FOI REF: 22/640

East Sussex Healthcare NHS Trust

22nd November 2022

Eastbourne District General Hospital
Kings Drive
Eastbourne
East Sussex
BN21 2UD

Tel: 0300 131 4500
Website: www.esht.nhs.uk

FREEDOM OF INFORMATION ACT

I am responding to your request for information under the Freedom of Information Act. The answers to your specific questions are as follows:

1. **Does your organisation have a policy that covers sexual safety, specifically preventing episodes of sexual misconduct and sexual violence involving patients, visitors and staff?**

   Yes.

2. **If your answer to question 1 was yes, please can you forward an electronic copy of the policy to me?**

   Please see attached East Sussex Healthcare NHS Trust's 'Dignity and Respect at Work Policy', Violence and Aggression Policy and Management of Security Policy.

3. **If your answer to question 1 was yes, what date did the policy become effective?**

   October 2022.

4. **If you have updated your policy within the past five years, please can you provide me with an electronic copy of the policy it replaced? If the information is available, please can you specify how your current policy is now different.**

   Not applicable.

5. **Has your organisation accepted vicarious liability for any cases of sexual assault or violence concerning any staff or patients in the past five years (2017 to date) (Please include any cases that may have led to an out of court settlement.)**

   The information requested above is collated by NHS Resolution and is available via their website which can be accessed using the link below:

   Factsheet 5 – trust and authority claims data 2020/21 - NHS Resolution

Cont…/

Freedom of Information requests to NHS Resolution can be made via the link below:

https://resolution.nhs.uk/freedom-of-information/

6. a) If your answer to question 5 was yes, please can you provide figures, specifically for the total number of cases and total compensation paid per year.

Please see above.

b) If possible, can you provide a breakdown for each case, specifying year; cost; whether the claimant was a patient, staff member or other (please specify): and whether the perpetrator was a staff member or patient?

Please see above.

If I can be of any further assistance, please do not hesitate to contact me.

Should you be dissatisfied with the Trust's response to your request, you have the right to request an internal review. Please write to the Freedom of Information Department (esh-tr.foi@nhs.net), quoting the above reference, within 40 working days. The Trust is not obliged to accept an internal review after this date.

Should you still be dissatisfied with your FOI request, you have the right of complaint to the Information Commissioner at the following address:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

Telephone: 0303 123 1113

Yours sincerely

Linda Thornhill (Mrs)
Corporate Governance Manager
esh-tr.foi@nhs.net

East Sussex Healthcare
NHS Trust

Dignity and Respect at Work Policy (Supporting a Culture of Civility and Respect)

Document ID Number:	2424
Version:	V1.0
Ratified by:	Clinical Documentation and Policy Ratification Group
Date ratified:	11 October 2022
Name of author and title:	[redacted], Associate HR Business Partner/[redacted] HR Advisor
Date Originally Written:	October 2022
Date current version was completed:	October 2022
Name of responsible committee/individual:	Chief People Officer, Human Resources
Date issued:	09 November 2022
Review date:	October 2025
Target audience:	All Staff
CQC Fundamental Standard:	Good Governance
Compliance with any other external requirements (e.g. Information Governance):	Advisory, Conciliation and Arbitration Service (ACAS)
Associated Documents:	Resolution Procedure Disciplinary Procedure Freedom to Speak Up; Raising Concerns (Whistleblowing) Policy Equality Diversity and Human Rights Policy

Did you print this yourself?
Please be advised the Trust discourages retention of hard copies of procedural documents and can only guarantee that the procedural document on the Trust website is the most up to date version

Version Control Table

Version number and issue number	Date	Author	Reason for Change	Description of Changes Made
V1	October 2022	[redacted]	Review and refine processes	Focus on creating positive culture; replaces Anti-Harassment & Bullying Policy

Consultation Table

This document has been developed in consultation with the groups and/or individuals in this table:

Name of Individual or group	Title	Date
Human Resources Directorate stakeholders		June 2022
Workforce Policies Partnership Group		September 2022

This information may be made available in alternative languages and formats, such as large print, upon request. Please contact the document author to discuss.

Table of Contents

1. Introduction

1.1 The Trust is committed to encouraging positive employee relations and providing a working environment free from harassment and bullying and ensuring all colleagues are treated and treat each other with civility and respect; in line with Trust Values.

1.2 We expect all colleagues to consistently demonstrate the Trust Values. However, as part of their professional and other standards our expectation is that colleagues act and take ownership to challenge inappropriate behaviour and address concerns, speak up about concerns and / or compassionately address concerns.

1.3 The Trust leaders endeavour to create an environment where people feel safe to speak up and have the confidence that any concerns will be addressed.

1.4 It is important to recognise incivility and act on it to prevent behaviours escalating. A timely resolution will be aided by addressing incivility in a respectful and caring manner, with open dialogue.

2. Purpose, Principles and Scope

2.1 This policy covers inappropriate behaviour including, incivility, discrimination, harassment or bullying which occurs at work and out of the workplace, such as on business trips or at work-related events or social functions. It covers bullying and harassment by colleagues (which may include external consultants, volunteers, contractors, and agency workers) and by third parties such as patients, suppliers, or visitors to our premises.

2.2 This policy does form part of the contract of employment, and it may be amended at any time following the usual process for changing policies.

2.3 Should colleagues raise a concern regarding incivility, harassment, discrimination, or bullying, privacy and confidentiality will be respected as far as possible; however, colleagues must be aware the issues raised may be disclosed through the process when seeking a resolution.

3. Definitions

3.1 What is Civility?

3.1.1 Civility is a collection of positive humane behaviours that produce feelings of respect, dignity, and trust. It's as simple as being polite to each other.

3.1.2 Civil workplaces provide better job satisfaction and improved mental health. Civility also builds trust and improves patient satisfaction and outcomes; civility saves lives. **Home | Civility Saves Lives | England**

3.2. What is incivility?

3.2.1 Incivility is different for each of us. Some people don't like to hear bad language, some don't like shouting. In general terms, incivility is belittling behaviour, being treated rudely or disrespectfully. It can also be gossiping, being ridiculed or excluded or being subjected to jokes or teasing that go too far. These experiences and perceptions can emerge over weeks, months or years and be so subtle that they may not fit a formal definition of bullying, harassment, or discrimination.

3.3 What is Discrimination?

3.3.1 **Direct Discrimination** is the unfair or unjust treatment of someone regarding one or more protected characteristic related to age, disability, gender reassignment, marital or civil partner status, pregnancy or maternity, race, (colour, nationality, ethnic or national origin), religion or belief, sex, or sexual orientation. A single incident can amount to discrimination.

For Example:

An employer is looking to hire an Executive Assistant. In the job application form, there's a question asking if the applicant has any disabilities that will make doing the job difficult.

As disability is a protected characteristic, this question is against the law. The employer should instead ask all applicants if they need any reasonable adjustments to complete the interview or any part of the recruitment process.

3.3.2 **Indirect Discrimination** is where there are rules or arrangements that apply to a group of employees, but in practice are less fair to a certain protected characteristic.

For example:

An employer decides that all staff must start a new shift pattern which involves working late in the evening. No staff can opt out. One member of the team takes medication which makes them feel very sleepy in the evenings, so they are not able to work late shifts.

This is likely to be indirect discrimination as it puts individual at a disadvantage.

But it will not be discrimination if the employer is able to justify the arrangement by showing that it is:

- for a good reason, and
- appropriate and necessary.

3.4 What is Harassment?

3.4.1 Harassment is any unwanted physical, verbal or non-verbal conduct that has the purpose or effect of violating someone's dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment for them. A single incident can amount to harassment.

3.4.2 It also includes treating someone less favourably because they have submitted or refused to submit to such behaviour in the past.

3.4.3 Unlawful harassment may involve conduct of a sexual nature (sexual harassment), or it may be related to age, disability, gender reassignment, marital or civil partner status, pregnancy or maternity, race, colour, nationality, ethnic or national origin, religion or belief, sex or sexual orientation. All harassment is unacceptable even if it does not fall within any of these categories.

3.4.4 Harassment may include for example:

a. unwanted physical conduct or "horseplay", including touching, pinching, pushing and grabbing;
b. unwelcome sexual advances or suggestive behaviour (which the harasser may perceive as harmless);
c. offensive emails, text messages, or social media content;
d. mocking, mimicking or belittling a person's disability;
e. unwelcome behaviour that is dismissed as 'banter'.

3.5 What is Bullying?

3.5.1 Bullying is offensive, intimidating, malicious or insulting behaviour involving the misuse of power that can make someone feel vulnerable, upset, humiliated, undermined, excluded, discriminated against, or threatened. Power does not always mean being in a position of authority but can include both personal strength and the power to coerce through fear or intimidation.

3.5.2 Bullying can take the form of physical, verbal, and non-verbal conduct. Bullying may include, by way of example:

a. physical or psychological threats;
b. overbearing and intimidating levels of supervision;
c. inappropriate derogatory remarks about someone's performance;

3.5.3 Legitimate, reasonable, and constructive criticism of someone's performance or behaviour, or reasonable instructions given to someone in the course of their employment, will not amount to bullying on their own.

4. Accountabilities and Responsibilities

Regardless of status, everyone working within the Trust is expected to treat colleagues with, civility, dignity, and respect in keeping with the Trust Values.

Every colleague has personal responsibility for their own behaviours in relation to this policy and to actively promoting civility in the workplace.

4.1 Management Responsibilities - It is the duty of managers to establish and maintain an environment that supports civility and respect and is free from harassment and bullying by:

4.1.1 ensuring that their own working practices reflect the above duty.

4.1.2 ensuring that all colleagues in their area of work are made aware that this policy exists and that they have a right to be treated with civility and respect and not be bullied, harassed, or discriminated at work.

4.1.3 taking prompt action to stop incivility, harassment, discrimination, and bullying. Highlighting that the behaviour is unacceptable, managers may be able to effectively put a stop to the problem without the need for formal action.

4.1.4 ensuring all complaints of incivility, harassment, discrimination, and bullying are treated seriously, compassionately and with confidence.

4.1.6 ensuring colleagues understand that the victimisation of anyone making a compliant or supporting someone making a complaint is unacceptable and where appropriate will be treated as a disciplinary matter.

4.2 All Staff – all colleagues have a responsibility to:

4.2.1. refrain from participating in, encouraging or condoning incivility, harassment, discrimination, or bullying.

4.2.2 report incidents of incivility, harassment, discrimination, or bullying in the knowledge that complaints will be dealt with in a sensitive manner.

4.2.3 support colleagues who raise concerns of incivility, harassment, discrimination, or bullying and encourage them to seek help from an appropriate source.

5. Procedures and Actions to Follow

5.1 If Colleagues are being treated with Incivility

5.1.1 Colleagues should consider whether they feel able to raise the problem informally with the person responsible. They should explain clearly to their colleague that their behaviour is not welcome or makes them feel uncomfortable. If this is too difficult or embarrassing, they should speak to their line manager (or line manager's manager), the Human Resources Department, their Trade Union Representative, or Speak up Guardian who can provide confidential advice and assistance in resolving the issues.

5.1.2 Addressing concerns informally are always the preferred course of action, the reasons for this are;

- sometimes colleagues are not aware that their behaviour is unwelcome, and an informal discussion can lead to greater understanding and an agreement that the behaviour will cease
- an informal process will always be less damaging to working relationships and less stressful for all those involved.

5.1.3 Should a colleague feel raising the problem directly with the colleague responsible has not been successful consideration should be given to whether further action under the Trust's Resolution Procedure will enable the matter to be resolved.

5.2 If you are being harassed, bullied, or discriminated against

5.2.1 Colleagues should consider whether they feel able to raise the problem informally with the person responsible. They should explain clearly and politely to them that their behaviour is not welcome or makes them feel uncomfortable. If this is too difficult or embarrassing, they should speak to their line manager (or line manager's manager), the Human Resources Department, the Freedom to Speak Up Guardian, or their Trade Union Representative who can provide confidential advice and assistance in resolving the issues formally or informally.

5.2.2 Raising concerns informally may be appropriate if the colleague raising the concern believes the behaviour is unintentional and the person accused is unaware of its impact.

5.2.2 If informal steps are not appropriate, or have not been successful, colleagues should raise the matter through Formal Resolution under the Trust's Resolution Procedure.

5.2.3 If appropriate, concerns will be investigated in a timely and confidential manner, in accordance with the Resolution Procedure. The investigation will be conducted by someone with appropriate experience and who has had no prior involvement in the complaint, wherever possible. Details of the investigation and the names of the person making the complaint and the person accused will be disclosed on a "need to know" basis. Consideration will be given to whether any steps are necessary to manage any ongoing relationship between the colleague raising the concern and the person accused during the investigation.

5.2.4 Once the investigation is complete, colleagues will be informed of the decision. If it is considered that a colleague has been harassed or bullied by another colleague, the matter may be dealt with under the Disciplinary Procedure as a case of possible misconduct or gross misconduct. If the harasser or bully is a third party such as a patient, or other visitor, the Trust will consider what action would be appropriate to deal with the problem. Whether or not the complaint is upheld, it will then be considered how best to manage any ongoing working relationship between the colleague raising the complaint and the person concerned.

5.3 Victimisation – Protection and support for those involved

5.3.1 Should a colleague make a complaint or participate in good faith in any investigation they must not suffer any form of reprisal or victimisation as a result. Anyone found to have retaliated against or victimised others in this way will be subject to disciplinary action under our Disciplinary Procedure.

5.3.2 Should a complaint be raised against a colleague and subsequently the outcome is the complaint is unfounded the colleague raising the complaint must not suffer any form of reprisal or victimisation as a result. Anyone found to have retaliated or victimised in this way will be subject to disciplinary action under our Disciplinary Procedure.

5.3.3 Should it be found that a complaint is malicious or vexatious, further action may be taken under the Trust's Disciplinary Procedure.

5.4 Employee Support

5.4.1 Being subject to incivility, bullying, discrimination, harassment, or victimisation or being subject to difficulties in the workplace giving cause to raise concerns can be very upsetting and stressful for the member of staff and other colleagues affected, including those whom allegations may have been raised against. Managers will use the Staff Support Checklist to ensure that support is identified for all colleagues affected (Appendix A).

5.4.2 Where there are concerns about an employee's health or wellbeing, Occupational Health advice will be obtained.

5.4.3 Members of staff, including other colleagues affected, will have access to Carefirst and can obtain information on support services available via the Occupational Health and Wellbeing, Supporting the Emotional Wellbeing of Staff extranet page

5.4 Record Keeping

5.4.1 Information about a complaint by or about a colleague may be placed on their personal file, along with a record of the outcome and of any notes or other documents compiled during the process. These will be processed in accordance with our Data Protection Policy.

Data collected from the point at which the Trust commences action under this policy is held securely and accessed by, and disclosed to, individuals only for the purposes of managing a complaint.

Inappropriate access or disclosure of employee data constitutes a data breach and should be reported in accordance with the organisation's data protection policy immediately. It may also constitute a disciplinary offence, which will be dealt with under the Trust's disciplinary procedure.

6. Equality and Human Rights Statement

An Equality and Human Rights Impact assessment has been carried and is documented in Appendix B.

7. Training

Please refer to the Induction and Mandatory training policy and the Training Needs Analysis. On-line guidance of the policies referred to in this policy can be found via the Extranet Page, Human Resources.

8. Monitoring Compliance with the Document

Monitoring Table

Element to be Monitored	Lead	Tool for Monitoring	Frequency	Responsible Individual/Group/ Committee for review of results/report	Responsible individual/ group/ committee for acting on recommendations/action plan	Responsible individual/group/ committee for ensuring action plan/lessons learnt are Implemented
Number of informal and formal complaints, time taken, outcomes and learning	Deputy Director of HR	HR case management log which provides data on cases in terms of ethnicity, age, gender and staff group	Half Yearly	Quality and Safety Committee	People and Organisational Development Committee.	Quality and Safety Committee
Staff Perceptions of Harassment and Bullying	Assistant Director of HR; Workforce Development	Staff Survey Results	Annually	Assistant Director of HR to provide a report to Management Team.	People and Organisational Development Committee	People and Organisational Development Committee

9. References

ACAS – Bullying and Harassment at Work

NHS Terms and Conditions of Service
Civility saves lives website
Just culture
Safety II Suzette Woodward
Equality Act 2010

Appendix A
Staff Support Checklist

This checklist should be used to ensure that staff are provided with timely and appropriate support and that a record of actions taken is kept.

This form should be completed as appropriate (at the outset of the process and revisited on at least one further occasion) and retained by the manager until the matter is at an end. A copy of checklist should be forwarded to the HR Dept. so that it may be used for the annual audit process.

Employee name	
Job title	
Manager name	
Date completed	

SUPPORTING STAFF		**Initial support**	**Follow-up**
		Date	
1.	Has a 'Buddy/Mentor' been offered, identified and agreed?		
2.	Has the staff member been signposted to Care First?		
3.	Was a referral to Occupational Health & Wellbeing discussed with the employee? give details, dates etc		
4.	Has other support been offered to the employee? Yes / No If yes, detail any support taken up. *Include any considerations given for staff with protected characteristics and the impact any action may have e.g. disability, race; where necessary seek advice from ESHT Workforce Human Rights & Equality lead.*		
5.	Has a copy of the procedure been provided to the employee and the process explained?		

Initial Support	
Manager Signature	**Date**
Employee Signature	**Date**

Follow-Up Support	
Manager Signature	**Date**
Employee Signature	**Date**

ACTIONS
Copy of completed form given to employee
Original Form to be filed in staff member's file
Copy of completed form sent to Human Resources

Appendix B – EHRA Form

Equality Impact Assessment Form

1. Cover Sheet

Please refer to the accompanying guidance document when completing this form.

