Reference Number: UHB 037 Version Number: 4 Date of Next Review: 09 APR 2022 Previous Trust/LHB Reference Number:

SECURITY SERVICES POLICY

Policy Statement

The Security Services Policy of the Cardiff and Vale University Health Board (UHB) sets out the security arrangements which are to be implemented in all areas of Cardiff and Vale UHB.

Security in Cardiff and Vale UHB is concerned with the provision of safeguards to protect the safety of those who work for the UHB and those using UHB premises and property. It is the intention of the UHB to work towards the reduction and elimination of all security breaches, whether directed at staff, patients, contractors or visitors. This must be done in such a way that it balances with a duty of care, providing comfortable, user-friendly, easily accessible services.

Policy Commitment

The protection of patients, staff, visitors and UHB assets will enable the continuation of our core activity, that is, the treatment and care of our patients to be conducted in a safe environment, free from worry or concern over the damaging effect that crime or the threat of violence gives. It will create an atmosphere of care and foster a better-motivated workforce. Additionally, the protection of assets, either corporate or personal will enable resources to be focused into patient care, rather than be diverted in the direct and consequential costs of losses incurred by criminal activity.

The objectives of the Security Policy are:

- a/. Prevention or detection of crime and disorder
- b/. Apprehension and Prosecution of offenders
- c/. Interest of public and employee Health and Safety
- d/. Protection of Public Health
- e/. Protection of NHS property and assets

Supporting Procedures and Written Control Documents

This Policy is supported by the following documents:

- Health and Safety Policy.
- Security Management Framework for NHS in Wales
- Fire Safety Policy
- Lone Worker Policy
- Counter Fraud and Corruption Policy
- Equality, Diversity and Human Rights Policy
- Major Incident Plan
- ID Badge Policy

Document Title: Security Services Policy	2 of 19	Approval Date: 09/04/2019
Reference Number: UHB 037		Next Review Date: 09/04/2022
Version Number: 4		Date of Publication: 15/07/2019

- Patients Property Policy
- Incident, Hazard and Near Miss Reporting Policy
- Closed Circuit Television (CCTV) Policy

Scope

This policy applies to all of our staff in all locations including those with honorary contracts.

Equality Impact Assessment	An Equality Impact Assessment (EqIA) has found there to be no impact.	
Health Impact Assessment	A Health Impact Assessment is not required for this policy.	
Policy Approved by	Health and Safety Committee	
Group with authority to approve procedures written to explain how this policy will be implemented	Health and Safety Committee	
Accountable Executive or Clinical Board Director	Director of Planning.	
Disclaimer		
If the review date of this document has passed please ensure that the version you are using is the most up to date either by contacting the document author or the		

Governance Directorate.

Summary of reviews/amendments			
Version Number	Date Review Approved	Date Published	Summary of Amendments
1	November 2010	08/06/2011	Revised and updated from previous Trust version.
2	22/01/2013	21/02/2013	Policy Reflects Organisational Change
3	26/01/2016	20/05/2016	Review - (sub section entitled 'Overlap with other policies' removed as these are now highlighted above as supporting documents)
4	09/04/2019	15/07/2019	3 yearly review period. Reviewed in line with new policy arrangements

Document Title: Security Services Policy	3 of 19	Approval Date: 09/04/2019
Reference Number: UHB 037		Next Review Date: 09/04/2022
Version Number: 4		Date of Publication: 15/07/2019

Policy Contents

Roles and Responsibilities	pages 4
Local Management and Staff Responsibilities	page 5
Resources	page 7
Reporting of security incidents	page 7
Security Incident Response plans	pages 8
Personal Safety	page 9
Lone Worker	page 10
Security of Building and Departments	page 11
Key control	page 11
Security of Monies	page 12
Malicious Intent / Threats	page 13
Appendix 1 – Security Services Structure	

Appendix 2 – Security Incident Response Plans

Appendix 3 – Lone Worker Devices

Appendix 4 – Malicious Intent / Threat flow chart

Document Title: Security Services Policy	4 of 19	Approval Date: 09/04/2019
Reference Number: UHB 037		Next Review Date: 09/04/2022
Version Number: 4		Date of Publication: 15/07/2019

Security Roles and Responsibilities

The Chief Executive

The Chief Executive is responsible for security arrangements, policy and Health and Safety implementation within Cardiff and Vale UHB.

