.
[40]Figures from Learning Development 27 Apr 2020.

5 Conclusion/Year Ahead

In addition to maintaining and progressing the activity already covered by this report, we will also seek to:

- Stand by to support and guide the Trust on future security specifications, architecture and environment as it enters a phase of re-organisation and re-development of both hospitals (Hospitals Transformation Programme (HTP)) and do the same in relation to the refurbishment and/or maintenance of existing areas/new builds not affected by HTP and security risk assessment work.

- Continue to invest in the training of the security team to deal with conflict resolution and support clinical staff with agitated and confused patients.

- Continue to ensure clear messages are sent to perpetrators of unwelcome and anti-social behaviour to reinforce the Board's robust approach to abuse of staff and patients and at the same time support staff in reducing harm or injury from clinically aggressive patients.

- Continue to work closely with the Police and CPS to ensure the Trust continues to maintain its high prosecution of offenders

- Continue work to progress our intention to progress the recruitment and deployment of more security staff which should take place in Spring/Summer 2020 (numbers will increase from two to three on duty at each site 24/7).