Strategy, policy or service name	Dignity and Respect at Work Policy (Supporting a Culture of Civility and Respect
Date of completion	16 September 2022
Name of the person(s) completing this form	Mark Roper
Brief description of the aims of the Strategy/ Policy/ Service	The Trust is committed to encouraging positive employee relations and providing a working environment free from harassment and bullying and ensuring all colleagues are treated and treat each other with civility and respect; in line with Trust Values.
Which Department owns the strategy/ policy/ function	Human Resources
Version number	V1.0
Pre Equality analysis considerations	None
Who will be affected by this work? **E.g. staff, patients, service users, partner organisations etc.**	Staff
Review date	3-yearly
If negative impacts have been identified that you need support mitigating please escalate to the appropriate leader in your directorate and contact the EDHR team for further discussion.	To whom has this been escalated? Name: Click here to enter text. Date: Click here to enter a date.
Have you sent the final copy to the EDHR Team?	No

2. EIA Analysis

<table>
<tr><td></td><td>☺ 😐 ☹</td><td>Evidence:</td></tr>
<tr><td>Will the proposal impact the safety of patients', carers' visitors and/or staff?

Safe: Protected from abuse and avoidable harm.</td><td>Positive</td><td>Procedure will allow staff to raise and resolve issues relating to dignity and respect at work, maintaining positive employee relations</td></tr>
<tr><td>Equality Consideration
Highlight the protected characteristic impact or social economic impact (e.g. homelessness, poverty, income or education)</td><td></td><td>
<table>
<tr><td>Race</td><td>Gender</td><td>Sexual orientation</td><td>Age</td><td>Disability & carers</td></tr>
<tr><td>☒</td><td>☒</td><td>☒</td><td>☒</td><td>☒</td></tr>
<tr><td>Gender reassignment</td><td>Marriage & Civil Partnership</td><td>Religion and faith</td><td>Maternity & Pregnancy</td><td>Social economic</td></tr>
<tr><td>☒</td><td>☒</td><td>☒</td><td>☒</td><td>☒</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td>Is the proposal of change effective?

Effective: Peoples care, treatment and support achieves good outcomes, That staff are enabled to work in an inclusive environment. That the changes are made on the best available evidence for all involved with due regards across all 9 protected Characteristics</td><td>Positive</td><td>Procedure will allow staff to raise and resolve issues relating to dignity and respect at work, maintaining positive employee relations</td></tr>
<tr><td>Equality Consideration
Highlight the protected characteristic impact or social economic impact (e.g. homelessness, poverty, income or education)</td><td></td><td><table>
<tr><td>Race</td><td>Gender</td><td>Sexual orientation</td><td>Age</td><td>Disability & carers</td></tr>
<tr><td>☒</td><td>☒</td><td>☒</td><td>☒</td><td>☒</td></tr>
<tr><td>Gender reassignment</td><td>Marriage & Civil Partnership</td><td>Religion and faith</td><td>Maternity & Pregnancy</td><td>Social economic</td></tr>
<tr><td>☒</td><td>☒</td><td>☒</td><td>☒</td><td>☒</td></tr>
</table></td></tr>
<tr><td>What impact will this have on people receiving a positive experience of care?</td><td>Neutral</td><td>Click here to enter text.</td></tr>
<tr><td>Equality Consideration
Highlight the protected characteristic impact or social economic impact (e.g. homelessness, poverty, income or education)</td><td></td><td><table>
<tr><td>Race</td><td>Gender</td><td>Sexual orientation</td><td>Age</td><td>Disability & carers</td></tr>
<tr><td>☒</td><td>☒</td><td>☒</td><td>☒</td><td>☒</td></tr>
<tr><td>Gender reassignment</td><td>Marriage & Civil Partnership</td><td>Religion and faith</td><td>Maternity & Pregnancy</td><td>Social economic</td></tr>
<tr><td>☒</td><td>☒</td><td>☒</td><td>☒</td><td>☒</td></tr>
</table></td></tr>
</table>

<table>
<tr><td>Does the proposal impact on the responsiveness to people's needs?</td><td>Positive</td><td>Procedure will allow staff to raise and resolve issues relating to dignity and respect at work, maintaining positive employee relations</td></tr>
<tr><td>Equality Consideration Highlight the protected characteristic impact or social economic impact (e.g. homelessness, poverty, income or education)</td><td></td><td>
<table>
<tr><td>Race</td><td>Gender</td><td>Sexual orientation</td><td>Age</td><td>Disability & carers</td></tr>
<tr><td>☒</td><td>☒</td><td>☒</td><td>☒</td><td>☒</td></tr>
<tr><td>Gender reassignment</td><td>Marriage & Civil Partnership</td><td>Religion and faith</td><td>Maternity & Pregnancy</td><td>Social economic</td></tr>
<tr><td>☒</td><td>☒</td><td>☒</td><td>☒</td><td>☒</td></tr>
</table>
</td></tr>
<tr><td>What considerations have been put in place to consider the organisations approach on improving equality and diversity in the workforce and leadership?</td><td>Positive</td><td>Procedure will allow staff to raise and resolve issues relating to dignity and respect at work, maintaining positive employee relations</td></tr>
<tr><td>Equality Consideration Highlight the protected characteristic impact or social economic impact (e.g. homelessness, poverty, income or education)</td><td></td><td>
<table>
<tr><td>Race</td><td>Gender</td><td>Sexual orientation</td><td>Age</td><td>Disability & carers</td></tr>
<tr><td>☒</td><td>☒</td><td>☒</td><td>☒</td><td>☒</td></tr>
<tr><td>Gender reassignment</td><td>Marriage & Civil Partnership</td><td>Religion and faith</td><td>Maternity & Pregnancy</td><td>Social economic</td></tr>
<tr><td>☒</td><td>☒</td><td>☒</td><td>☒</td><td>☒</td></tr>
</table>
</td></tr>
<tr><td colspan="3">Access
Could the proposal impact positively or negatively on any of the following:</td></tr>
<tr><td>• Patient Choice</td><td>Neutral</td><td></td></tr>
<tr><td>• Access</td><td>Neutral</td><td></td></tr>
<tr><td>• Integration</td><td>Neutral</td><td></td></tr>
</table>

Equality Consideration *Highlight the protected characteristic impact or social economic impact (e.g. homelessness, poverty, income or education)*		<table><tr><td>**Race**</td><td>**Gender**</td><td>**Sexual orientation**</td><td>**Age**</td><td>**Disability & carers**</td></tr><tr><td>☒</td><td>☒</td><td>☒</td><td>☒</td><td>☒</td></tr><tr><td>**Gender reassignment**</td><td>**Marriage & Civil Partnership**</td><td>**Religion and faith**</td><td>**Maternity & Pregnancy**</td><td>**Social economic**</td></tr><tr><td>☒</td><td>☒</td><td>☒</td><td>☒</td><td>☒</td></tr></table>
Engagement and Involvement How have you made sure that the views of stakeholders, including people likely to face exclusion have been influential in the development of the strategy / policy / service:	Positive	Stakeholders have been involved in the drafting of the policy
Equality Consideration Highlight the protected characteristic impact or social economic impact (e.g. homelessness, poverty, income or education)		<table><tr><td>**Race**</td><td>**Gender**</td><td>**Sexual orientation**</td><td>**Age**</td><td>**Disability & carers**</td></tr><tr><td>☒</td><td>☒</td><td>☒</td><td>☒</td><td>☒</td></tr><tr><td>**Gender reassignment**</td><td>**Marriage & Civil Partnership**</td><td>**Religion and faith**</td><td>**Maternity & Pregnancy**</td><td>**Social economic**</td></tr><tr><td>☒</td><td>☒</td><td>☒</td><td>☒</td><td>☒</td></tr></table>
Duty of Equality Use the space below to provide more detail where you have identified how your proposal of change will impact.	Positive	
Characteristic	**Rating** ☺ ☹ 😐	**Description**
Race	Positive	Procedure will allow staff to raise and resolve issues relating to dignity and respect at work, maintaining positive employee relations
Age	Positive	As above
Disability and Carers	Positive	As above
Religion or belief	Positive	As above

Sex	Positive	As above
Sexual orientation	Positive	As above
Gender re-assignment	Positive	As above
Pregnancy and maternity	Positive	As above
Marriage and civil partnership	Positive	As above

Human Rights

Please look at the table below to consider if your proposal of change may potentially conflict with the Human Right Act 1998

Articles		Y/N
A2	Right to life	**No**
A3	Prohibition of torture, inhuman or degrading treatment	**No**
A4	Prohibition of slavery and forced labour	**No**
A5	Right to liberty and security	**No**
A6 &7	Rights to a fair trial; and no punishment without law	**No**
A8	Right to respect for private and family life, home and correspondence	**No**
A9	Freedom of thought, conscience and religion	**No**
A10	Freedom of expression	**No**
A11	Freedom of assembly and association	**No**
A12	Right to marry and found a family	**No**
Protocols		
P1.A1	Protection of property	**No**
P1.A2	Right to education	**No**
P1.A3	Right to free elections	**No**

East Sussex Healthcare NHS Trust

Violence and Aggression Policy (including Red/Yellow card system)

Document ID Number:	695
Version:	V6
Ratified by:	Policy Ratification Group
Date ratified:	14 July 2020
Name of author and title:	John Kirk, Facilities and Security Manager John Harmer, Security Manager
Date originally written:	December 2008
Date current version was completed:	November 2020
Name of responsible committee/individual:	Chris Hodgson, Associate Director – Estates
Date issued:	21 December 2020
Review date:	21 November 2023
Target audience:	All Staff
Compliance with CQC Fundamental Standard	
Compliance with any other external requirements (e.g. Information Governance)	
Associated Documents:	• Incident Reporting and Management Policy • Policy for the Investigation of Incidents, Complaints and Claims • Policy and Procedure for the Recording, Investigation and Management of Complaints, Comments, Concerns and Compliments (4C Model) • Lone Worker Policy • Health and Safety at Work Policy • CCTV Policy • Supporting Staff • Policy Mandatory • Training Policy • Management of Security • Equality Policy

Did you print this yourself?
Please be advised the Trust discourages retention of hard copies of procedural documents and can only guarantee that the procedural document on the Trust website is the most up to date version.

Version Control Table

Version number and issue number	Date	Author	Reason for Change	Description of Changes Made
V2 2011060 (Policy for Management and Prevention of Aggression and Violence)	December 2008	East Sussex Hospitals NHS Trust - Head of Complaints & Legal Services, Risk Manager and the Security Manager		
V3	December 2009	Joint PCT - Health and Safety Officer		Policy arrangements on the Management of Violence and Aggression
V4	March 2010	Joint PCT - Health and Safety Officer		Policy on With holding Treatment from Violent and Abusive Patients
V4.1 2012195	September 2012	John Harmer, John Kirk et al		
V4.2 2013132	June 2013	John Harmer, John Kirk et al	Alignment with NHSLA requirements	Responsibilities Definitions
V5 2015118	May 2015	John Kirk	Review	General review
V6	November 2020	John Kirk	Complete review	Changes to the whole document including Letters

Consultation Table

This document has been developed in consultation with the groups and/or individuals in this table:

Name of Individual or group	Title	Date
Cross-Site Security Group	All members	March 2015
Estates & Facilities Management Team	All members	April 2015
Health & Safety Steering Group	All member	April 2019 and May 2020
Damien Reid: Director of Finance	Security Managing Director (SMD)	May 2020

This information is available in alternative languages and formats, such as large print, upon request. Please contact the document author to discuss.

Table of Contents

1. Introduction

The Trust is committed to providing an environment that is safe and secure for all staff, service users and visitors as far as is reasonably practicable. Staff, service users and visitors have an obligation to behave in a suitable and appropriate manner. Therefore acts of violence, abuse or threatening behaviour are not acceptable and the Trust will aim to eliminate, minimise and control the risk of violence and aggression.

Our values ensure that all our colleagues are working to create high standards of care and a positive experience for all our service users. This policy is underpinned by the core behaviours linked to our values, e.g. Working Together, Respect and Compassion, Engagement and Involvement, Improvement and Development. These are important to everyone, and are embedded in our culture. We expect to see these behaviours demonstrated at all times by our colleagues at work and the people who use our services.

The Health and Safety Executive has adopted the following definition of work related aggression and violence as "*any incident in which a person is abused, threatened or assaulted in circumstances relating to their work, involving an explicit or implicit challenge to their safety, well-being or health*" (HSE Policy on Management of Work-related Aggression & Violence 2018; Linking Service & Safety: Together Creating Safer Places of Service, McKenna K., 2008).

2. Purpose

2.1. Rationale

The purpose of this policy is to ensure that staff, patients, contractors and visitors are provided with an environment that is safe and secure and minimises the risk of violence and aggression. It also provides framework as to the steps to take should an individual experience violence and aggression in our health care settings.

2.2. Principles

NHS Protect (formerly the NHS Security Management Service) was disbanded in 2018 but its standards and guidance are still used in the NHS. Namely the protection of:

- Patients, staff and visitors
- NHS Property and assets
- Drugs, prescription forms and hazardous materials.

These objectives will be achieved as follows:

- Security surveys will continue to be undertaken for Trust premises and specific working practices where required.
- All departments will undertake an annual security risk assessment and action as appropriate.
- ESHT will ensure that security advice is provided by the Trust Security Department to ESHT staff and others who work or use Trust properties.
- All staff have a responsibility to assist with any security risk assessment in order to highlight measures taken to reduce and/or control any identified risks.
- ESHT will provide relevant training, including Conflict Resolution and other specialist breakaway/restraint training as highlighted within the organisational training needs analysis and the Mandatory Training Policy.

Staff Support Policy makes it clear that ESHT will support staff if they become victims of physical or non-physical abuse but that also staff must be aware of their actions and the effect of those actions when dealing with patients, relatives and visitors. In the event of an incident with physical or psychological repercussions, Occupational Health will support staff in affiliation with specialist services if indicated.

This Policy does not in any way preclude any member of staff from pursuing a private prosecution of any description. Any individual has the right to report an actual or perceived assault to the police.

Any physical assault on ESHT staff described by the NHS SMS definition should be reported as soon as practicable to the Police by the person assaulted, their manager or colleague. ESHT cannot report assaults on a member of staff to the Police if:

- That member of staff does not want to pursue it; or
- That a member of staff wishes to drop the case against a person who has committed the assault.

2.3. Scope

This policy applies to all ESHT staff working for or on behalf of the organisation including volunteers. All ESHT employees will be treated in a fair and equitable manner and reasonable adjustments will be made where appropriate. This policy also applies to patients, visitors, volunteers and contractors.

3. Definitions, Sources and examples of Violence & Aggression

3.1 Violence and Physical Assault

"The intentional application of force against a person or another without lawful justification, resulting in physical injury or personal discomfort"
Source: Physical Assault Definition contained within Directions to NHS Bodies November 2003.

3.2 Aggression (non-physical assault)

"The use of inappropriate words or behaviour causing distress and/or constituting harassment"
Source: Non-Physical Assault Definition contained within Directions to NHS Bodies November 2003.

The difference between aggression and assertiveness must be understood and able to be recognised in a situation by staff so that a judgment can be made as to whether the incident actually constitutes nonphysical assault.

- Aggression - The person being aggressive will have a total disregard for the other person's interests or position. Aggressive behaviour has the result of the other person feeling hurt, belittled, controlled or humiliated.

- Assertiveness - A person is honest, direct and stands up for themselves in such a way that does not intimidate, belittle or leave the other person feeling violated.

3.3 Hate Crime

Hate crime is any criminal offence committed against a person or property that is motivated by hostility towards someone based on their disability, race, religion, gender identity or sexual orientation. In these cases a sanction should be considered.

3.4 Lone Working

Lone workers can be at a greater risk and this is defined as working without a colleague nearby or when out of earshot or sight of a colleague. Situations include:

- Staff arriving early on a regular basis to open a department.
- Community staff and other domiciliary staff.
- Maintenance staff working alone in plant rooms or grounds staff.
- Clinical staff working autonomously.

The Trust has a separate Lone Workers and Personal Safety Policy which is available on the Health and Safety section of the extranet. Managers who have staff working alone must undertake a risk assessment which can be completed in line with the Security assessment.

3.5 Clinical Exceptions to Violence or Aggression

There may be occasions when a clinical specialist advises that the assault was unlikely to have been intentional - the assailant did not know what they were doing or they did not know that what they had done was wrong. This may be due to a medical illness, mental ill-health, a severe learning disability or as a result of treatment administered.

Before considering a Yellow/Red card, all other options highlighted in Appendix A, C and D should be considered.

4. Sources of Violence and Aggression

It is important that Trust staff can recognise and understand how and when banter, innuendo, raised voices, rude gestures or environmental stressors can arise, escalate and provoke people to become frustrated and angry and this can subtly or very quickly turn into overt aggression or violence.

In making a risk assessment the following factors *(these are not exhaustive lists or examples)* are just some of the multi-faceted ways which may indicate that there is a likely risk of abuse or violence occurring when dealing with members of the public/patients/visitors/relatives i.e. people who are:

1. Angry at waiting times or delays in treatment.
2. Afraid / lonely / emotionally charged / cold and hungry.
3. Children and teenagers who are immature and/or have limited sense of their responsibilities.
4. Confused / disorientated / suicidal / distressed / depressed.
5. Intoxicated / drug or medication abusers / people who self-harm, self-mutilate, self-neglect.
6. Suffering from mental illness / stress / bereavement / domestic or sexual abuse.
7. Alzheimer patients / patients who have had a stroke or a head injury.
8. Have a criminal history of violence / recidivists.
9. Referred to ESHT because they were abusive or violent in other NHS organisations or GP practices.

4.1 Examples of Non-Physical assault/inappropriate behaviour

This recognition is an essential part of assessing the potential risks of imminent dangers to staff. The following are just some examples of unacceptable standards of behaviour that may result. These are also examples of the types of abuse incidents that staff must complete a DATIX for; including near-miss and incidents where it is assessed are ‘no-harm’.