Executive Director of Planning (EDP)

The EDP is responsible for promoting security at Board level and for monitoring and ensuring compliance with the requirements and directions of the Welsh Government and Department of Health in relation to security.

Head of Security Services

The Head of Security Services reports to the Head of Commercial services.

The Head of Security Services is responsible for:

- Assisting Cardiff and Vale UHB to realise the requirements and directions issued by the Welsh Government, Department of Health and the Counter Fraud and Security Management Service.
- Responsible for the daily management of all security throughout the UHB, ensuring a high quality and responsive service to patients, visitors and staff.
- To advise on the appropriateness of crime prevention and security by design.
- Reducing crime against Cardiff and Vale UHB property and assets.
- The provision of specialist security advice, information and guidance.
- Ensuring crime prevention, personal safety and security awareness training for staff is available.
- Ensuring that physical assaults against Cardiff and Vale UHB staff are investigated.
- Securing prosecutions (where possible) in relation to assault, theft, damage to UHB property or anti-social behaviour and gather evidence without notice.
- To liaise with the police, and other interested stakeholders and take action on their behalf as required in the best interests of Cardiff and Vale UHB.

Document Title: Security Services Policy	5 of 19	Approval Date: 09/04/2019
Reference Number: UHB 037		Next Review Date: 09/04/2022
Version Number: 4		Date of Publication: 15/07/2019

Security Services Manager

The Security Services Manager is:

- Responsible for supporting the Head of Security Services in all aspects of security throughout the Health Board, ensuring a high quality and responsive service to patients, visitors and staff.
- Responsible for supporting the Head of Security Services in the daily management of all security throughout the UHB, ensuring a high quality and responsive service to patients, visitors and staff.
- Supporting the Head of Security Services who is operationally responsible for the security service aspect of the UHB.
- Responsible for supporting the Head of Security Services to ensure that performance management targets are met.
- Responsible for ensuring the standards for Processes, Capability and Monitoring identified within the Security Management Framework for NHS in Wales are implemented.
- Responsible for supporting the Head of Security Services who is operationally responsible for the security service aspect of the Health Board in the absence of the Security Operations Manager.

Case Manager/Personal Safety Adviser

The Case Manager/Personal Safety Adviser:

- Is the lead expert on Violence and Aggression Management/Personal Safety within the Cardiff and Vale UHB.
- Will contribute to the creation of a safe and secure environment for staff and members of the public so that the highest standards of clinical care can be made available to patients.
- Will provide support and information for the victims of violence and aggression, whilst at the same time using the process of case management to take forward prosecutions in partnership with stakeholders within the NHS and external organisations such as the Police and Crown Prosecution Service.

Local Management and Staff Responsibilies

Directors, Heads of Service, Departmental Leads.

Security is a management responsibility. All directors, heads of service and departmental leads are accountable for the day to day implementation of security arrangements within their areas of responsibility.

They should ensure that:

Document Title: Security Services Policy	6 of 19	Approval Date: 09/04/2019
Reference Number: UHB 037		Next Review Date: 09/04/2022
Version Number: 4		Date of Publication: 15/07/2019

- Security risks are regularly assessed and appropriate controls are put in place.
- On receipt of an Incident Reporting Form from staff, they complete the relevant sections following investigation, provide feedback to staff member, action accordingly and forward to the Health and Safety Department.
- Staff receive security and crime prevention training appropriate to their workplace and are made aware of incidents reports and security trends in their Directorate.
- Adequate measures are in place in relation to the physical security of UHB premises and property including lock down of premises and areas when not in use.
- Adequate local arrangements exist to maintain the security of staff, patients, contractors, visitors, premises under their control.
- Breakdown of local security measures such as defective locks, broken windows etc are reported to the appropriate department for repair / replacement.
- All patient data and records are held securely (see UHB Data Protection Policy).

Staff

Cardiff and Vale UHB staff must co-operate with management to achieve the aims of this Security Policy.

All staff have the following responsibilities:

- Comply with approved guidelines and policies.
- Protect the interests of patients.
- Safeguard patient property.
- Guard against assault.
- Guard against theft of personal and / or NHS property.
- Be aware of when, and in what circumstances to contact the Police.
- Be aware of their duty to fellow staff members and to the UHB.
- Report all incidents to person in charge and complete the UHB Incident Reporting Form.
- Wear Identification Badges at all time whilst on duty.
- All staff must be aware that it is an offence to remove any UHB property without written agreement from their line manager / supervisor.