1. Threatening or abusive language involving swearing or offensive remarks and behaviour.
2. A lot of abuse can be face to face, but it may also come by other forms of messaging such as by telephone, letter, Texts, e-mail, graffiti, tweets, Instagram, Facebook or photographs.
3. Pointing fingers, staring, inappropriate touching or invading personal space.
4. Abusing alcohol or drugs in Trust hospitals and premises.
5. Excessive noise e.g. loud or intrusive conversation or shouting; also, abusive telephone conversations, playing loud music, an instrument or mobile phone sounds.
6. Throwing acid, any other corrosive substance or any other fluid or object.
7. Derogatory racial, ethnic or religious remarks, provocations, signs or actions.
8. Offensive sexual gestures or behaviours, openly defecating, urinating or spitting.
9. Malicious allegations, stalking or blackmail relating to staff, other patients or visitors.
10. Creating noxious fumes, smoking in a waiting rooms, clinics or wards.
11. Arson or any other wilful damage to personal property, Trust property, medical equipment, or theft thereof.
12. Inciting other people, dogs or animals to attack.
13. Any incident where there are weapons (knives or guns) present, or brandishing of articles such as walking sticks, crutches, cricket bats, kitchen cutlery, household furniture, laser pens, which are used to threaten and intimidate.
14. Overt violence, conflict, malicious acts or deliberate intentions to commit such acts / kicking, biting, scratching, lashing out.
15. Filming, taking photographs or mobile phone videos without permission.
16. Unreasonable behaviour or non-co-operation.

5. Accountabilities and Responsibilities

5.1. Chief Executive

The Chief Executive will ensure that ESHT has robust policies and procedures in place for security and security arrangements.

As stipulated by The NHS Security Management Service in Directions to NHS Bodies on Security Management Measures 2004 (Amendment) Directions 2006.

The Chief Executive will also ensure that:

- A Security Management Director is appointed – currently the Director of Finance.
- That a Security Management Non-Executive Director is appointed to assist in the improvement of ESHT security.
- That a Local Security Management Specialist (LSMS) is appointed to lead on the day to day management of security work within ESHT, to advise the Directors and Senior Managers, and to enable the implementation of the Policy.

5.2. Security Management Director (SMD) / Non-executive Director

Executive Director responsible (currently Director of Finance) for security and security management arrangements is responsible for providing, so far is reasonably practicable, a safe and secure working environment and ensuring the safety and security of employees, patients, users and others.

The non-executive Director is available to support any security related projects or themes.

The SMD will communicate at Board level on strategies to tackle violence against staff. They will also ensure that systems, processes and procedures are in place to manage violence and aggression.

5.3 Security Department and Local Security Management Specialist

The Security Department with the LSMS is responsible for providing day to day management of security. In addition they will:

- Advise on the implementation of security and security management policies and specific control measures.
- Compile an Annual report and Work plan.
- Undertake security surveys of Trust premises and risk rate, highlighting necessary actions.
- Ensure clear procedures are in place to accurately record all relevant information relating to incidents involving violence and aggression in order to identify trends.
- Ensure full cooperation is given to the police in respect of investigations and any subsequent action taken.
- Review all security related incident reports via Datix database and where necessary make contact with the person or service reporting the security incident in line with the organisation Incident Management Policy.
- Provide a six monthly Security report to the Health and Safety Steering Group to include Performance Indicators.
- Review the provision of contracted security services on a monthly basis.

5.4 Integrated Education

Integrated Education will undertake an annual training needs analysis. The training needs analysis will take into account;

- The sources of violence and aggression.
- The level of training that all staff are required to undertake for example:
    - Conflict Resolution Training
    - Breakaway training
    - Disengagement Training
    - Physical Intervention or Clinical Restraint training.
- The role of staff and specific risks including whether these are:
    - Non clinical staff including ward clerks, porters and switchboard for example
    - Front line Emergency care staff
    - Community based domiciliary staff
    - Ward based staff including Frailty and Dementia.

In addition they will:

- Undertake an annual review of the training needs analysis.
- Monitor the efficacy of the training in conjunction with the Security department.
- Determine the commissioning of the training where required.
- Report on the compliance levels of mandatory training.
- Report on the levels of specialist training.

5.5 Divisional Governance Leads, General Managers/Heads of Nursing

Divisional Governance Leads, General Managers/Heads of Nursing will:

- Disseminate this Policy through the management structure effectively in order that all areas within the span of their control are aware of the Policy.
- Fully support their line managers in carrying out the requirements of this Policy. Any

concerns will be raised at Divisional Governance meetings.
- Report on incidents relating to Violence and Aggressive as part of standardised reporting to the Trust Health and Safety Steering Group and the Trust Security Group.

5.6 Managers/Matrons

Managers/Matrons have a delegated responsibility for the safety of their staff and patients, in particular for ensuring compliance with this policy. Managers/Matrons will disseminate the Policy contents to staff within their Unit, Ward or Department, in addition they will:

- Ensure mandatory training (e.g. Conflict Resolution training) is undertaken by themselves and all staff they manage.
- Undertake Workplace Activity Risk Assessments that include violence and aggression and lone working and keep those risk assessments reviewed as stated by the Risk Assessment Policy.
- Undertake an annual Security risk assessment in order to identify environmental and other risk factors that may contribute to the risk of security, violence or aggression.
- Make sure that any member of staff who is a victim of violence and aggression is given positive practical support in line with the Trust Dignity at Work Policy.
    - Refer the individual to Occupational Health and Wellbeing: referrals may be flagged as urgent if required.
    - Signpost staff to Care First so that staff can access immediate emotional support from the Trust Employee Assistance Programme.
- Report any incident, whether witnessed or experienced using the Trust Incident Reporting Systems as soon as is practically possible.

5.7 Staff

All staff have a responsibility to take care of the health and safety of themselves and others who may be affected by their acts or omissions. In addition responsibilities include:

- To make themselves aware of the contents of this Policy.
- Actively contribute to risk assessments and the implementation and use of control measures.
- Report any shortcomings or failings in the control measures to their manager or the LSMS if necessary.
- Undertake Violence & Aggression Training in accordance with local needs where identified.
- Report any incidents of violence and aggression to their manager so they can be offered appropriate help and support.
- Reporting incidents on the Trusts incident reporting system.
- Consider calling the Police in the event of a physical assault, serious verbal abuse, or a hate crime.

5.8 Occupational Health and Wellbeing

Occupational Health and Wellbeing will:

- Review any Datix incidents rated 3 or above which involve a staff member being a victim of violence and aggression and make contact with the employee to offer additional support including access to specialist services as required.
- Assist both staff members and their managers in terms of rehabilitation back to work following an incident.

5.9 Human Resources

Human Resources will offer support, advice and guidance, they will:

- Refer to policies including Support for Staff following and Incident, Complaint or Claim as well as policies for attendance, redeployment or stress.
- Receive information from managers where an incident occurs between members of staff so the incident can be investigated under the Dignity at Work or Disciplinary Policy.

5.10 Legal Department

The Legal Department provides advice on all matters where there is a risk of legal claims being filed against the Trust as well as providing advice on matters where the legal rights of staff and individuals to whom the Trust owes a duty of care are jeopardised or infringed. Incidents of violence or aggression may well interfere with the legal rights of those who are the victims and the Legal department can be contacted for advice directly should this be the case.

5.11 Shared Services/Independent Contractors

ESHT offers and shares a number of unique services in partnership with other local agencies and at various locations including GP practices, Dental services, Pharmacists, etc. Shared services are employers in their own right and as such shared services have an obligation for the protection of staff and patients.

In buildings where GP's and other shared services operated, ESHT have a duty under the Health and Safety at Work Act 1974 and the Management of Health and Safety at Work Regulations 1999 to conduct health and safety assessments and advise shared services of the findings.

Security risk assessments will be conducted by the LSMS for physical security measures such as CCTV, access control and intruder alarm systems.

Shared services / independent contractors have a responsibility to their staff to conduct lone workers assessments that may impact on violence and aggression, violence and aggression assessments, general security arrangements and training.

6. Managing Violence and Aggression proactively

All incidents must immediately be reported to a line manager and a Datix entry completed. Consideration should also be given to calling security and reviewing if a sanction is appropriate.

6.1 Identifying and managing risk to reduce incidents of Violence and Aggression

6.1.1 Risk Assessment

All departments must complete:

- Workplace Activity Risk Assessment in accordance with the Trust Risk Assessment Policy.
- Annual Security Assessment.

A plan of action to address risks identified by the risk assessment must be developed. These risks will be monitored and managed by divisional Governance Managers in conjunction with the Security Team.

Risk Assessments must be reviewed should there be a revision to service, the level of risk or the environment.

6.1.2 Environmental Risks

The security risk assessment should also reflect the local environment and any factors that may contribute to a persons' behaviour. Risks can be reduced by using the following hierarchy:

- Design the problem out
- Eliminate or remove the risk
- Substitute with a less risky option
- Isolate from people
- Reduce time of exposure and numbers exposed
- Safe systems of work/protocols
- Supervision/training
- PPE.

The assessor should also consider:

1. The hospital environment itself and the sounds and smells therein.
2. Cancelled clinics and appointments or delays in ambulance transport.
3. Family disputes and disagreements on a patient's care or treatment.
4. Inadequate or confusing direction signage and instructions.
5. Lack of amenities, parking spaces, toilet facilities, refreshments, disabled access, wheelchairs.
6. Overcrowded, hot / cold and noisy waiting rooms, inadequate seating and long delays in clinic appointments.
7. Medical or IT equipment failures and cancellation of operations, possibly at short notice and without adequate explanation.
8. Poor clinic or ward layout / mixed male / female units which compromises dignity and privacy.
9. Shortages of managers and reception staff resulting in a lack of information, poor or absent communications and services.
10. Smoking or vaping within the hospital and its grounds.

6.1.3 Security Work Plan

Security Management is monitored in line with security management service guidelines with an annual report and security work plan by the LSMS and agreed with the SMD. The following points show how violence and aggression is managed within ESHT:

- Annual roadshow to raise staff awareness of how to tackle violence and aggression.
- Personal attack alarms are provided free on request to all staff.
- Reminders and advice are included in the quarterly Security Wise publication.
- Any member of staff who reports any verbal and / or physical assault will be fully supported by their line manager or human resources. Support from OH & W can be accessed via self-referral.
- Incident pattern analysis will be conducted to highlight problem areas so actions can be targeted as appropriate.
- Site security surveys will be conducted to help reduce the risks of incidents. Action plans resulting from risk assessments will be agreed with managers to tackle problem areas and monitored annually via security audits.
- Staff will receive Conflict Resolution Training on a 3 yearly basis Information is available from the LSMS and internal security extranet page. In ESHT buildings violence and aggression posters must be displayed and audited by the LSMS.

7. Dealing with Violence and Aggression Reactively

All options detailed in Appendices A, B and C should be reviewed before considering a Yellow / Red card.

7.1 Yellow Card Warnings

A YELLOW Card is issued when:

- Patients and visitors non-physically assault Trust, contracted staff and /or professionals who work in, or provide services, to the NHS or engage in other forms of anti-social behaviour.
- Capacity/children/chronically ill – see App N for guidance

These individuals must be able to be readily identified by staff.

The individuals may be issued with a formal written warning of the consequences of such behaviours (A "Yellow Card Warning"). Non-physical assaults include but are not limited to verbal abuse, threats, intimidation, malicious communication.

Divisional General Managers (Band 7 or above) / Head of Department are responsible for ensuring Yellow Card warnings are issued in a timely fashion. The Trust Security Advisor may provide advice to line managers on the appropriateness of issuing Yellow Card Warnings or other sanctions.

If a patient complies with the terms of the Yellow Card Warning they can expect that:

- Their clinical care will not be affected in any way.
- Where substance abuse has been identified, appropriate assistance will be provided through the normal appropriate referral processes.
- East Sussex Healthcare NHS Trust will fully investigate all valid concerns raised by the patient, visitor or visitor's relative.
- The Yellow Card Warning will lapse after one year from the date of the incident provided that there have been no repeat occurrences.

A copy of the Yellow Card Warning will be included in the patient's Health records, attached to the relevant Datix Incident Report and a record made in the Special Register on Oasis E-Searcher. It is important to note that a Yellow Card Warning or Red Card Sanction may not be issued without a Datix Incident Report being raised.

Where the perpetrator is a relative accompanying a patient who was receiving treatment at the time of the incident, both the perpetrator's records and the patient's records will be annotated to record that the relative has received a Yellow Card Warning. This does not reflect on the patient's conduct, affect their access to treatment but merely acts to warn staff of the potential risk of violence and aggression. The patient and perpetrator will be informed in writing by the Head of Department that their records have been marked.

All Yellow Card warning letters will be logged by the Trust LSMS. Yellow Card warnings will be shared with the police, ambulance service and patient's G.P. as a matter of routine. Police and the ambulance service will be informed by the Trust Security Advisor by secure e-mail, i.e. nhs.net and police.pnn e-mail. G.P.s will receive a copy of the letter from the issuing manager by secure e-mail or by post. The Trust reserves the right to inform other external agencies, e.g. other healthcare providers that an individual has been issued with a Yellow Card Warning. PAS and Datix will be updated by the LSMS.

Failure to comply with the Yellow Card Warning and at the request of the relevant Executive Director will result in the exclusion from the Trust ("Red Card Sanction").

7.2 Red Card Sanction

A RED card is issued when:

Patients and visitors physically assault staff, patients and professionals who work in, or provide services to, the NHS;

Or

Conduct is in breach of a Yellow Card Warning, thus triggering a Red Card Sanction being issued;

Or

An offence where no physical assault has taken place but the disruption to the delivery of care is so severe that a Yellow Card Warning is deemed insufficient.

The individual's identity must be able to be established by staff.

Capacity/children/chronically ill – see App N for guidance

General Managers (or nominated deputy in their absence) are responsible for drafting Red Card Sanction letters for authorisation by an Executive Director. Where the perpetrator was a patient at the time of the incident, the General Manager must seek the written approval (e-mail confirmation will suffice) from the consultant in charge in the patient's care at the time of the incident. The consultant will determine that the patient had capacity and that there were no mitigating clinical factors which would preclude the perpetrator from receiving a Red Card Sanction.

The Clinical Director or Clinical Lead MUST sign off the Consultant's approval prior to the Red Card Sanction letter being submitted to the Executive Director for signature.

Where the patient's consultant is not available to advise and would lead to a prolonged delay in issuing the Sanction (more than three working days) the Clinical Lead or Clinical Director will be consulted. In the Clinical Director or Clinical Lead's absence the Medical Director will be approached for sign off.

A patient who was drunk or under the influence of illegal substances at the time of the incident has no defence in law and the issue of capacity should not normally be a determinant.

The authorising Executive Director will normally be the Director of Nursing in their capacity as the Security Management Director. The Trust Security Advisor may provide advice to line managers and the Executive Director on the appropriateness of issuing Red Card Sanctions or other sanctions.

If a patient does not use Spoken English as their main method of communication, a copy of the letter must be sent to esh-tr.accessibleinformation@nhs.net for translation into the perpetrator's first language. Translation normally takes 1-2 working days and therefore this timeframe/delay must also be taken into consideration. Both the English and alternative language version must be placed on the patients' record.

The conditions of a Red Card Sanction
are:

- Access to Trust services limited to EMERGENCY care only.
- Entitlement to attend outpatient appointments or undergo pre-planned procedures at

this Trust is withdrawn.
- Entitlement to enter Trust premises as a visitor is withdrawn unless approved in advance in writing by the Trust.
- If attendance at hospital for emergency care occurs, the Trust staff may call on security staff / police to be in attendance during this treatment. If the senior clinician on duty believes the recipient does not require emergency care they will be instructed to leave the hospital premises; failure to do so will result in the Trust to take appropriate action to remove them from the hospital. Similarly, if they do require emergency care, they will be instructed to leave the hospital premises once medical treatment has been concluded; failure to do so will result in the Trust taking appropriate action to remove them from Trust premises.
- The Trust may also seek a prosecution under criminal or civil law, and/or apply for an injunction or other appropriate sanctions.

A Red Card Sanction does not have an Expiry Date.

A copy of the Red Card Sanction will be included in the patient's health records, attached to the relevant Datix Incident Report and a record made in the Special Register on Oasis E-Searcher.

Where the perpetrator is a relative accompanying a patient who was receiving treatment at the time of the incident, both the perpetrator's records and the patient's records will be annotated to record that the relative has received a Red Card Sanction. This does not reflect on the patient's conduct, affect their access to treatment but merely acts to warn staff of the potential risk of violence and aggression. The patient is to be informed in writing that their records have been marked.

Red Card Sanctions will be logged by the LSMS who will also update Oasis E-Searcher and Datix.

Red Card Sanctions will be shared with the police, ambulance service and patient's G.P. as a matter of routine. The Trust reserves the right to inform other external agencies, e.g. other healthcare providers that an individual has been issued with a Red Card Sanction.

7.2.1 Management of Red Card recipients who still require emergency care

Where a Red Card recipient attends the Emergency Department, security should be called to attend immediately. The senior doctor/nurse on duty will decide if the attendee genuinely requires emergency treatment. If the attendee does require emergency treatment, serious consideration should be given to having security staff remain in attendance for the duration that treatment is required in the department. Once treatment is complete and the attendee is fit for discharge, then the attendee must leave immediately or be subject to removal as defined within this policy.

However, if admission is unavoidable serious consideration should be given to having security remaining in attendance for at least the first 24 hours after admission. An appropriately trained member of staff will determine the need for security attendance. Prolonged security staff attendance for an in-patient is not a core service and will be charged at the appropriate hourly rate.

Where the Red Card recipient does not require emergency treatment they are to be instructed to leave immediately or be subject to removal as defined within this policy.

A Datix Incident Report must be completed for any Red Card recipient coming on Trust premises regardless of their conduct.

Where a person attends Trust premises in breach of a Red Card Sanction, and not requiring emergency care, an Anti-Social Behaviour Injunction should be considered. The LSMS must be contacted in such circumstances for this action to be considered and actioned if appropriate.

7.3 Appeals: Yellow Card Warning

The recipient of the Yellow Card Warning is entitled to appeal against the decision in writing to the Chief Executive within fourteen working days of receipt of the notification.