Further Information

Further information and advice, including Security telephone contact numbers, procedure for obtaining an ID Badge and other useful information can be found at: <u>Security Services</u>

Document Title: Security Services Policy	7 of 19	Approval Date: 09/04/2019
Reference Number: UHB 037		Next Review Date: 09/04/2022
Version Number: 4		Date of Publication: 15/07/2019

Resources

Health and Safety Committee

The Health and Safety Committee has over arching responsibilities for the coordination of health and safety matters within the UHB. This includes issues surrounding security, personal safety, lone worker and violence and aggression.

Security and Personal Safety Strategy Group (SPSSG)

The Security and Personal Safety Strategy Group chaired by the Head of Health and Safety has specific responsibilities in relation to the development of Security Services and the protection of UHB assets. Membership includes Health and Safety Services, Staff Representatives, Directorate Managers, Clinical Board Managers, Risk Managers, the Police and representatives from Cardiff University. The SPSSG reports to the Health and Safety Committee.

Reporting of Security Incidents

In order for the Cardiff and Vale UHB to effectively monitor and evaluate security risks it is vitally important that all crime and breaches of security are reported.

Reporting Process

The Incident Reporting Form is available via the e-datix link on the Cardiff and Vale UHB intranet. The UHB fully supports and encourages the use of these forms.

The completion of Incident forms will:

- Allow the reporting of actual and potential security incidents or risk.
- Provide a record of investigation and action taken to reduce risk.
- Provide information for the monitoring and evaluation of security incidents or risk by the health and safety department.
- Help to identify specific trends.

Where a security incident or crime is in progress it should be reported immediately to the security control room. They will initiate an appropriate response i.e. dispatch security officers, contact the police. An e-datix incident form should be completed as soon as is practicable after the incident has been resolved. If the police are involved a crime/occurrence number and action taken should be recorded on the form.

Security incidents discovered after the event e.g. theft, should also be reported to the security department and via the e-datix incident reporting form.

Document Title: Security Services Policy	8 of 19	Approval Date: 09/04/2019
Reference Number: UHB 037		Next Review Date: 09/04/2022
Version Number: 4		Date of Publication: 15/07/2019

Where the theft involves any item containing patient information e.g. computers, laptops, memory sticks etc. this must be reported to your line manager immediately as a potential breach of data protection.

Audit

Security incidents will be audited via:

- Risk management arrangements at Directorate level.
- Annual report to the Executive Director for Security.
- Security incident statistics and summary of the action taken obtained from data held on e-datix incident reporting system.
- Thefts and losses report to the Executive Director of Finance.
- Crime statistics

Security Incident Response Plans (SIRP)

Security Incident Definition

In simplistic terms a 'security incident' may be considered to be one which involves crime or the suspicion of crime whether it is serious or of low value. For example, if the outcome of the incident, when taken to its conclusion, would result in the injury or fear of injury to a member of staff or anybody on UHB premises, or the loss or damage of UHB or personal property.

Security Incident Response Plans (Local)

The primary intention of a Security Incident Response Plan (SIRP) is to provide a practical and effective method of reaction to both general and specific events that fall within the meaning of the term 'security incident'. The plans should set out, in clear and practical terms, the roles and responsibilities of all those who may be aware of the need for a response.

A Security Incident Response Plan (SIRP) should be prepared for each base and service within the UHB. It is the responsibility of the local manager / head of service to ensure that response plans are in place, relevant and that they are regularly audited. This will be particularly important following refurbishment, relocation or changes of room usage. The local manager / head of service should:

- Nominate those who have a role within the plan.
- Ensure staff are aware of the plan and their responsibility within it.
- Ensure that the Incident Reporting Procedures are reflected within the plan.

Following any security incident an e-datix incident reporting form must be completed. The effectiveness of the SIRP may be measured against how the

Document Title: Security Services Policy	9 of 19	Approval Date: 09/04/2019
Reference Number: UHB 037		Next Review Date: 09/04/2022
Version Number: 4		Date of Publication: 15/07/2019

incident was managed and how successfully the situation was resolved. A review of the SIRP should be supported by feedback from staff, especially those who have been closely involved, following the incident.

Principles of SIRP's

SIRP's are, in effect, an integral part of the Crime Reduction Plan (CRP). The principles on which they should be formulated are those of the CRP which are that they should:

- Deter criminal activity where possible.
- Deny the criminal the opportunity and delay the attack if it happens.
- Detect crime when it happens and
- Respond effectively to any event.