The written communication requesting an appeal must include all evidence to be relied upon by the recipient. The appeal will be carried out and decisions reached based upon the written submissions only from both parties. There is no right of audience for either party involved.

On receipt of the written request for appeal, the Chief Executive must nominate a senior member of staff (normally a Director or Deputy / Associate Director) to carry out an appeal hearing. The nominated senior member will contact the author of the Yellow Card letter within fourteen days of the notification of appeal to obtain evidence for consideration. This may include written statements from any/all witnesses to the alleged offence and any other evidence which might be available. The Trust Security Advisor will provide advice and assist if required.

The appeal will result in the following:

- To uphold the Yellow Card Warning
- To withdraw the Yellow Card Warning.

The outcome of appeal panel's decision will be communicated in writing to the recipient within fourteen days, be binding and final.

7.4 Appeals: Red Card Sanctions

The recipient of the Red Card Sanction is entitled to appeal against the decision in writing to the Chief Executive within fourteen working days of receipt of the notification.

On receipt of the request for appeal, the Chief Executive will nominate an appropriate Director, Deputy Director or Associate Director to carry out an initial desktop review of the facts concerning the issuing of the Red Card. The desktop review may make a number of recommendations:

There is no prime facie case for changing the Red Card, in which case an Appeal Hearing will be convened to consider the facts and make a final decision.

1. The Red Card Sanction may be down-graded to a Yellow Card Warning, in which case the appellant will be advised and asked if they wish to appeal against the Yellow Card. The Yellow Card appeals procedure will be followed to consider the appeal.

2. The Red Card may be cancelled as the violence/aggression was attributable to the appellant's clinical condition at the time of the incident and no further sanctions applied; however the appellant is still considered to pose a risk to staff. The Special Register on PAS will be annotated to warn staff of the risk and how the risk is to be managed. The appellant is to be notified of this fact.

3. The Red Card may be cancelled and no further sanctions applied.

The Appeal Panel may consist of: one Executive Director, Trust Security Advisor and a clinical representative familiar with the patient and their care.

The author of the Red Card letter will be invited to present the 'Management case' including the

presentation of any other evidence deemed relevant. They may also call on any witnesses deemed appropriate.

The alleged offender may then present the 'Defence case' and may bring a friend or family member to support them, but the alleged offender is not entitled to be represented by a legal representative. The offender may call on any witnesses they choose specific to the event and may additionally include a witness as to their good character.

The Management and Defence parties will not be entitled to question each other directly, but questions to either side will be allowed through the Chair of the Panel.

The appeal panel may decide to:

- Uphold the Red Card Sanction
- Withdraw the Red Card Sanction
- Extend the offender's access to hospital care to include non-urgent care with conditions.

The outcome of appeal panel's decision will be communicated in writing to the recipient, be binding and final.

7.5 Reviews of warnings and sanctions (Yellow and Red Cards)

Yellow and Red Card letters are measures designed to protect staff and improve behaviour. Staff who report incidents which culminate in the issuing of warnings and sanctions will be expected to support and fully engage with the process.

Six months after the date of the incident, an offender issued with a Yellow Card may request that the Trust reviews any restrictions placed on them. An offender issued a Red Card Sanction may request a review twelve months after the date of the incident. The offender will need to demonstrate how their behaviour no longer presents a risk to Trust staff.

The review of restrictions will be undertaken by an Executive Director. This may involve a meeting with the offender and consideration of relevant evidence. The offender will be advised of the outcome of the review in writing and there will be no right of appeal. All paperwork relating to the review will be placed on the individual's health record where possible.

8. Equality and Human Rights Statement

An Equality and Human Rights Analysis has been completed, and has not identified any Equality and Human Rights issues that impact on groups related to this policy.

9. Monitoring Compliance with the Document

9.1 Process for Monitoring Compliance

See table below.

9.2 Document monitoring

ESHT adopts the NHS policy of "zero tolerance" towards violence and aggression. Incidents are captured on the Trust's incident reporting system, Datix, and investigated locally at department or clinical unit level. Statistics are also reported by the Security Department to the Health & Safety Steering Group and to the Trust Board.

Document Monitoring Table

Element to be Monitored	Lead	Tool for Monitoring	Frequency	Responsible Individual/Group/ Committee for Review of Results/Report	Responsible Individual/ Group/Committee for Acting on Recommendations/ Action Plan	Responsible Individual/group/ Committee for Ensuring Action Plan/Lessons Learnt are Implemented
Board Level Accountability	LSMS	Annual Report	Yearly	Board/SLF	CEO/Board/SLF	CEO/Board
Risk Assessments Undertaken	Divisional Governance Leads	Assure – compliance report	Quarterly	HSSG	Divisional Governance Lead	Divisional Governance Meeting
Training Needs Analysis	Integrated Education	Training Needs Analysis	Yearly	Security Group	Divisional Governance Leads, Clinical unit Manager	Divisional Governance Meetings Health and Safety Steering Group
Staff Referrals and Support	OH & W	eOPAS	Quarterly	HSSG	OH & W Manager	Health and Safety Steering Group
Training Compliance	Workforce	ESR	Monthly	Divisional Governance Lead	SLF	CEO/Board/SLF

10. References

Violence and Aggression posters and advice are available from ESHT Local Security Management Specialist (LSMS). Such information can be downloaded from www.CFSMS.nhs.uk

Acknowledgement

NHS Leeds, Violence and Aggression Policy, November 2009
Violence & Aggression Policy, East Kent Hospitals University NHS Foundation Trust 2012

11. Associated Documentation

This policy is supported by Trust and other related references: Secretary of State Directives and other legislation.

- Management of Security in the NHS 2004
- Tackling Violence against NHS Staff 2006
- Equality Act 2012
- Health and Safety at Work Act 1974
- Police and Criminal Evidence Act 1984
- Criminal Law Act 1977 (powers of arrest) Regulation of Investigatory Powers Act 2000
- Protection from Harassment Act 1997
- Criminal Justice & Immigration Act 2008
- NHS Security Management Measures 2004

Appendix A

General guidance for the management of people exhibiting Violent and Aggressive Behaviour

Throughout this section "people" or "person" includes patients/service users/relatives/visitors/staff

Introduction

Experience shows that often violence is minor and in the majority of cases, skilled action can resolve the incident quickly and satisfactorily without serious confrontation or restraint becoming necessary. A violent attack seldom occurs but when it does it is usually over quickly. It is important that a staff member at the scene notifies other staff, the appropriate medical staff and a manager if a person shows signs of potential violence.

The distress which is associated with physical and mental illness often reveals itself in fear, turmoil and agitation in people. A mood of suspicion and irritability may escalate into apparent hostility, which is a symptom of underlying desperation felt by the individual and usually does not lead to violence, provided the response is not antagonistic.

Recognition of potential violence

Violent behaviour cannot always be prevented, as it is sometimes impulsive. However, it is possible to recognise someone who may be potentially violent and what situations are likely to precipitate such violence. It follows therefore, that most incidents of violent behaviour should not take staff by surprise but should be planned for in advance.

Some of the factors, which may indicate that violence might occur, include:

- The person may be noisy, abusive or impulsive.
- The person may appear to be having disturbed relationships.

Causative factors

- Drug dependency
- Alcoholism
- Alcohol consumption
- Metabolic disturbance dementia
- Cerebral lesions Mania Depression
- Suicidal tendencies.

Knowledge and understanding of a particular person may reveal signs of impending violence, e.g. in the person's face, gestures or conversation.

It may be known that the person has a history of violence or aggressive behaviour. Staff may be aware of emotional instability, anxiety, frustration or hostile feelings in a person. There may be environmental factors or a conflict between people.

Summoning assistance

It should never be assumed that people will automatically give assistance. They should be asked to help, as otherwise they may not be aware help is needed. Staff can develop local coded responses to use to alert colleagues that help is required.

If necessary and if the circumstance applies, the police should be contacted to help safeguard other people and maintain the rest of the service.

Prevention of violence and dealing with aggression and verbal abuse

1. Identify themselves, presenting their ID, avoid confrontation and arguing back.
2. Adopting a sympathetic, empathic, understanding approach, and attempt to show some affinity with the other person's position.
3. Speaking and standing calmly with open posture, but always remaining balanced and ready to move away.
4. Speaking clearly and slowly and not necessarily stopping talking because the other person does not respond.
5. Distracting the person from the immediate cause of concern by changing the course of conversation – buying time to think, to plan, to obtain assistance.
6. Trying to identify the source of concern and offering to help if possible.
7. Not disagreeing or countering an argument where it is not necessary.
8. Not giving orders or using status or authority as a threat.
9. Not making threats or promises that cannot be carried out or offering rewards for what probably started out as improper and possibly unlawful conduct.
10. Controlling behaviour in body language, feelings, expressions or gesticulations.
11. Being alert and sending for assistance and being prepared to leave immediately to avoid an escalation of the situation or possible injury.
12. Remain calm and state politely but assertively that the behaviour is unacceptable, pointing out why the particular behaviour is inappropriate or offensive.

Dealing with episodes of violence
Restraint and the laying of hands upon another person is technically a common assault.

General guidelines

- Always call for assistance
- Ask other people to summon help

All staff should be appropriately dressed when on duty and before dealing with potentially violent incident. They should remove objects that could be potentially dangerous from their clothing.

- Try to appear calm, talk to the person continually and quietly.

Appendix B

Management of Patient/Service Users Exhibiting Violent and Aggressive Behaviour in the Community and ESHT Building

Principle of prevention

The best way to deal with violence is to prevent it, always in a professional manner. The following guidance, which is intended for use by any other member of staff when their work takes them out into the community, is intended to highlight some of the preventative measures that can be taken.

Members of staff should consider the issues raised and develop their own plan to ensure that their work can be carried out safely as possible.

Those conducting risk assessments and managers must consider the following guidance, when deciding on control measures for ESHT activities taking place in the community.

Every member of staff in contact with patients/service users in the community should have regular opportunities to discuss problems and methods of dealing with them with colleagues, their manager and medical staff.

Checklists for home visits

Before leaving

- Make appointments with the patient/service users prior to the visit and avoid self-referrals wherever possible.
- Contact a colleague or manager if you are unhappy about making a visit alone. Check records and risk assessment forms for known difficulties. If you are deputising for another member of staff make sure that they brief you on foreseeable difficulties.
- Check the destination and make sure that the route to be taken is as safe as possible. Always consider the time of day, weather conditions, breakdown etc.
- Check that the vehicle is regularly serviced and that fluid and fuel levels are satisfactory.
- Let others know where you are going and when you are expected to return.
- Be aware that wearing jewellery may make you vulnerable, e.g. a necklace could be tightened around your neck or non-stud earrings ripped out during an attack. Jewellery that is noticeable may also increase the risk of muggings, as is walking and talking on a mobile phone, carrying equipment etc.
- Avoid using earphones and listening to music while walking as this could increase the likelihood of attack.

En-route

- Consider the time and route you are taking. Lock your vehicle doors whilst travelling.
- Do not leave equipment on view inside your vehicle; where possible store them in your boot.
- Check that you are not being followed. If you feel uneasy or uncertain remain in your vehicle and drive to a place of safety. Contact your base to advise them of the situation and if necessary contact the Police.

Car jacking

- Whilst travelling, if you are signalled to stop your vehicle by anything other than a marked police vehicle do not stop and drive to a point of safety. Keep your doors locked until you can identify those requesting you to stop. A police officer will produce a warrant card.
- If unsure keep doors and windows locked, if under attack sound the horn, flash the lights and if possible ring the Police by dialling 999.

On arrival

- Park your car safely, and in such a position that you could drive off easily in an emergency and if possible park in a well-lit area as close to your destination point as possible.
- Before leaving the car ensure all equipment, medicines and prescription pads are out of view, preferably locked in the boot.
- Close all windows and lock the car.
- Do not advertise 'Doctor/Nurse on call' unnecessarily. Be alert of your surroundings.
- Use your judgment before entering lifts; could other occupants become violent or someone enter the lift at another level?
- If you are in any doubt about the premises you are visiting, do not enter them: seek advice and assistance. If this is not feasible, abort the visit and return to your base.

During the visit

- Watch out for hazards in a home, such as poor lighting, trailing flexes, narrow or steep staircases, fire hazards and pets. Alert colleagues who may also be visiting.
- Never force your way into a patient's/service user's home. Always ask permission to enter if you have not been invited in.
- Always explain clearly the purpose of your visit and/or any procedure to be carried out.

After the visit

- Confirm that you have completed the visit with the appropriate person so that they are aware that you are leaving.
- If necessary debrief your manager, team leader etc. of any problems encountered on the visit. Ensure that any information which could be useful to staff making visits in future is recorded.
- If necessary, contact other agencies following a visit. Agencies include the Police, Social Services etc. If in doubt on whom you can contact, discuss with ESHT Information Governance Manager and/or the Trust solicitor.

Appendix C

Guidance for Dealing with Incidents of Violence and Aggression in the Community and Patients' Homes

Dealing with a violent incident in patient's/service user's home:

- Staff should make every effort to call the alleged offender; they should speak firmly but quietly to them. In rare circumstances where the presence of another individual is making the situation worse, it is sometimes best to seek a way of separating the patient/service user from the other individual.

- It is recommended emergency contact numbers via your speed dial button are programmed into your mobile phone. Speed dial numbers can include the police.

- Extra help should be called if possible if it seems that it may be needed. At this point, when violence is only a possibility, other people should not burst upon the scene, this could easily precipitate violence. They should either stay just outside the room where the disturbed patient/service user is, or if any of the relatives are on particularly good terms with the patient/service user, that individual could help.

- If violence is directed to a member of the family and they are sustaining an injury, contact the Police for emergency assistance.

- In all cases, staff should not forget to bring their mobile phones on visits.

- If violence is directed at a child, the ESHT Safeguarding Children Team should be contacted as per Trust policy.

- If violence is directed at an adult, the ESHT Safeguarding Adult Team should be contacted as per Trust policy.

- If violence is directed at a member of ESHT staff when no help is available, and you are unable to manage the patient/service user, turn and break free, leave immediately and inform management and the Police if a member of staff would like to pursue an allegation.

- In all such circumstances an incident report form must be completed.

- ESHT will ensure all relevant frontline staff receives Conflict Resolution Training.

Dealing with a violent incident in a clinic setting:

- ESHT staff and patients matter more than property. If a patient is damaging property, move patients away and if possible contact the Police.

- If another patient is being attacked staff must not place themselves in any danger, seek assistance, and contact the Police.

- If a violent attack takes place or a violent attack is threatened call for assistance. If a building is fitted with a panic alarm system staff must be trained on its use and the system should be activated.

- Some systems are connected to the Police, but for the most panic alarm systems will only sound within the building itself.

- Actions from your local risk assessment should be included for staff to react to.

- If a panic alarm is sounded, contact the location the alarm has been activated from by phone. Where CCTV is installed check the area before attending the scene.

- If attending the scene, be alert and don't rush into a situation. If an alarm has been activated inside a room and the door is closed, do not rush in; try and contact the room by telephone. If no reply knock on the door but do not enter and if necessary contact the Police.

- If the alarm has been set off by mistake, ask the person inside the room to present themselves to the main reception area.

Appendix D

Yellow Card Warning (Formal Warning)

The issuing of a Yellow Card can only be instigated in the event of inappropriate behaviour. For patients, this should be following review by the individual's clinical team. See section 6.1 of Policy. Visitors may be issued a Yellow Card without review by a clinical team. Yellow Card templates are available at Appendix G.	
Authorised by	**Actions Required**
Head of Department/ Divisional Lead	The incident must be reported via the Datix Incident Reporting System giving the detailed nature of abuse, specific language used and that a Yellow Card (formal warning) has been issued. A Yellow Card cannot be issued until the incident is recorded on Datix. Note: Information and advice should be sought from the patients Consultant, a senior member of the medical team if appropriate.
	The offender must be informed of the staff concerns. If still on site, discuss concerns in person and confirm in writing. If off-site in writing only. The Yellow Card procedure must be explained to them and the consequences of failure to comply with the standard of behaviour required.
	Within seven working days, the offender should be given the formal letter of notification and be informed of their right to appeal.
	Relevant people within the Trust should be informed of this decision including: • Trust Security Advisor • Site Management • Director of Human Resources • Clinical Governance Department • General Managers & Matrons.
	The line manager is to ensure a copy of the Yellow Card sanction is sent to the patient's G.P and Trust Security. The Trust Security Advisor will notify SECAmb and the Police that a Yellow Card Warning has been issued. Other healthcare providers and neighbouring acute Trusts may be notified if deemed appropriate.
	The Trust Security Advisor will: • Annotate PAS to record that Yellow Card warning has been issued. • Request Health Records of recipient so that copy of Yellow Card Warning can be inserted at front of health record. Note: The Trust Security Advisor will remove Yellow Card warnings from PAS and health records at the appropriate time.

Appendix E

Red Card Sanction (Access to Emergency Care Only)

<table>
<tr><td colspan="2">A Red Card limits an individual's access to the hospital to emergency care only. See section 6.2 of Policy. Upon issue, the Trust may seek other sanctions including prosecution.
Security staff must be informed immediately without delay if an excluded individual returns under any circumstances, even if it is to receive care in an emergency (life threatening).
A Red Card template is available at Appendix H.</td></tr>
<tr><td>Authorised by</td><td>Actions Required</td></tr>
<tr><td>It can only be issued by an Executive Director (Normally the Director of Nursing).

Issuing of a Red Card Sanction must not be delayed due to the absence of the Director of HR.</td><td>The incident must be reported via the Datix Incident Reporting System, giving the detailed nature of the incident. Full details of the incident and any staff members concerns must be recorded. It must be established whether a Yellow Card is currently in force.

Note: Approval must be sought from the patient's Consultant, a senior member of the medical team where the perpetrator is a patient in order to determine patient's capacity and any mitigating clinical factors at the time of the incident. The relevant Clinical Director or Clinical Lead must sign off the decision before the draft Red Card letter is submitted to the Executive Director for signature.

The authorising Executive Director will send a letter of the decision to the patient's home address.</td></tr>
<tr><td rowspan="5"></td><td>The offender must be informed of the staff concerns. If still on site, discuss concerns in person and confirm in writing. If off-site, in writing only.

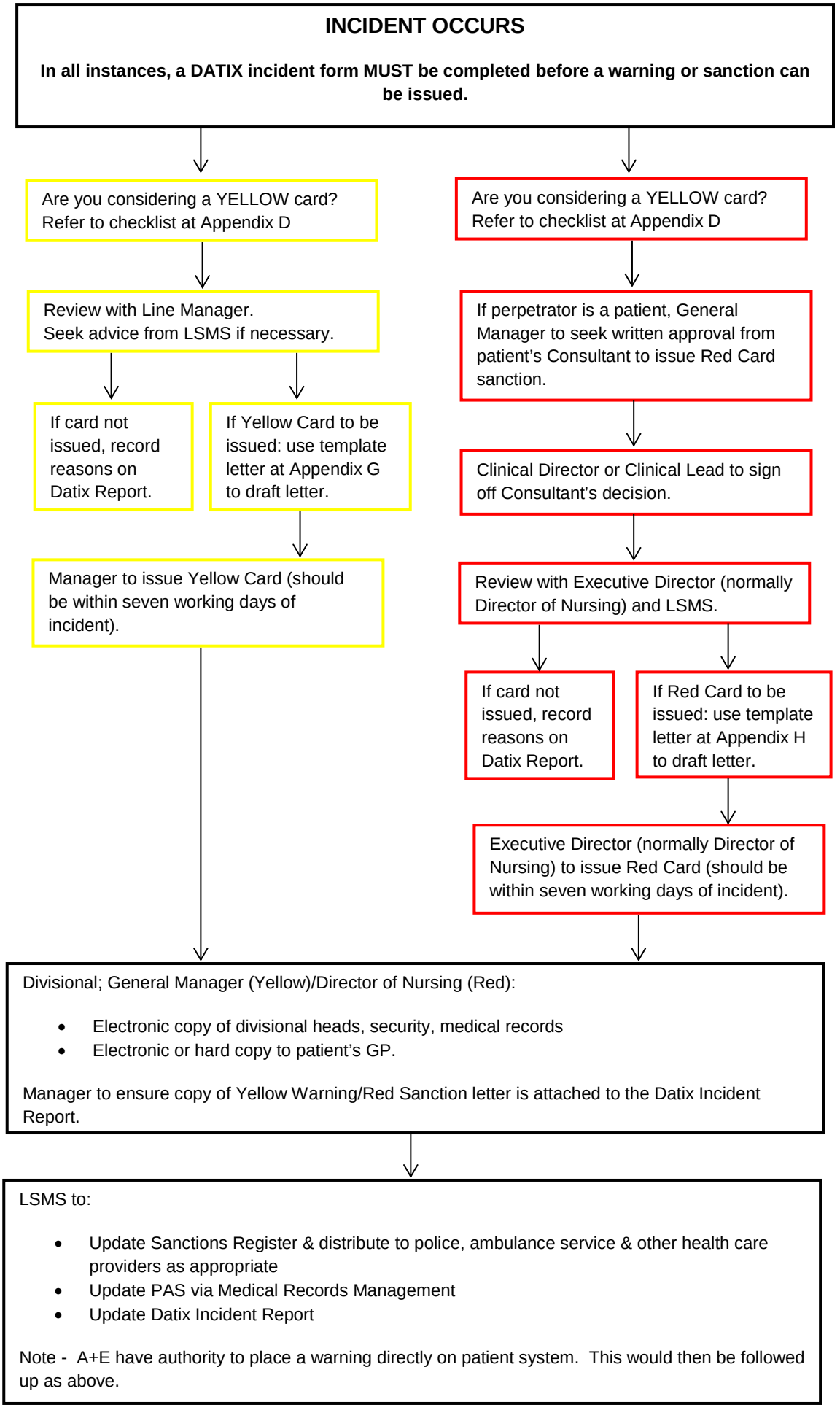
The Red Card procedure must be explained to them and the consequences of this action.</td></tr>
<tr><td>If on-site, the offender must be given the formal letter of notification and be informed of their right to appeal.</td></tr>
<tr><td>Relevant people within the Trust should be informed of this decision including:
Trust Security Advisor
Site Management
Director of Human Resources
Clinical Governance Department
General Managers & Matrons.</td></tr>
<tr><td>The line manager is to ensure a copy of the Red Card sanction is sent to the patient's G.P.

The Trust Security Advisor will notify SECAmb and the Police that a Red Card Sanction has been issued. Other healthcare providers or neighbouring acute Trusts may be notified if deemed appropriate.

The Trust Security Advisor will:
• Annotate PAS to record that a Red Card Sanction has been issued.
• Request Health Records of recipient so that copy of Red Card Sanction can be inserted at front of health record.</td></tr>
<tr><td>Note: The Trust Security Advisor will remove Red Card warnings from PAS and health records at the appropriate time.</td></tr>
</table>

Appendix F

Sanctions Flow Chart



Template Letter: Yellow Card Warning

East Sussex Healthcare NHS Trust

Private and Confidential

Hospital Number: **[Insert Hosp Number]**
NHS Number: **[Insert NHS Number]**

[Insert Patient's Name, Full address including postcode]

Date: **[Insert Date]**

Eastbourne District General Hospital
Kings Drive
Eastbourne
East Sussex
BN21 2UD
Direct Line Tel: 01323 41****
Email:****@nhs.net
Website: www.esht.nhs.uk

Datix No. **[Insert WEB*****]**

Dear **[Insert Name]**

We are committed to providing a safe and secure environment for our staff, patients and visitors. It has been reported to me that on the **[Insert Date]** you **[account of what happened including detailed nature of abuse including any specific language used]**.

I have evidence of this behaviour in the form of **(incident form/witness statements/ CCTV footage]**. (Optional - At the time, it is reported that you were under the influence of drugs/excessive alcohol). This behaviour has been reported to the police, the ambulance service and your G.P. for their information. The Trust reserves the right to inform other external agencies, e.g. other healthcare providers that you have been issued with a Yellow Card Warning. Optional if appropriate: This incident has been reported to the police for investigation.

NHS staff are entitled to be treated with courtesy and respect, and I hope that now you have had time to reflect, you will agree that your behaviour was unacceptable.

Because of the seriousness of what has happened, I am issuing you with this letter which is to be regarded as a 'Yellow Card Warning', that is, a first and final formal warning. If you should behave with disregard to the safety and wellbeing of our staff again, you may be issued with a 'Red Card Sanction' which will mean your access to Trust premises will be limited to emergency care only.

In order to protect the safety of our staff in future, a copy of this letter will be placed on your electronic and paper health record, and will also be flagged to alert staff on the Patient Administration System.

If you wish to appeal against this action, you are entitled to write to the Chief Executive, in writing, within fourteen working days of receipt of this letter. A copy of the appeals process is enclosed. This warning will remain valid for 12 months from the date of issue.

You may request this to be reviewed after 6 months provided no further similar incidents have occurred.

I hope that this warning will deter you from any future poor behaviour on NHS premises.

[Signature of authorising officer]

[Name of authorising officer]
[Role Title]

Enclosed: Appeals process

cc: **[Patient's G.P]**

Appendix H

Template Letter: Red Card Sanction

East Sussex Healthcare NHS Trust

Private and Confidential

Hospital Number: **[Insert Hosp Number]**
NHS Number: **[Insert NHS Number]**

[Insert Patient's Name, Full address including postcode]

Date: **[Insert Date]**

Eastbourne District General Hospital
Kings Drive
Eastbourne
East Sussex
BN21 2UD
Direct Line Tel: 01323 41****
Email:****@nhs.net
Website: www.esht.nhs.uk

Datix No. **[Insert WEB*****]**

Dear **[Insert Name]**

It has been reported to me that on the **[Insert Date]** you **[account of what happened including detailed nature of abuse including any specific language used]**. I have evidence of this behaviour in the form of (incident form/witness statements/CCTV footage). This behaviour has been reported to the police and the ambulance service. The Trust reserves the right to inform other external agencies, e.g. other healthcare providers, that you have been issued with a Red Card Sanction.
(Optional - For gross and extreme behaviour):

This is extreme behaviour caused significant risk/harm/injury to NHS staff/property and as such was reported immediately to the police as a serious criminal matter. I understand the police are **[details of police, charging, arrest, prosecution]** and the Trust is helping them with their enquiries.

(For repetition of less extreme behaviour, following previous Yellow Card):

You have previously been warned about abusive/violent behaviour on the **[insert date/s]** and were advised that any repetition of such behaviour may result in a 'Red Card' sanction may be issued.

As a consequence of your actions I am issuing you with this letter which is to be regarded as a "Red Card' sanction under which the Trust is entitled to limit your access to this hospital to EMERGENCY care only. You will not be entitled to attend outpatient appointments or undergo pre-planned procedures at this Trust. You may not enter Trust premises as a visitor unless approved in advance in writing by the Trust.

- Your access to this hospital is for EMERGENCY care only.
- You will not be entitled to attend outpatient appointments or undergo pre-planned procedures at this Trust.

- You may not enter Trust premises as a visitor unless approved in advance in writing by the Trust.
- If you need to come to hospital for emergency care, the Trust staff may call on Security staff /Police to be in attendance during this treatment. If the Senior Clinician on duty believes you do not require emergency care you will be instructed to leave the hospital premises; failure to do so will result in the Trust to take appropriate action to remove you from the hospital. Similarly, if you do require emergency care, you will be instructed to leave the hospital premises once medical treatment has been concluded; failure to do so will result in the Trust taking appropriate action to remove you from Trust premises.
- We may also seek a prosecution under criminal or civil law, and/or apply for an injunction or other appropriate sanctions.

In order to protect the safety of our staff in future, a copy of this letter will be placed on your electronic and paper health record, and will also be flagged to alert staff on the Patient Administration System.

A copy will be sent to your GP; so that they can make alternative arrangements with another hospital should you need non urgent care or treatment.

If you wish to appeal against this action, you are entitled to appeal to the Chief Executive, in writing, within fourteen working days of receipt of this letter. A copy of the appeals process is enclosed. This warning will remain valid for an indefinite period from the date of issue. You may request this to be reviewed after 12 months provided no further similar incidents have occurred.

I am taking this action to protect the wellbeing and safety of staff working in this Trust and other patients and visitors using our services.

[Signature of authorising officer]

[Name of authorising officer]

[Role Title]

Enclosed: Appeals process

cc: **[Patient's G.P]**

Appeals: Yellow Card Warning (Delete as appropriate)

The recipient of the Yellow Card Warning is entitled to appeal against the decision in writing to the Chief Executive within fourteen working days of receipt of the notification.

The written communication requesting an appeal must include all evidence to be relied upon by the recipient as the appeal will be carried out and decisions reached based upon the written submissions only from all parties. There is no right of audience for either party involved.

On receipt of the written request for appeal, the Chief Executive must nominate a senior member of staff to carry out an appeal hearing. Within fourteen days, the nominated senior member will contact the author of the Yellow Card letter to obtain evidence for consideration of the appeal. This may include written statements from any/all witnesses to the alleged offence and any other evidence which might be available. The Trust Security Advisor will provide advice and assist if required.

The appeal will result in the following:

- To uphold the Yellow Card sanction
- To withdraw the Yellow Card sanction.

The outcome of appeal panel's decision will be communicated in writing, be binding and final.

Appeals: Red Card Sanctions (Delete as appropriate)

The recipient of the Red Card Sanction is entitled to appeal against the decision in writing to the Chief Executive within fourteen working days of receipt of the notification.

On receipt of the request for appeal, the Chief Executive will nominate an appropriate Director to convene an Appeal Hearing. The Appeal Panel may consist of: two Executive Directors or; one Executive Director, and a clinical lead familiar with the patient and their care, and The Trust Security Advisor.

The author of the Red Card letter will be invited to present the 'Management case' including the presentation of any other evidence deemed relevant. They may also call on any witnesses deemed appropriate.

The alleged offender may then present the 'Defence case' and may bring a friend or family member to support them, but it is not entitled to be represented by a legal representative. The offender may call on any witnesses they choose specific to the event and may additionally include a witness as to their good character.

The Management and Defence parties will not be entitled to question each other directly, but questions to either side will be allowed through the Chair of the Panel.

The appeal panel may decide to:

- Uphold the Red Card Sanction;
- Withdraw the Red Card Sanction;
- Extend the offender's access to hospital care to include non-urgent care with conditions.

The outcome of appeal panel's decision will be communicated in writing, be binding and final.

Reviews of Warnings and Sanctions (Yellow and Red cards)

Six months after the date of the incident, an offender issued with a Yellow Card may request that the Trust reviews any restrictions placed on them. (Delete as appropriate)

An offender issued a Red Card Sanction may request a review twelve months after the date of the incident. The offender will need to demonstrate how his/her behaviour no longer presents a risk to Trust staff. (Delete as appropriate)

The review of restrictions will be undertaken by an Executive Director. This may involve a meeting with the offender and consideration of relevant evidence. The offender will be advised of the outcome of the review in writing and there will be no right of appeal. All paperwork relating to the review will be placed on the individual's health record where possible.

Appendix J

Template Letter: Letter to patient regarding marking of records due to relative's conduct

NHS
East Sussex Healthcare
NHS Trust

Private and Confidential

Hospital Number: **[Insert Hosp Number]**
NHS Number: **[Insert NHS Number]**

[Insert Patient's Name, Full address including postcode]

Date: **[Insert Date]**

Eastbourne District General Hospital
Kings Drive
Eastbourne
East Sussex
BN21 2UD
Direct Line Tel: 01323 41****
Email:****@nhs.net
Website: www.esht.nhs.uk

Datix No. **[Insert WEB*****]**

Dear **[Insert Name]**

I am informing you that as a result of an incident which occurred in **[insert ward/dept]** on **[insert date]** when you were accompanied by **[insert name of perpetrator]** whom we understand is your **[insert nature of relationship, e.g. spouse, partner, parent etc]**, **[insert name of perpetrator]** has been issued with a Yellow Card Warning/Red Card Sanction (delete as appropriate). Failure to comply with a Yellow Card may result in a Red Card Sanction being issued.

A Yellow Card warning is a first and final warning and does not affect access to the hospital or any treatment. A Red Card Sanction means:

- Access to this hospital is for EMERGENCY care only.
- There is no entitlement to attend outpatient appointments or undergo pre-planned procedures at this Trust.
- Entering Trust premises as a visitor is prohibited unless approved in advance in writing by the Trust.

In order to protect the safety of our staff in future, a copy of this letter will be placed on both yours and **[insert name of perpetrator]**'s electronic and paper health record, and will also be flagged to alert staff on the Patient Administration System. The fact that your records have been marked in no way reflects on your conduct or character; does not affect access to the hospital or any treatment in any way but is merely to alert staff of the potential risk of violence and aggression from **[insert name of perpetrator]** who may accompany you to the hospital in the future.

If you wish to appeal against this action, you are entitled to appeal to the Chief Executive, in writing, within fourteen working days of receipt of this letter. A copy of the appeals process is enclosed.

Yellow Card Warnings remain valid for 12 months from the date of issue. You may request this to be reviewed after 6 months provided no further similar incidents have occurred.
Red Card Sanctions remain valid for an indefinite period from the date of issue.

Whilst this action may seem unfair, I hope you will appreciate we have a duty to protect our staff and other patients from violence and aggression.