Format

All SIRP's should include the following key elements:

- Initial response.
- Consolidation.
- Recovery.
- Restoration of normality.

The suggested contents of the key elements are set out in Appendix 2.

Specific plans already exist to cover Major Incidents, Fire Safety and Child Abduction. These can be found on the respective Cardiff and Vale Intranet pages.

Personal Safety

Cardiff and Vale UHB recognises the importance of promoting and maintaining the personal safety of its staff. To fulfil these responsibilities the UHB will ensure that appropriate arrangements are in place for the personal safety of staff at work.

These arrangements will include conflict resolution training for front line staff, personal safety and risk assessment guidance. Local and Corporate induction for new staff should include reference to the Security Services Policy.

Staff should be made aware of security arrangements and procedures relevant to their area of work as well as general information on personal safety.

Document Title: Security Services Policy	10 of 19	Approval Date: 09/04/2019
Reference Number: UHB 037		Next Review Date: 09/04/2022
Version Number: 4		Date of Publication: 15/07/2019

Personal Safety Incidents

All incidents where staff are verbally abused, threatened or physically assaulted must be reported via the Incident, Hazard and Near Miss Reporting Policy and the information entered on the e-datix system. It is the responsibility of the member of staff's line manager to undertake a full investigation into the incident. The Case Manager should be notified of incidents that require case management support.

Staff Support

Following a personal safety incident, line managers should ensure that staff are given the opportunity to discuss the incident and receive assistance in the completion of reports. Staff should be given the opportunity to contact supportive agencies and given time off to attend if necessary. Further advice and assistance is available from the Case Management Team.

Lone Workers

Many NHS staff work on their own, either regularly or occasionally, without access to immediate support from work colleagues, managers or others. These lone workers need to be given organisational support, management and training to deal with the increased risks they face. They must also be empowered to take a greater degree of responsibility for their own safety and security.

It is the responsibility of line managers of staff who work alone to ensure that appropriate policies and procedures are developed, implemented, monitored and adhered to.

Lone workers have a responsibility to follow these policies and procedures for their own safety.

A quick guide for lone workers can be found as Appendix 3.

Further information:

The UHB Lone Worker Policy is available at : http://www.cardiffandvaleuhb.wales.nhs.uk/opendoc/169662

Staff Training

Cardiff and Vale UHB has made a commitment in accordance with the All Wales NHS Violence and Aggression Passport and Information Scheme, to deliver training to its staff in personal safety (violence and aggression). There is a legal requirement for staff to be provided with training to ensure the safe management of violence and aggression and to have the appropriate skills and knowledge to protect themselves and others from the risk of violence and

Document Title: Security Services Policy	11 of 19	Approval Date: 09/04/2019
Reference Number: UHB 037		Next Review Date: 09/04/2022
Version Number: 4		Date of Publication: 15/07/2019

aggression in the workplace. It is a management responsibility to ensure that staff receive the relevant level of training, and that records are kept and updated.

Further Information

Course information and other useful links are available via the health and safety section of the Cardiff and Vale Intranet.

Security of Buildings / Departments

Access Control/Swipe Card Security Systems

Access control systems are in operation at various locations within the UHB. The purpose of these systems is to ensure that only authorised persons are allowed access into certain areas/buildings or that access is restricted at certain times. The management of access control systems is via the Security Department.

All staff who work/access areas which have access control therefore have a responsibility to:

- Ensure that any faults are reported to the Security Department.
- Be vigilant of tailgaters.
- Never loan their Access Control Swipe card to anyone else.
- Report loss of Access Control Swipe cards to the Security Department immediately so that the card can be deactivated.

Key Control

Key control measures should be in place for all keys held locally in a department / building.

- All departmental keys should be kept in a locked key cabinet.
- There should be a register of all keys held.
- Members of staff/contractors who need to borrow a key must produce ID and sign a key control register when the key is issued/returned.
- Report lost or stolen keys to the Security Department.

Crime Prevention

It is the UHB's aim to raise awareness of incidence of crime taking place throughout the UHB. In doing so it is hoped to gain the commitment of all staff in working towards the reduction of crime. In order to ensure that incidence of crime is widely reported the following measures are in place:

• Security will continue to be a regular agenda item at Hospital User Group meetings.