[Signature of authorising officer]

[Name of authorising officer]

[Role Title]

Enclosed: Appeals process

Appendix K

Security and Environmental Risk Assessment Template from Assure

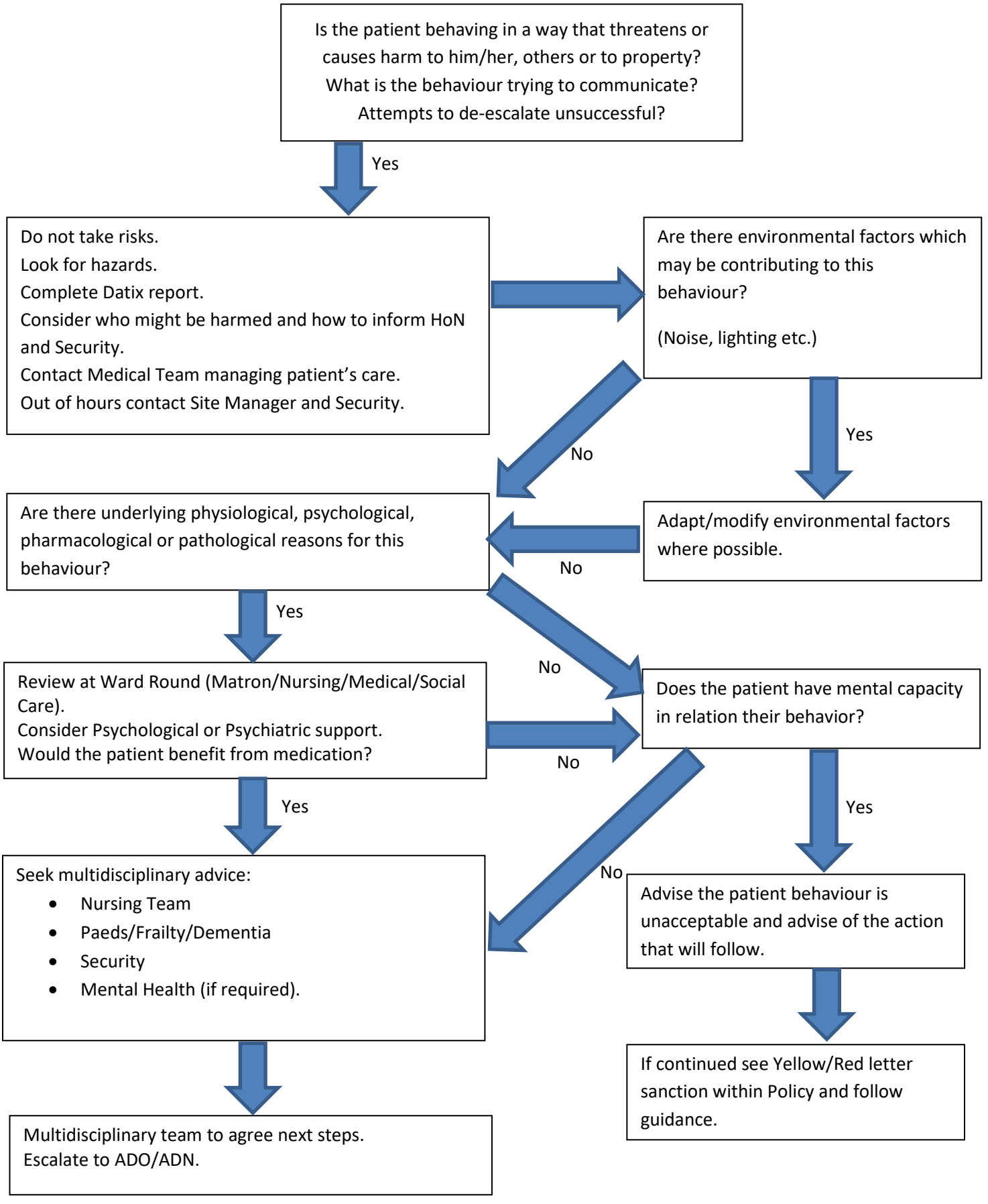
Security Checklist	
Area Security & Access Control	**Answer**
Are there existing access control systems for restricted areas?	
Do all staff have current and legible personal Trust (or SGUL) ID Badges & swipe cards?	
Are all staff aware of their responsibilities to prevent being followed into restricted areas (i.e. tail-gating)?	
Do staff routinely challenge individuals and request to see ID?	
Are staff aware of how to contact Security in an emergency?	
Do staff follow good procedure to prevent staff/patient habits affecting security (i.e. wedging self-closing doors open, leaving doors on the latch etc.?)	
Are keys properly controlled, limited in number and signed in and out?	
Are alarm systems, where fitted, adequate?	
If Yes – are these systems regularly tested?	
If Yes – if an alarm is sounded, are the reasons for sounding and subsequent actions recorded?	
Trust/Staff/Patient Property	**Answer**
Is there a local equipment inventory?	
If Yes – is this monitored and regularly updated?	
Are staff lockers available and in a secure location, i.e. staff changing room or office?	
Are staff routinely reminded to leave personal items and valuables, i.e. purse/wallet/handbag, in lockers or a secure area?	
Is the Patients' Monies & Property Procedure followed in regards to the storing and recording of patients' monies and valuables?	
Lone Working	**Answer**
Wherever possible, have tasks been designed to avoid them being undertaken alone?	
If tasks do have to be undertaken alone - has a Lone Worker Risk Assessment been completed on Assure?	
Are there any procedures in place to help ensure staff safety?	
Are there alarm systems in place by which staff can summon help in isolated areas, i.e. consulting rooms and cubicles?	
Are these alarms easily accessible to staff?	
Are the alarms easy to activate?	
Are staff trained in their use, including testing procedures?	
Do others know how to respond if the alarm is raised?	
Are there documented procedures in place for ensuring this?	
Can the alarm be heard in all areas of the ward/department?	
Security, Violence & Aggression	**Answer**

Are there systems in place to report Security or Violence and Aggression incidents?	
Have members of staff attended training appropriate to their role?	
Has a local Training Needs Analysis been completed, with the level of training and number of staff identified as requiring each level of training? E.g. Dementia training, Disengagement/Break-away training	
Are procedures in place to ensure that all members of staff have information and access to violence and aggression training as appropriate?	
Are security guards available when needed?	
Are staff aware of how to deliver a verbal and written warning to an abusive patient? Do they know the process to exclude a habitually abusive or aggressive patient?	
Are additional staff available when needed to provide 1:1 support for patients with Dementia/Mental Health/Other issues?	
Is there access to specialist mental health services where needed and an appointment for the patient?	
Have all staff (particularly those who are new and inexperienced) been made aware of the likelihood of abuse and what the local arrangements are for them to manage this safely?	
Are debriefs held with staff affected by violent or aggressive incidents; or a process in place for referral to Occupational Health and Wellbeing for more serious incidents?	
Environment	**Answer**
Have measures been taken to try and reduce (as far as possible) excessive noises which could cause distraction/distress etc.?	
Have any potentially isolated areas, i.e. treatment rooms or offices been identified and proportionate measures taken to reduce risk?	
Are these rooms laid out in such a way as to allow staff to exit in an emergency?	
Have measures been taken to ensure that an aggressor could not be situated between the employee and the door?	
Have any corridors/areas where aggressors could hide/congregate been identified and proportionate measures taken to reduce risk?	
Are there designated waiting areas?	
Are these adequately supervised?	
Is the lighting adequate?	
Is there adequate current information available to patients about the length of their wait and potential delays?	
Are the following readily available for patients in waiting areas: • **Toilets** • **Refreshments** • **Information services/points** • **Magazines** • **Television**	
Are all fixtures, fittings, furniture or equipment secure to prevent them being used as a weapon, as far as is reasonably possible?	
Are all the windows, skylights (or similar) in good working order, and can they be securely fastened?	
Is there adequate signage displaying the Trust's Zero Tolerance stance	

around Violence & Aggression?	
Are staff protected by additional security measures where required e.g. screens, security locks, intercoms, internal CCTV? This is of particular concern in 'hidden' areas.	
Are there any CCTV cameras recording the views of entrances, communal and/or access areas?	
Are there adequate parking spaces for staff and patients/visitors?	
Is there adequate lighting in and around the parking area?	
Is the car park reasonably close to the work area; or can staff move their vehicles closer?	
Policy & Procedures/Communication	**Answer**
Are all relevant Trust Policies and Procedures easily accessible to all staff? This should include (but not limited to) the following: • **Management of Security Policy** • **Violence & Aggression Policy** • **Physical Intervention/Restraint Policy** • **Health and Safety Management Lone Worker and Personal Safety Policy Arrangements** • **Patients' Monies & Property Procedure**	
Are relevant Trust Policies and Procedures discussed at staff meetings and huddles?	
Is Security reviewed at team/ departmental meetings on a regular basis?	
Is there a local departmental Policy/Procedure in place?	
If Yes – has this been reviewed within the past 12 months?	
Is the latest version of SecurityWise available to all staff?	

Appendix L

Violence & Aggression Flowchart



Appendix M

ESHT Guards Powers

Physical Restraint

- The contract security staff can restrain patients to both protect the patient and other staff from harm.

- The guards will require medical staff members present at all times during any restraint as the patient is under the care of East Sussex Healthcare NHS Trust and not that of a security company.

- The welfare of the patient and other staff members remain the responsibility of the Trust throughout the patients stay. All restraints are required to be at the minimal level to ensure the safety of the patent and all those in the immediate area. The patients' best interest will be paramount at all times.

Detention of Patients under DOLS/MH

- The Deprivation of Liberty Safeguards (DOLS) is being replaced with a scheme known as the Liberty Protection Safeguards for the future. For more information contact Sue Curties, Head of Safeguarding Acute and Community – Email: s.curties@nhs.net.

- All patients under any form of Mental Health detention remain the responsibility of East Sussex Healthcare Trust. The responsibility cannot be delegated to a third party contractor who will assist as best possible to insure the safety of all within the area the patient resides. Patients that are not under any section cannot be detained against their will by a security contractor all documents for the detainment are required to be in place prior to any intervention. A patient who 'might be' sectioned are insufficient grounds to reasonably detain them against their will. The guards will endeavour to use the powers of persuasion in the hope the patient complies with the wards request for them to stay

Powers of Search

- Only the Police have a power of search.

- The contract security staff does not hold any specific powers of search, they can attend a search that the Nursing Team are undertaking but normally only when the patient consents to the Nursing Team for this to be done. If the ward suspect the patient has items that are likely to be detrimental to the patient healthcare and treatment they can ask the local Police to support a search and give the Police the narrative as to why they suspect the patient is in possession of illegal substances.

- The contract security staff can ask both patients and visitors if they are in possession of any weapons and to surrender them to the staff. Any response from those asked cannot be taken as a statement of fact and as such all staff need to be mindful when interacting with those who are demonstrating erratic behaviour.

Patients who abscond

- The ward/department is responsible for all patients in their care while on NHS grounds. If it is felt by the ward/department that the patient is at 'risk of flight 'and they consider this to be detrimental to the patients wellbeing they might wish to consider allocating a 1-1 nurse to monitor the patient. Every patient who is not under DOLS or MHA needs to be risk assessed by medical personnel and an action plan put in place to safeguard the patient as best possible from 'risk of flight' If the patient leaves the 'footprint' of the grounds the contract security company have no means to retrieve them back onto NHS property. A missing patients protocol exists.

Nursing/Security Patient watch 1-1 cover

- The security contractor can only intervene when the patient under the care of East Sussex Healthcare Trust demonstrates either an attempt to self -harm or to injure other staff or patients.

- All 1-1 cover requires a Nursing presence during the period of patient care within the hospital. The security team is trained in managing Violence and Aggression and do not hold specific skills in interpreting the dialogue of those patients under the care of Mental Health. They cannot conversationally contribute towards the patients dependencies or mental health history as these are all matters that relate to the individuals overall medical care (the medical history is not known to the guards).

- They would however report anything which they interpret to be odd but as a Nurse is required to be present at all times during the cover the likelihood is quite low of this occurring. Please refer to the Policy for the Introduction and use of Enhanced Observations with Adult Patients.

- Initial set up would be a Registered Nurse or a Health Care Assistant or a final year Student Nurse who is deemed to be competent by the Registered Nurse in charge and be of the gender that the patient is most comfortable with.

- In extreme cases where there is evidence that the patient's behaviours/activities are a threat to other patients or staff, the short term use of security staff can be considered for the provision of supported observation with a nurse. These staff are to be supervised by a Registered Nurse.

    - Know the patient, their history, background and risk factors ;

    - Be familiar with the ward, the ward policy for emergency procedures and the potential risks within the environment;

    - The patient's views and needs should be taken into account when allocating an observer for older adults with cognitive impairments. Use of the 'This is Me' document is recommended.

The Nurse in Charge of the shift should create a roster of nurses and the times they will deliver enhanced observations.

Capacity, children, chronically ill – guidance to consider

Mental Capacity:

Patients who, in the judgement of an appropriate clinical professional, do not have the mental capacity to take responsibility for their actions will not be subject to the Warning or Red and Yellow Card Sanctions policy, eg an individual who becomes abusive as a result of an illness or injury, i.e. patients suffering from dementia or Alzheimer's.

The use of a Capacity Assessment Tool will assist on whether the patient has mental capacity.

The Trust recognises that in the interests of the patient and its staff, appropriate and effective steps must be taken to minimise the impact of such behaviour.

A clear management plan will be agreed with the patient's multi-disciplinary team to support the patient and provide a secure working environment for staff.

In order to minimise risk of harm to staff, the following steps should be undertaken:

- An appropriate care plan drawn up by senior members of staff identifying a strategy in minimising risk of harm to staff while ensuring continuity of care to the patient which includes care that might need to be delivered in the home.
- Issues to be addressed in the care plan should include some or all of the following:
  - Assigning specific members of staff to the patient
  - The provision of additional training to staff to help manage the patient's behaviour.
  - The provision of support and ongoing guidance to staff
  - The provision of additional support to the patient and to provide assistance in managing the patient's behaviour: psychologist, psychiatrist etc
  - Involvement of the Trust's security department and consideration for ward covers to support staff.
  - Regular review of the patient's mental capacity and the support and input from the relevant teams.

Children:

The Warning and Red and Yellow Card Sanction Policy will apply to violent/abusive patients who are 16 and over.

The Policy will also apply to patients aged 15 years of age and below in the event they are judged by health professionals to have reached a sufficient level of maturity and take responsibility for their actions (Gillick/Fraser Capacity)

CHRONICALLY ILL PATIENTS

A chronically ill patient is a patient who requires ongoing medical treatment and in the event that such treatment is withdrawn, will suffer serious harm or death.

An NHS Trust has a statutory duty to provide services to a patient who is in clinical need of that service.

Where a patient is being provided with treatment that is clinically required, the general position is

that treatment cannot be withdrawn. However, where a patient's behaviour is violent and abusive, there are circumstances where treatment can lawfully be withdrawn.

NHS Trusts have a legal duty to take reasonable steps to protect their staff from violent and abusive behaviour. This duty must be balanced against the need to provide healthcare to a patient where treatment is required.

East Sussex Healthcare NHS Trust

Management of Security Policy

Document ID Number:	827
Version:	V2
Ratified by:	Clinical Documentation and Policy Ratification Group
Date ratified:	13 September 2022
Name of author and title:	John Kirk, Facilities & Security Manager
Date originally written:	September 2006
Date current version was completed:	March 2022
Name of responsible committee/individual:	Chris Hodgson, Associate Director - Estates & Facilities
Date issued:	14 September 2022
Review date:	30 March 2025
Target audience:	All Staff
Compliance with CQC Fundamental Standard	Safeguarding service users from abuse and improper treatment (Regulation 13) Premises and Equipment (Regulation 15)
Compliance with any other external requirements (e.g. Information Governance)	Secretary of State Directives 2006 and 2007 NHSE/I Security Standards and Guidance
Associated Documents:	Violence and Aggression Policy ESHT Physical Intervention & Restraint Policy Patient Monies & Property Procedure Missing Patients Procedure Anti Fraud Policy

Version Control Table

Version number and issue number	Date	Author	Reason for Change	Description of Changes Made
V1 2006242	September 2006		New document	
V2 2008107	June 2008			
V3 2009155	August 2009			
V4 2010079	April 2010	John Kirk		Format, accountabilities and responsibilities
V1.0 2012124	June 2012	John Kirk	Policy review and format	Update to reflect new organisation
V1.1 2012173	August 2012	John Kirk	NHSLA advice	Additional information on annual security audit and proactive approach to risk assessment
V1.2 2012200	September 2012	John Kirk	Monitoring Table alterations	
V1.3 2015117	May 2015	John Kirk	Review	General review
V1.4	April 2018	John Kirk	Review	No changes to policy
V1.5	19 May 2021	John Kirk	Extension to review date due to Covid-19 pressures	Extended the review date from May 2021 to January 2022
V2	March 2022	John Kirk	Review	Reference to reviewed Violence & Aggression Policy, post HSE visit

Consultation Table

This document has been developed in consultation with the groups and/or individuals in this table:

Name of Individual or group	Title	Date
Facilities Board	All members	April 2015
Cross Site Security Group	All members	July 2022
Estates & Facilities Management Group	All members	July 2022

This information may be made available in alternative languages and formats, such as large print, upon request. Please contact the document author to discuss

Policy Summary Sheet
Management of Security Policy V2

This summary is a quick aide memoire and does not replace the requirement for staff to fully read the Trust Policies

MANAGEMENT OF SECURITY POLICY
KEY POINTS

- Security Manager 771481
- Security Advisor 771482
- Conquest Security Supervisor 734349 - EDGH Security Supervisor 735576
- Anti-Crime Specialist (Fraud) - see intranet for contact details

1	Contact Security in Emergency on ext 2222. Contact the Police via 999 in emergency or 101.
2	The Director of Finance is the Security Management Director.
3	The Trust Security Manager as Head of Service is the Local Security Management Specialist that provides specialist security advice to managers and staff and undertakes corporate security risk assessments.
5	All staff are responsible for security by maintaining a safe and secure environment for patients, staff, visitors and property against fraud, theft and damage.
6	All incidents of theft, damage, suspicious activity and trespass should be reported to Security and reported on the Trust's Incident Reporting System.
7	All staff must be in possession of their staff (swipe) ID badge and ensure that is worn and visible as appropriate whenever on Trust premises – challenge persons not wearing the badge if comfortable to do so – otherwise call Security for assistance.
8	All staff must be aware of members of the public 'tailgating' through secure Department/ward doors and should contact Security for assistance if required.
9	All staff should ensure the security of patient and personal property e.g. handbags, laptops, mobiles and do not take large amounts of cash or valuable/attractive items to work unnecessarily.
10	All staff should ensure that the Ward/Department is secured and alarmed (as appropriate) out of hours together with the safe issue and custody of keys.
11	All staff should be aware of any special security requirements relating to their place of work and the action to take in the event of a security incident.
12	All staff should undertake training relevant to this Policy e.g. Governance/risk management/health and safety & security training which forms part of the Trust's mandatory training programme. The Policy must form part of the local departmental Induction.
13	Staff should report building faults that may compromise security to Estates Helpdesk (Hospital based staff) or to the appropriate building landlord (Community based staff)
13	Clinical Unit must consult the Trust Security Adviser on the development of Operational Policies.
14	Clinical Units, Estates and Capital Projects staff should inform the Trust Security Adviser of any plans for new builds, refurbishment or re-configuration of Trust premises so that crime prevention measures can be designed in.
15	Managers are required to complete ward, department, or workplace security risk assessments and develop local workplace security procedures
16	Managers should inform the appropriate Governance Manager, Trust Security Adviser and Health and Safety Manager of any security risks.
17	Managers are responsible for ensuring that staff return name badges/swipe cards/PAC fobs, building/security keys, and uniforms on leaving Trust employment
18	Staff have an obligation to manage patient's property and follow CQC standards.

Table of Contents

Table of Contents

1. Introduction

The Trust follows Directives issued by the Secretary of State that clearly define security management work in the NHS. This is governed under the remit of NHSE/I.

As part of this service it is advisable that each NHS Trust has responsibility to employ a Security Management Specialist to provide professional skills and expertise to tackle security management issues across a generic range of proactive and reactive issues. The overall objective of the Security Management Service is to deliver an environment, which is safe and secure to patients, staff and visitors, so that the highest standard of clinical care can be achieved.