Document Title: Security Services Policy	12 of 19	Approval Date: 09/04/2019
Reference Number: UHB 037		Next Review Date: 09/04/2022
Version Number: 4		Date of Publication: 15/07/2019

- In an effort to raise awareness, prevent recurrence and promote good practice security incidents will be brought to the attention of managers and staff throughout the UHB via the Cardiff and Vale intranet and email alerts.
- The Security Department's management will continue to work closely with the Police, Cardiff University and other local partners.
- Security alerts will continue to be issued (where appropriate) in conjunction with the Counter Fraud and Security Management Service (CFSMS) and the Police.

Security of Monies

At various locations throughout the UHB varying amounts of cash will be held at any one time. Staff who work with or hold cash should be advised of the following.

Cash handling

- Cash should be counted in an office or suitable location away from members of the public and other staff members.
- Where possible cash should be banked on a daily basis.
- Any losses or potential thefts of cash should be reported to your line manager.
- The line manager should report such thefts to the Security Operational Manager who will advise on the appropriate course of action, e.g. Police.

UHB Cash Banking

Where cash has to be taken to a bank/cashier the following procedure must be followed:

- A security officer escort should accompany the member of staff responsible for taking the cash to the bank/cashiers.
- When/where a security officer is not available cash should be taken by 2 members of staff.
- For regular (daily/weekly) banking, where possible routes/times should be varied.
- All cash should be carried in a suitable bag or brief case.

Keys/Codes

- Only authorised personnel should have knowledge of where safe and cash box keys are kept.
- Where coded/combination locks are used, knowledge of the code/ combination should be restricted to the minimum number of staff as possible.

Document Title: Security Services Policy	13 of 19	Approval Date: 09/04/2019
Reference Number: UHB 037		Next Review Date: 09/04/2022
Version Number: 4		Date of Publication: 15/07/2019

• It is recommended that codes/combinations are changed at least every 12 months or following a suspected security breach.

Malicious Intent/Threat

Cardiff and Vale UHB has the potential to attract the attention of terrorists who may be politically or otherwise motivated to plant explosive devices with a view to damaging property or maiming/killing people.

Person receiving the call

The attached (Appendix 4) provides a reference guide for staff who may receive a telephone call in relation to a bomb threat. A copy should be kept in all reception areas. The recording form should be completed with as much information as possible during the telephone call. On completion of the call the person taking the call should:

- Contact the Police on 999.
- Inform the line manager.
- Inform the Head of Security Services
- Inform Security Control room.
- Inform Site Practitioner/Nurse in charge.

Management Action

Immediately after the telephone threat the line manager should:

- Review the information entered on the recording form,
- Ensure instructions issued from HSS, Police, etc are followed.

Following resolution of the threat the line manager should:

- Produce a detailed report of the incident with statements.
- Support staff who may have been affected by the incident.
- Review the incident and ensure an e-datix Incident Reporting Form is completed.

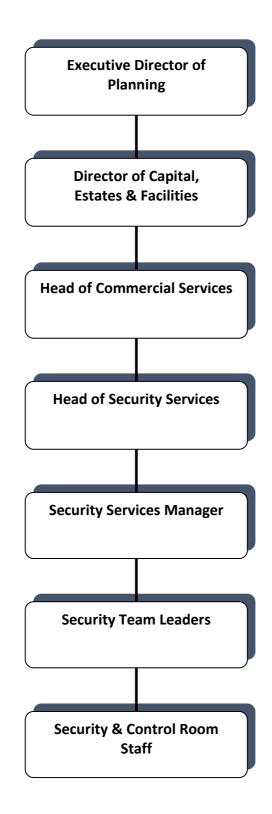
Distribution

This document will be distributed in accordance with the Cardiff and Vale University Health Board Policy for the Management of Policies, Procedures and all other written Control Documents and will be reviewed every three years.

Document Title: Security Services Policy	14 of 19	Approval Date: 09/04/2019
Reference Number: UHB 037		Next Review Date: 09/04/2022
Version Number: 4		Date of Publication: 15/07/2019

Security Services Structure

Appendix 1



Document Title: Security Services Policy	15 of 19	Approval Date: 09/04/2019
Reference Number: UHB 037		Next Review Date: 09/04/2022
Version Number: 4		Date of Publication: 15/07/2019

Security Incident Response Plans Appendix 2

The actions and responses shown are a guide to cover all types of incident. Minor incidents will only require a limited response compared to those for more serious events.