2. Purpose

2.2. Rationale

The Trust follows Directives issued by the Secretary of State that clearly define security management work in the NHS. Implementation and rollout were managed by NHS Protect and more recently NHSE/I.

2.2. Principles

- Protection of the personal safety of patients, staff, visitors and all others on the Trust premises is paramount
- The organisation will seek to protect Trust property and equipment against fraud, theft and damage.
- The protection of personal property of patients, staff, visitors and all others against theft and damage.
- That criminal activity is deterred and that there is an effective response to all security incidents.
- Incidents of crime and disorder are reported to the Police by the victim or security department.
- That the delivery of healthcare is uninterrupted, and provisions are made in respect of major incidents.
- The education and training of staff in proactive security and general security awareness.
- That staff are fully supported when reporting incidents of violence, fraud, theft or damage or other security related incidents.
- Creation of a pro-security culture
- Establishment of systems that deter crime
- Robust crime prevention measures
- Systems to support detection
- Clear methods of Investigation
- Effective set of sanctions that can be applied
- Seek redress against offenders

2.2. Scope

This policy applies to all premises and assets owned by East Sussex Healthcare NHS Trust and all staff. Where there are Trust staff resident in premises owned/managed by others, the relevant manager should seek assurance as to the robust nature of the landlord's security policy and procedures. With assistance from the Trust Security Adviser.

3. Definitions

LSMS
Local Security Management Specialist; accredited security professional

ACS
Anti-crime Specialist; accredited fraud specialist

NED
Non-Executive Director (a nominated voting member of the Board)

NHSE/I
National body, responsible for security within the NHS

CTSA
Counter Terror Security Adviser

Risk
Is defined as the 'potential for unwanted outcome', or 'the possibility of incurring misfortune or loss', which may be in relation to people, buildings, environment, equipment, systems, management, finance, and Trust's reputation.

SMD
Security Management Director (a nominated voting executive member of the Board)

Security Risk Management
Is a systematic method of identifying, analysing and evaluating the risks associated with the activities of the organisation. It is a proactive approach which addresses the various activities of the organisation. It seeks to identify the risks, assess for potential frequency, severity and to reduce the effect of the risks that cannot be eliminated.

4. Accountabilities and Responsibilities

4.1 The Trust Board

Accountable for the provision of security within the Trust which provides safeguards to protect patients, staff and visitors, their property and belongings and for providing resources for the effective management of security risks and loss prevention.

The Board holds corporate responsibility for the implementation of security management within the Trust, and for the appointment of a Non-Executive Director and Security Management Director to support security within the hospital.

4.2 Non-Executive Director (NED)

The requirement for an NED at each NHS body is set out in Secretary of State Directions to NHS Bodies on Security Management Measures 2004 (amended 2006). The NED

must be nominated from a trust's non-executive directors or a body's non-officer members.

The role of the NED is to support and, where appropriate, challenge the SMD on issues relating to security management at Executive Board level.

4.3 The Security Management Director (SMD)

As provided by the legal framework documents, the SMD must be voting executive director, or in the case of an NHS body other than a trust, from the officer members.

Ultimately it is the responsibility of the nominated SMD, along with the Chief Executive, to ensure that adequate security management provision is made within their NHS health body, as specified particularly in paragraphs 2 and 7 of the Secretary of State Directions 2004. This is regardless of whether or not the LSMS and/or security staff are directly employed by the health body or provided by an external contractor.

4.4 The Associate Director, Estates & Facilities

The above is the named executive for the implementation of the Trust's operational security needs.

4.5 Local Security Management Specialist (LSMS)

Is the responsible person for the implementation of the Trust Security Policy.

The LSMS shall be responsible for carrying out full investigations under the Police and Criminal Evidence Act and taking appropriate action with the Police Prosecution Service/Legal Protection Service within the Counter Fraud and Security Management Service.

Shall review risk assessments and security incidents to identify trends / hot spots and develop a Trust wide Action Plan where necessary to address issues raised.

4.6 Divisional Leads and Line Managers

- Implement the Trust's security procedures and will ensure that appropriate security training is provided in their areas of responsibility.
- Fully understand the Violence & Aggression Policy and how to apply sanctions
- Will ensure that, as far as is reasonably practicable, security and the safety of patients, visitors, and staff are reflected in all appropriate departmental procedures. Such procedures will require regular monitoring, review and updating as necessary.
- Seek advice from the Security Advisor of any changes with regard to their Department that affects the security of the premises.
- Ensure that staff within their Department wear the Trust Photo-ID Badges at all times.
- Ensure that staff within their Department are instructed to only allow authorised persons to enter staff only areas and, where it is safe to do so, challenge and prevent entry of all unauthorised persons. In circumstances where this action would put staff at risk, they should call security immediately or through Switchboard on extension 2222 to validate identity
- Record details i.e. make, type, serial number etc. of all valuable or otherwise important property within their Department and to ensure that these items are clearly security marked and where possible secured and protected against theft or malicious damage.
- Keep a record of all keys issued to staff in their Department and reporting all losses of keys to the Security Department.
- Ensure that arrangements are made to secure the Department out of working hours and the safe custody of keys.

- Ensure that any security alarm or device to protect the department out of hours are set and regularly tested.
- Ensure Managers are completing security risk assessments in line with Trust Policy
- Provide each employee with information, instruction and training as necessary to ensure the safety of themselves and others from the security risks associated with the activities they are employed to undertake. Ensure that staff are fully supported when completing Incident reports concerning fraud, violence, theft and damage or other security related incidents.
- Ensure that appropriate action is taken in respect of persons who are suspected of committing a criminal offence, misconduct, or other breaches of security in contravention to these procedures by contacting the Local Security Management Specialist.
- Advise the Security LSMS of any Police attendance
- They will also inform the Director of Finance who will involve the ACS if fraud is suspected. The ACS may also be engaged direct.

4.7 Security Department

The principle operational duties of Security staff are:

- Conflict Resolution and Management
- Attending emergency calls
- Investigation of incidents
- Patrolling of buildings and the site
- Production of ID badges
- Operation of CCTV equipment and access control of the various sites
- Security surveys
- Prevention and or deterrence
- Sanctions and redress
- Review of risk assessments

Guards receive control and restraint training which will include up-skilling to provide a better understanding when dealing with patients with a disability, capacity issues, dementia, etc.

See Appendix A for full contact details and how to report crime

4.8 Trust Staff and Nursing Staff

- Will follow the current Patient Monies & Property Procedure, logging details of patient's property and safeguarding valuables. This includes advising the Trust Safeguarding Lead of any reports of theft.
- Responsible for not only safeguarding their own wellbeing and property, but also that of patients and visitors to the Trust
- Will be responsible for promoting and maintaining security at all times by being involved in crime prevention and security measures, anticipating risks and taking action to remove, reduce or transfer them and receive training as provided by the Trust on these issues. All staff must be fully aware of this Policy.
- Be aware of the security needs of the Trust and be familiar with the specific aspects of all security procedures which affect their own area of work.
- Report all incidents of criminal activity including assaults, theft, fraud and criminal damage including those incidents to be of a suspicious nature to their appropriate Supervisor, Ward Manager who will inform the Security

Management Specialist. An incident form must be completed at all times. Lost medicines should also be reported to Pharmacy
- Be fully conversant with the methods and procedures for contacting Security Staff.
- Wear the Trust ID badge at all times and report the loss of the ID Badge tothe Security Department immediately.
- Report the loss of any Departmental keys to Security Department immediately.
- Will follow the Missing Patients Procedure and the Violence and Aggression Policy ESHT

4.9 Cross Site Security Group

The Cross Site Security Group meets four times a year and they will monitor the measures to improve security related incidents brought to its attention, as well as implementation of the policy and the proactive Trust wide risk assessment. An action plan will then be produced and monitored.

4.10 Safeguarding Lead

Will review any incidents with safeguarding concerns and raise them with Adult Social Care or Security as appropriate.

4.11 Violence & Aggression Group

The Group meets bi-monthly and is led by the Violence and Prevention Lead.

5 Working in Partnership with Sussex Police

The Trust maintains a professional relationship with the local Police.

In the event of a member of staff reporting a security incident the telephone number for non-emergency response is 101. For emergency response dial 999.

When staff are completing incident forms and there has been a Police response the following details must always be recorded in order that the Security Advisor can contact the relevant Police Officer when carrying out further investigations.

- Reference number or crime number
- The name of the Officer

6 Procedures and Actions to Follow

6.1 The Assessment of Security Related Issues

Security is a necessary part of managing the Trust's business. It needs to address both internal and external threats. Poorly managed, it will be seen as an obstruction by both management and staff to the normal and necessary conduct of business. Security should be subject to a risk assessment exercise to ensure that the measures taken are proportionate to the risks to the organisation.

Security involves the protection of all assets of the Trust, not just physical assets. It includes the protection for staff, equipment and premises. The response to the perceived risks will be a combination of procedural, physical, manual and electronic measures. The Risk Management Policy & Procedure should be followed.

It is the Departmental manager's responsibility to carry out risk assessments annually or more frequently in the event of an incident occurring. These should be undertaken with the support of the Security Manager/Advisor, and in conjunction with the staff in the department to ensure that all potential and actual risks are captured, and review them annually.

When conducting a security risk assessment managers should consider issues such as:

- Ease of access to authorised areas by unauthorised people
- Security of Trust, patient and staff property
- Security of medical records

- Lone working
- Ease of access to controlled drugs and other pharmaceutical items
- Safety of staff who collect count, handle and transport money
- Baby/infant abduction and child safety
- Reducing the risks of vulnerable patients from absconding
- Criminal damage to staff or patient property

As with any risk assessment the emphasis should be to:

- Identify the risk
- Avoid the risk
- Reduce/mitigate the risk
- Control the risk

Security Incidents are logged onto the Trust risk and incident reporting database (Datix). The Local Security Management Specialist will review information with regard to all security related incidents reported. This information, along with completed risk assessments will be used to highlight areas for concern, which will be included on a Trust wide risk assessment with an associated action plan

The LSMS will:

- Complete a written report which will be presented to the Health and Safety Steering Group and the Audit Committee or Trust Board annually.
- Ensure that the Trust's Corporate Risk Register is continuously updated with any trust wide security risks which are graded 15 and above.

6.1 Violence and Aggression Risk Assessment

The Violence and Aggression Policy should be referred to. Staff can be exposed to the risk of violence and aggression whilst at work. Those at risk can be identified from the following:

- All Medical, Nursing, Security, Parking, Ward Clerk's etc
- Work location e.g. mental health unit
- Lone working role
- Particular aspects of the job e.g. cash handling/till operation, community visits
- Trend analysis based on incidents

If a staff member or group are potentially at risk, the Departmental Manager must undertake a risk assessment. This must fully:

- Identify and assess the risk
- Identify existing control measures
- Confirm an action plan
- Put in place a programme to deliver the action plan,
- Monitor
- Review

The assessment must be recorded on Assure and held locally so that all staff have clear and unrestricted access. It must also be managed, controlled and reviewed through the department's regular governance/risk meetings. Any unresolved actions must be presented to the Trust's Health & Safety Committee for resolution. The security team will assist by providing specialist advice, departmental surveys, staff personal attack alarms, and training.

Conflict resolution training (CRT) (see policy Section 8) is mandatory for all front line staff that may be at risk from violence or aggression. Certain staff groups will automatically receive training e.g. nursing, medical, porters, ward clerks, receptionists, security. Compliance on mandatory CRT is reported to the H&S Steering Group as a key performance indicator.

Breakaway training is provided for front line wards and departments once the risk has been assessed.

6.2 Use of Trust Property

It is an offence for members of staff to remove property belonging to the Trust without written authority. Failure to seek authority from line management could result in disciplinary action or criminal proceedings being taken. Staff must take all reasonable steps to safeguard Trust property whilst in their care.

6.3 Security Marking of Trust Property

All valuable and attractive items of equipment i.e. IT Equipment, televisions, videos etc must be security marked by the local Department with advice from the LSMS if required. This has a deterrent factor and will assist in the identification following loss or theft.

6.4 Patients Property

- Each Ward/Department will follow the Trust procedure regarding the security of patient's personal property.
- On admission the patient must be asked if they wish to have their valuables/money secured. If they choose to retain valuables or money on their person during their stay, a disclaimer notice to that effect must be signed by the patient. In the event of a patient being confused and unable to exercise rational Patient Monies & Property Procedure
- If the patient is transferred between Wards the property list must be checked each time to ensure consistency and to ensure that if a theft takes place an investigation can be completed thoroughly by Security Personnel who will
- ascertain when the theft took place i.e. date, time. (See Patient Monies & Property Procedure

6.5 Staff Property

- The Trust does not accept responsibility for the loss or damage to personal property including motor vehicles and cycles whilst at work. Staff are further advised to take adequate precautions to ensure the safety of their possessions and not to bring valuables to work if at all possible.
- Where a locker is provided for personal use, the individual will be responsible for providing a suitable locking device.
- Staff must report any loss or damage to their belongings and co-operate in any subsequent enquiry carried out either by Security or Police.
- Staff required to provide and use their own equipment should discuss the need for adequate facilities with their manager and advice can also be sought from the Security Manager

6.6 Lost & Found Property

- All found property must be handed over to the site Security Guard for safekeeping, registration and disposal.
- Community hospitals should have a local arrangement for recording found property and an audit trail. Items reported lost should also be recorded.

6.7 Key Security

The following principles provide adequate control over keys:

- Departmental keys should be held in a lockable key case and a record maintained of the issue and return of the keys.
- No extra keys should be cut which belong to the Trust.
- In the event of lost/stolen keys they should be reported immediately to the Security Department and the Estates Department immediately.
- No master or sub-master key should be left unattended and should be booked in/out from the site Porters Lodge. Local sites to have a similar arrangement usually controlled by the reception desk or site manager

6.8 Use/Misuse of Telephones

The Trust has a separate policy on the use of the Trust's telephone system and for making private calls. The misuse of Trust telephones is considered as an act of fraud and will lead to disciplinary action and possible prosecution.

6.9 Fraud

- The Trust's Standing Financial Instructions shall be strictly followed at all times.
- Any allegations of fraud should be reported to the ACS to counter fraud and corruption.
- All allegations of fraud are taken seriously, and the Trust is committed to reducing the effect of fraud on its finances. The Trust have adopted the NHSCFA approach to pursuing criminal, civil, disciplinary and regulatory standards in cases of fraud, bribery and corruption. All options may be considered and pursued when and where appropriate.
- See the Anti Fraud, Bribery and Corruption Policy

6.10 Communication of Security Issues

Issues relating to Security within the Trust will be communicated through training, Core Brief, Securitywise and on the Security Website on the Trust Intranet.

6.11 Release of Information

The Security department will adhere to all Information, Governance and Data Procedures and Policies before the release of information to the Police and the Media. Any requests should be directed to the relevant Department.

Staff must avoid unwittingly providing visitors/general public with information likely to bring discredit to the Trust.

6.12 Purchase of Security Systems

Security systems e.g. access control systems (including video/intercom systems/swipe/proximity card readers), CCTV and intruder alarms must not be purchased by Divisions/Departments without prior consultation and approval of the Security Management Specialist.

This will ensure compatibility of the system with the Trust's existing systems and that other statutory regulations and guidance are complied with.

6.13 Staff Identification

The Trust staff badges have the following purposes:

- The ability for patients to identify the bona fide staff members
- The ability for staff to distinguish between staff and patients and visitors
- A clear basis for staff to challenge people requiring access to sensitive areas within the site
- It allows staff entry into restricted areas
- It allows access by staff into authorised staff parking areas
- It allows a degree of protection for staff when handing over keys, money, patient property or sensitive documents.

All members of staff and volunteers working within the Trust are required to wear a staff ID badge whilst on duty. The badge is to be worn in a position so that the public, patients and other staff members can see it, unless medical or operational situations prevent this.

7 Equality and Human Rights Statement

The Trust recognises the diversity of the local community and those in its employment. Our aim is, therefore, to provide a safe environment free from discrimination and a place where all individuals are treated fairly, with dignity and appropriately to their need. The Trust recognises that equality impacts on all aspects of its day-to-day operations and has produced an Equality Policy Statement to reflect this. All policies are assessed in accordance with the Equality Impact Assessment Toolkit, the results for which are monitored centrally. The EHRA analysis does not indicate any issues which need to be addressed with the implementation of this policy. A copy of this assessment which is Trust wide is held by the Security Manager.

8 Training

The Trust acknowledges the need for effective training of staff to deal with security-related issues and violence. Training and advice on all security matters including violence will be provided to all new employees at the local induction.

The Trust provides Conflict Resolution for front line staff with a refresher every three years. Breakaway training is also available for front line areas. In addition a Personal Safety Course is also available

The local Police Counter Terror Officer delivers terrorism awareness sessions for staff every year – this is open to all

Training is recorded on the Electronic Staff Record held within Workforce. The process for monitoring compliance with training is undertaken in line with the reporting process contained within the Mandatory Training Policy.

9 Training & Awareness

The Trust Security Adviser and Local Security Manager are trained and accredited as LSMS to carry out their duties in accordance with this policy. They will attend other training, conferences, seminars as and when deemed necessary to enable them to carry out their duties efficiently and effectively as required by Secretary of State Directions.

The Local Security Manager is responsible for ensuring security officers are at all times properly and adequately notified, trained and instructed (including if reasonably practicable by way of continuing professional development) to a level commensurate with the task that has to be performed.

10 Developing a Pro-Security Culture

- Security awareness and management is included at the local induction process.
- Divisional Governance Meetings are used as a conduit
- Security publication “Securitywise” is issued quarterly to all staff
- Cross Site Security Meeting is held quarterly and attended by all divisions
- Datix – all security incidents including violence, aggression and abuse are reviewed and any learning identified
- Bespoke training is delivered
- Crime investigation – security supervisors will present outcome at a local level to help with learning

10.1 Applying Sanctions

Zero tolerance is applied though each case is reviewed with regards to intent and capacity and reference should be made to the Violence & Aggression Policy. A two stage sanction is employed

10.2 Risk Assessments

These should be managed and retained locally.