Initial Response

- Identify the type of incident.
- Raise the alarm.
- Detain suspect if personal safety is not put at risk.
- Alert Security Department, telephone operators, Police and UHB personnel as appropriate.
- Initiate procedure to secure area, building or clinical area.
- Isolate and protect the scene of crime (if necessary move patients).
- Obtain and circulate suspect's description within the location.
- Seek information from staff, patients and visitors.

Consolidation

- Keep a timed record of all actions.
- Record details of all witnesses and others in the unit/location at the time of occurrence.
- Protect and support victims.
- Check all personnel are aware of their roles.
- Arrange effective communications with incident management team, Police, emergency services etc.

Recovery

- Continue support and counselling of staff.
- Fully de-brief all involved.
- Prepare report of the incident and its outcome.

Return to Normality

- Reassure all patients, visitors and staff.
- Ensure that premises/individual working practices are returned to normal as soon as possible.
- Provide feedback to staff on outcome of incident.
- Review security incident response plans and make amendments where necessary.
- Review security equipment and crime prevention procedures.

Document Title: Security Services Policy	16 of 19	Approval Date: 09/04/2019
Reference Number: UHB 037		Next Review Date: 09/04/2022
Version Number: 4		Date of Publication: 15/07/2019

Within the format detailed above both general and specific plans may be made.

Specific plans already exist to cover Major Incidents, Fire Safety and Child Abduction. These can be found on the respective Cardiff and Vale Intranet pages.

Document Title: Security Services Policy	17 of 19	Approval Date: 09/04/2019
Reference Number: UHB 037		Next Review Date: 09/04/2022
Version Number: 4		Date of Publication: 15/07/2019

Lone workers advice

Appendix 3

- Familiarise yourself with the UHB's Lone Working policy.
- All staff have a legal duty to take reasonable care of their own safety.
- Make sure you have received up-to-date training in the prevention and management of violence (e.g. conflict resolution and lone worker personal safety).
- Know the risks of aggressive and violent behaviour by patients/service users and the appropriate measures for controlling these risks.
- Ensure you can access the appropriate safety equipment (e.g. lone worker alarm devices) and know how to use and maintain it.
- Remember the importance of thorough planning be aware of the risks and do everything you can in advance to ensure your safety.
- Always leave an itinerary with your manager or your colleagues and keep in regular contact with your base.
- Risk assessments should be completed for all lone working situations and know the circumstances under which visits can be terminated.
- Never put yourself or colleagues in danger. If you feel threatened, withdraw immediately.
- For further support, advice and guidance contact the Personal Safety Advisor, Health and Safety Department, UHW.

Document Title: Security Services Policy	18 of 19	Approval Date: 09/04/2019
Reference Number: UHB 037		Next Review Date: 09/04/2022
Version Number: 4		Date of Publication: 15/07/2019

Malicious Threat - telephone call procedure Appendix 4

DO NOT PUT DOWN THE RECEIVER OR CUT OFF THE CALLER. OBTAIN AS MUCH INFORMATION AS YOU CAN.

Complete this form as you go along. Ask questions as detailed below.

THREAT MESSAGE (Exact Words).

Where is the	
threat?	
If an incendiary	
device, what time	
is it set to go off?	
What does it look	
like?	
What kind of	
device is it?	
What will cause it	
to go off?	
Did you place the	
device yourself?	
Why are you doing	
this?	
Who do you	
represent?	
Is there some way	
we can contact	
you?	

Complete the following as soon as possible:

Telephone extension number where call received	
Date and Time of call	
Duration of call (approx.)	
Details of caller – Male / Female	
Approximate age:	

Document Title: Security Services Policy	19 of 19	Approval Date: 09/04/2019
Reference Number: UHB 037		Next Review Date: 09/04/2022
Version Number: 4		Date of Publication: 15/07/2019

Language – e.g. Well-spoken, Foul,	
Irrational, Taped, Reading a message	
etc	
Callers Voice – e.g. Calm, Angry,	
Slow, Loud, Laughing, Slurred,	
Disguised, Accent, Stutter, Lisp,	
Familiar	
If familiar, who did it sound like?	
Background Noises – e.g.	
Interruptions, Street noises, Voices,	
Music, Machinery, Children, Animal,	
Motors etc	
Any other Remarks	
Name of Person Receiving Call	
Extension no:	Ward/ dept:
Signature	