11 Monitoring Compliance with the Document

Please see table on next page

Document Monitoring Table

Element to be monitored	Lead	Tool	Frequency	Reporting Arrangements	Acting on recommendations and Lead(s)	Ensure lessons are shared & actions completed
How the organisation manages security	LSMS	Review of risk assessments, action plans, risk registers, presented to the Cross Site Security Group Annual report will be presented to the Health and Safety Steering Group and Audit Committee	Quarterly Annually	Cross Site Security Group. Audit Committee and H&S Steering Group via the Annual report	Security Management Director, LSMS, Divisional Governance Managers	Changes in practice will be shared with the Security Group and recommendations and changes implemented by the appropriate division or security department
Crime levels	Security Manager	Datix Information	Quarterly	Cross-Site Security Group	Security Manager and Divisional Managers	Cross-Site Security Group
Risk Assessment	Divisional Manager Governance Manager	Divisional Governance Procedures	Quarterly	Department H&S Group and Cross-Site Security Group	Departmental heads and Divisional Governance Manager	
Department Security Procedures	Divisional Manager Governance Manager	Report	Quarterly	Divisional H&S Group and Cross-Site Security Group	Department H&S Group and Divisional Governance Manager	
Assaults	Divisional Manager	Datix	Weekly	Divisional and Trust H&S Groups National database	Divisional t Managers and LSMS	

12 Review

The policy has been developed in the light of currently available information, guidance and legislation that may be subject to review. Notwithstanding, this Policy will be reviewed after 3 years.

13 Reference Documents & Bibliography

The following are important references, although by no means an exhaustive list, in relation to this policy

National agreements with the NHS

- Memorandum of Understanding with Association of Chief of Police Officers
- Memorandum of understanding with Crown Prosecution Service
- Concordat with Health and Safety Executive
- Concordat with the National Offender Management Service and CFSMS
- Internal Memorandum of Understanding with the NHS Counter Fraud Service
- Internal Memorandum of Understanding with the Human Resources Department

Care Quality Commission:

- Regulation 7 – Safeguarding People Who Use services from Abuse.
- Regulation 9 - Management of Medicines
- Regulation 10. - Safety and Suitability of Premises.

Department of Health, *Secretary of State Directions to NHS bodies on measures to deal with violence against NHS staff* (November 2003). Also see amended Directions (2006).

Department of Health, *Secretary of State Directions to NHS bodies on security management measures.* (April 2004). Also see amended Directions (2006).

NHS Security Management Manual. Web-based manual. Restricted access.

NHS Counter Fraud and Security Management Service, *A Professional Approach to Managing Security in the NHS* (December 2003).

NHS Counter Fraud and Security Management Service, *Non-Physical Assault Explanatory Notes* (November 2004).

NHS Counter Fraud and Security Management Service, *Tackling Violence against Staff. Explanatory notes for reporting procedures introduced by Secretary of State Directions in November 2003* (January 2007).

NHS Counter Fraud and Security Management Service, *Not Alone – A Guide for the Better Protection of Lone Workers in the NHS* (March 2005).
NHS Counter Fraud and Security Management Service, *Conflict Resolution Training Implementing the National Syllabus* (2004)

The Management of Health and Safety at Work Regulations (1999)

The Health and Safety at Work Act (1974)

.

Secured by Design (Hospitals). Association of Chief Police Officers (ACPO). April 2005

ACPO – 'Safer Car Parks'.

All currently valid Health Technical Memoranda (HTMs) and Health Building Notes (HBNs) published by the Department of Health.

CABE/Design Council – Reducing Violence and Aggression in A&E Departments.

14 Associated Documentation

The Security Policy should be read in conjunction with the Health & Safety at Work Policy and the Fire Safety Policy. These policies will act as enabling documents for the production of a series of risk management / health & safety / fire safety procedures and other relevant documents.

Trust Safety Procedures which support this Policy are:-

- Workplace Health Safety & Welfare Arrangements Policy
- Health & Safety at Work Policy
- Medicines Policy
- Security of Newborns
- Abduction - under 16
- Lone Worker & Personal Safety Arrangements
- Counter Fraud Policy
- Missing Patients Procedure
- Risk Management Policy

Appendix A: Contact Information for Security Department

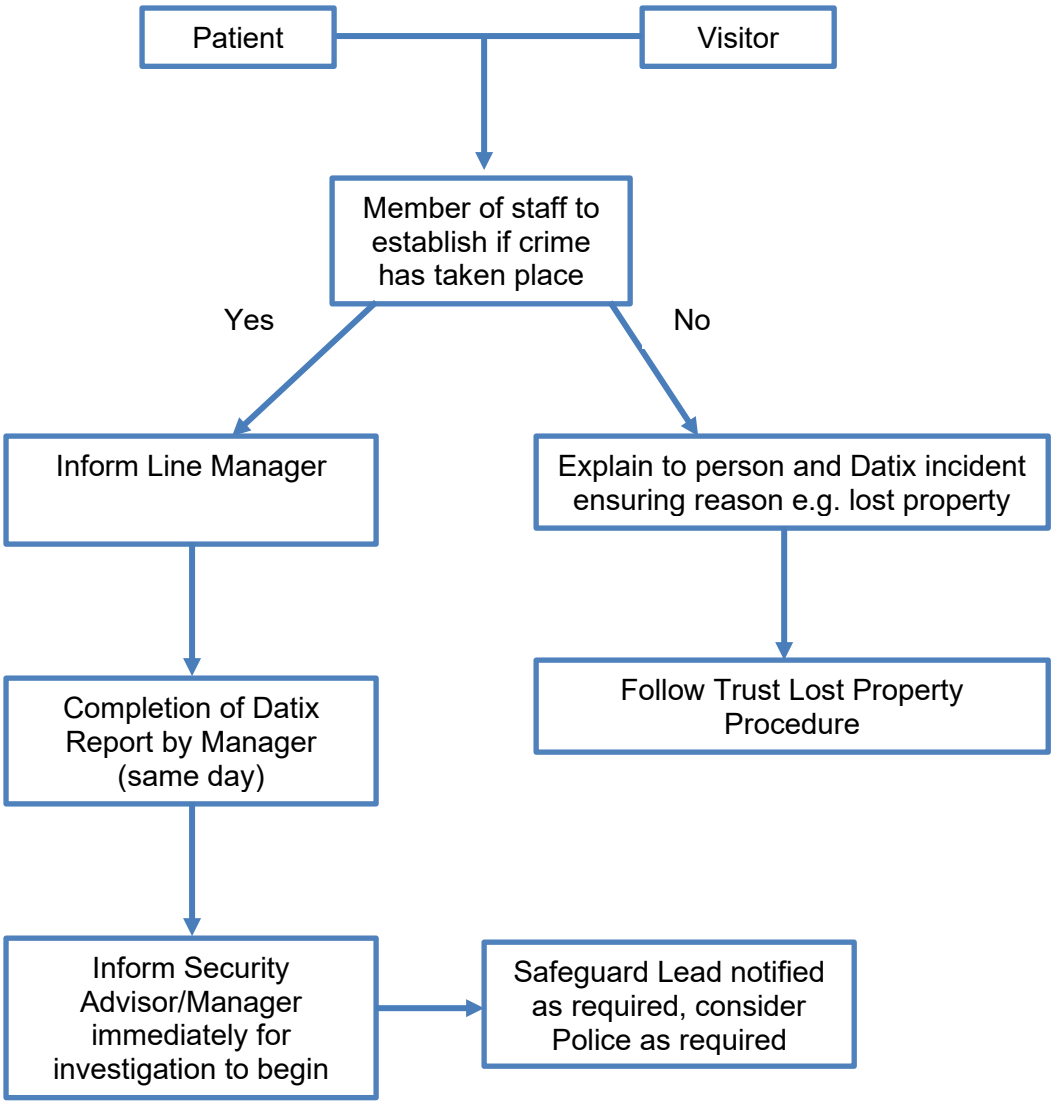
The Security Service can be contacted by phone or pager through Switchboard on the following numbers:

▪ Security Manager	Phone	771481
▪ Security Advisor	Phone	07812 461562
▪ DGH Security (24 hours)	Bleep	0739
▪ Conquest Security (24 hours)	Bleep	2603
▪ Security ID/Access control DGH	Phone	735576
▪ Security ID/Access control Con	Phone	734349

The Security Service will respond in the first instance to all security incidents.

The emergency number for the Police and all emergency services is 999 (112 Mobile).
Non- emergency is 101.

Reporting Incident of Crime NHS



Appendix B: Identification Badges

The Trust staff ID badges have the following purposes:

- The ability for patients to identify the bona fides staff members
- The ability for staff to distinguish between staff and patients and visitors
- A clear basis for staff to challenge people requiring access to sensitive areas within the site
- It allows staff entry into restricted areas
- It allows access by staff into authorised staff parking areas
- It allows a degree of protection for staff when handing over keys, money, patient property or sensitive documents.

The ID badge also allows staff members' access into the staff car parks and certain areas of the Trust buildings. If this access is required then staff members when approaching the barrier/door are to pass the badge through the reader located to the side of the barriers or door. Once the badge has been through the reader, a record is created and the barrier arm will rise or door open. Exit from most controlled doors can be obtained by pressing the exit button located at the side of the door.

Procedures to follow:

Listed below are instructions relating to the most obvious questions:

How to get an ID Badge
All new staff members are to complete the ID badge request paperwork available from their place of work or the security office. This completed paperwork must include the signature of the appropriate manager. The staff member shall then report to the Security Office with the completed request and an ID badge will be produced. This service is available Monday to Friday from 0900 at the Conquest and DGH ID office.

What to do if a badge is lost/stolen
Report the loss to the Manager of the Department and the Security Office. A replacement badge will then be issued at the discretion of the Security Office.

What happens when staff leave
It is the responsibility of the line manager to ensure that the ID Badge is returned to the Security Office

Temporary ID Badges
A temporary ID Badge can be obtained from the Security Office for personnel working within the Trust. Requests for temporary ID are to be e-mailed or a memo sent by the relevant line manager to the Security Office. Staff should note that a temporary ID Badge may not allow the bearer access through some restricted area readers.

ID
All contractors working within the Trust receive work permits and if necessary ID from the Estates and Facilities Department.

Appendix C: Department Guidance on Security Risk Procedures and Assessments

DEPARTMENT GUIDANCE ON SECURITY RISK PROCEDURES AND ASSESSMENTS

GUIDANCE - FACTORS TO CONSIDER AND INCLUDE

The following guidance provides a list of factors that should be considered when producing a local security procedure for your department, ward or work area.

Once completed, the document should be displayed in a staff area and all staff made aware of it. CQC Auditors may question staff on its contents.

The list is not exhaustive as each department, ward or work area will have its own unique issues to consider. However, this guidance should assist authors in the preparation of local security procedures. Further guidance can be obtained from this Policy in the first instance or the Trust's Security Manager or Advisor.

Security related risk assessments are a **MANDATORY** requirement for each separate department, ward or work area If areas of risk are identified concerning physical security, lone working or violence and aggression, the Trust's risk assessment process is to be followed and control measures put in place – templates for risk assessments.

Completed local procedures and all security related risk assessments/local action plans identified above are to be E mailed to the Trust Security Adviser and Local Security Management Specialist (LSMS) for monitoring and CNST purposes.

The following factors should be considered and included as appropriate.

1. REPORTING SECURITY INCIDENTS:

a. Who do staff call? (see contact details- Appendix A)
b. How are incidents reported and to whom should they be sent? (Incident Report to be completed in a timely manner)

2. SECURITY ADVICE

a. Who can provide advice and support for any security issue? (see contact details- Appendix A)

3. SECURITY RELATED POLICIES AND RISK ASSESSMENTS

a. Mention should be made of the Trust's Security, Lone Worker, and Management of Violence & Aggression policies as well as the Policy and Procedure for the Use of Control and Restraint Techniques as appropriate and where they can be found in the Dept / Trust Intranet.

4. PHYSICAL SECURITY:

Outline that all staff are responsible for reporting faults with doors, windows, alarms, windows, video/intercoms etc., to Estates on the Estates Helpdesk 770553.

a. Department doors

- Who is responsible for locking/unlocking them?
- Can they be locked effectively?
- What time are they locked / unlocked?
- Are the locking devices in a good state of repair?
- What precautions are taken to reduce the chance of tailgaters gaining access?
- What action to be taken to prevent a patient lacking mental capacity from leaving (Deprivation of Liberty Safeguards)?

b. Keys / Fobs

- What procedure is in place to control the use of keys / fobs and record kept of who has which keys / fobs?
- What procedure is to be followed in the event of lost keys / fobs?
- Who issues fobs and manages local fob system?

c. Windows

- What condition are the windows in?
- Who is responsible for locking / securing them?
- Can they be secured effectively?

d. Alarms

- What is the alarm for?
- Where are the alarms situated?
- Who responds if they are activated?
- How often are they tested?
- Who are the key holders for out of hours access?
- Who maintains the alarm?
- Who is responsible for activating/de-activating the alarm, how and at what time is this undertaken?

e. Staff Property

- Do staff have any lockers supplied with locks or areas which are secure for storing valuable items?
- What locations are provided?
- What rules are in place to ensure staff lock valuables away?
- Advice on what to bring into work should be clarified e.g. as little as possible.

f. Patient Property

- What is the procedure for booking in /out and securing patient property while in the Dept?
- Reference should be made to the patient property policy.

g. Departmental Property

- What are the procedures for locking / securing departmental equipment / property?
- Is departmental property security marked? How?
- What accounting procedures are in place for attractive property items? Property registers? Who is responsible?
- Are patients required to sign in/out Departmental property on loan?

h. Controlled Substances and Prescription Forms

- What procedure is in place for the security and accounting of controlled substances and prescription forms?

5. POTENTIAL FOR VIOLENCE, ABUSE AND AGGRESSION:

a. Front line staff to be identified and mandatory Conflict Resolution Training attended; staff in higher risk areas should receive breakaway training.
b. What factors in the department could cause visitors to become abusive e.g. lack of communication, excessive waiting times etc.
c. Mention should be made of the Trust Management of Violence and Aggression Policy and where staff can access it
d. What hazards exist in the department that could have an impact on violent or abusive behaviour? Has a departmental work area violence and aggression risk assessment been undertaken? What control measures are in place?
e. What is the process for reviewing and documenting amendments to a violent or aggressive patient's care plan? This must include undertaking a violent patient risk assessment.
f. Do you have any Lone Workers? Have risk assessments been completed if identified and local procedures/communications plans produced for their protection?

6. VISITORS:

a. How are visitors (public or staff) monitored and their access restricted through controlled doors?
b. How many visitors per bedside? Are there signs for this?
c. Are visitors signed in and out?
d. Is there a nurse base/reception area for visitors to be directed to?

7. STAFF:

a. Staff to wear ID badges at all times (reference to be made to Trust Security Policy)
b. Staff to be encouraged to challenge staff not displaying ID badges/ members of the public seen wandering around

8. IT PROTECTION, MEDICAL RECORDS AND CONFIDENTIALITY:

a. What procedures are in place to ensure the security and confidentiality of patient information?
b. How is patient information handled, stored and destroyed?
c. Are computers secured to desks/walls and is viewing by the public prevented? (See Information Systems Security Policy)

9. UNIDENTIFIED PACKAGES / BOMB THREATS:

a. Identify the action to be taken. Reference to be made to the Trust Major Incident Policy

10. MISSING PATIENTS:

a. Identify the action to be taken. Reference to be made to the Trust Missing Patients Policy

Appendix D: Due Regard, Equality & Human Rights Analysis

Due Regard, Equality & Human Rights Analysis

Title of document: Management of Security Policy
Who will be affected by this work? E.g. staff, patients, service users, partner organisations etc. All the above.
Please include a brief summary of intended outcome: To provide a clear policy and procedure for the management of security and to support integration and not to discriminate.

		Yes/No	Comments, Evidence & Link to main content
1.	**Does the work affect one group less or more favourably than another on the basis of:** (Ensure you comment on any affected characteristic and link to main policy with page/paragraph number)		
	• Age	No	
	• Disability (including carers)	No	
	• Race	No	
	• Religion & Belief	No	
	• Gender	No	
	• Sexual Orientation (LGBT)	No	
	• Pregnancy & Maternity	No	
	• Marriage & Civil Partnership	No	
	• Gender Reassignment	No	
	• Other Identified Groups	No	
2.	**Is there any evidence that some groups are affected differently and what is/are the evidence source(s)?**	No	
3.	**What are the impacts and alternatives of implementing / not implementing the work / policy?**	Clear guidance is essential as it would impact on reputation and safety	
4.	**Please evidence how this work / policy seeks to "eliminate unlawful discrimination, harassment and victimisation" as per the Equality Act 2010?**	All security staff are trained/accredited and licensed. Training includes recognition of characteristics, how to raise concerns, and how to relate and understand all. Trust values apply and all staff undertake mandatory training for equality and diversity.	
5.	**Please evidence how this work / policy seeks to "advance equality of opportunity between people sharing a protected characteristic and those who do not" as per the Equality Act 2010?**	The Policy seeks to meet the needs of all our users.	

6.	**Please evidence how this work / policy will "Foster good relations between people sharing a protected characteristic and those who do not" as per the Equality Act 2010?**	The Policy seeks to meet the needs of all our users.
7.	**Has the policy/guidance been assessed in terms of Human Rights to ensure service users, carers and staff are treated in line with the FREDA principles (fairness, respect, equality, dignity and autonomy)**	Yes
8.	**Please evidence how have you engaged stakeholders with an interest in protected characteristics in gathering evidence or testing the evidence available?**	Estates & Facilities Group 2022 Working Policy Group 2021 Policy Ratification Group 2021 These groups have considered the needs of protected characteristics
9.	**Have you have identified any negative impacts or inequalities on any protected characteristic and others? (Please attach evidence and plan of action ensure this negative impact / inequality is being monitored and addressed).**	None have been identified.