NHS
Kernow
Clinical Commissioning Group

Security Policy

Date approved: 20 May 2019

Document control sheet

Title of document:	Security Policy
Originating Directorate:	Local Security Management (via corporate governance)
Originating team:	Local Security Management (via corporate governance)
Document type:	Policy
Subject category:	Health & Safety
Author(s) name:	Mo Jackson, Local Security Management Specialist, ASW Assurance Jess James, Head of Corporate Governance, NHS Kernow
Date ratified:	20 May 2019
Ratified by:	Senior Management Team
Review frequency:	Three years (standard, unless otherwise indicated)
To be reviewed by date:	20 May 2022
Target audience:	All staff
Can this policy be released under FOI?	Yes
	Give reasons for exemption if no:

Version control

Version No	Revision date	Revision by	Nature of revisions
V1.0	March 2019	JJames	Initial draft.
V1.1	May 2019	TCorsellis and MJackson	Clarifications and review by LSMS
V2	20 May 2019	JJames	Ratification information updated and amendment of words ‘staff or patients’ to read ‘people’.

Contents

1. Introduction 4
2. Purpose 5
3. Responsibilities 5
4. Security procedures 8
5. Violence and aggression 9
6. CCTV 10
7. Emergency preparedness, resilience and response 10
8. Bomb threats 10
9. Reporting of security incidents 11
10. Assisting the police or other law enforcement agencies 11
11. Fire 12
12. PREVENT 12
13. Counter fraud 12
14. Monitoring compliance and effectiveness 12
15. Training 13
16. Associated policies 13
Equality Impact Assessment 14

1. Introduction

NHS Kernow Clinical Commissioning Group (CCG) is committed to promoting the security of its staff, its assets and the people who use the services it commissions. This policy has been produced by the Local Security Management Specialist (LSMS), with the support of the Corporate Governance team, and is intended as a guide for all employees on all NHS Kernow security matters.

NHS Kernow aims to provide a safe working environment, people can be confident of their personal safety and security of their possessions and where the CCG can be assured of the security of its buildings and assets.

All NHS Kernow employees are responsible for ensuring that security procedures are adhered to at all times. Managers should take a leading role in promoting a pro-security culture to ensure the safety of all colleagues.

The LSMS is an expert in all matters regarding security and can be contacted via the Corporate Governance team should a potential security concern arise. In the case of an immediate emergency, NHS Kernow's nominated LSMS can be contacted directly on 01392 356034 / 07824 606899.

NHS Kernow does not tolerate violence towards people, the theft of CCG assets or damage to CCG buildings. In order to reduce the likelihood of these acts being carried out, NHS Kernow has adopted the following operational framework:

- **Strategic Governance** – not tolerating violence and aggression towards people or theft/damage caused to NHS Kernow assets; making this clear to all staff; and monitoring, the effectiveness of the arrangements in place. NHS Kernow has appointed a qualified Local Security Management Specialist (LSMS) to support this commitment.
- **Inform and Involve** – through setting clear policies and a code of conduct for all staff; raising awareness of the risks; and liaising with other organisations to develop a shared resistance to violence and aggression, theft and criminal damage.
- **Prevent and Deter** – through focused assessment of risks in existing processes and the creation of recommendations to improve identified system weaknesses.
- **Hold to Account** – through the investigation of security-related incidents, should such situations arise, and through the application of appropriate sanctions.

Effective security management is linked to other policy areas, including fraud and bribery, bullying and harassment, emergency preparedness, resilience and response (EPRR) and lone working.

2. Purpose

NHS Kernow recognises its responsibility to provide a safe and secure working environment for all employees. This policy relates to all matters of security including the security of staff, property and assets. The overall aims of this policy are to:

- Improve the knowledge and understanding of all NHS Kernow employees irrespective of their position, about security within the organisation.
- Assist in promoting a climate of openness and a pro-security culture where staff feel able to raise concerns sensibly and responsibly.
- Ensure the appropriate sanctions are considered following an investigation.

This policy applies to all employees of NHS Kernow, regardless of position held, as well as consultants, vendors, contractors, and/or any other parties who have a business relationship with the CCG.

3. Responsibilities

Security is the responsibility of all staff in not only safeguarding themselves and their property, but also property belonging to NHS Kernow. The primary objectives of security management are:

- The prevention of violent or aggressive behaviour towards NHS Kernow staff, visitors, or the people who use the services we commission.
- The protection of life from malicious criminal activity or other hazards.
- The protection of premises and assets against theft and damage.
- The detection and reporting of suspected offenders committing offences against people, property or private property within NHS Kernow premises.
- The education of all staff in security awareness.
- The smooth and uninterrupted delivery of health care and commissioning services.

The Governing Body has delegated to the Workforce committee its responsibility for gaining assurance that adequate arrangements are in place to ensure that all staff are aware of the standards of personal and professional behaviour expected of them and that all staff have access to this policy.

The Health and Safety sub- committee is responsible for gaining assurance that:

- NHS Kernow has appointed a qualified Local Security Management Specialist (LSMS) to lead the drive to maintain and improve the standards and processes

for deterring, detecting and investigating wrongdoings and seek prosecution where wrongdoing is discovered.
- The annual Security Management Workplan is adequate and provides a reasonable balance between raising security awareness across the organisation and evaluating the effectiveness of NHS Kernow's security systems and controls.
- Receiving annual reports from the LSMS on the progress against the Security Management Workplan and updates of the progress of any investigations.

The Workforce committee will receive regular reports from the Health and Safety sub-committee as well as be responsible for receiving and responding to or approving to recommendations from any investigations or matters escalated.

The Deputy Director of Corporate Governance is the lead for all Security Management work in NHS Kernow and monitors and ensures compliance with SC24 of the NHS England standard commissioning contract and is responsible for:

- Managing the continuity of appointment of a qualified LSMS for NHS Kernow;
- Overseeing the delivery of services from the LSMS.
- Providing the relevant required support to the LSMS in any investigations or pro-active work that they carry out.
- Informing appropriate senior management accordingly, depending on the outcome of investigations (whether on an interim/on-going or concluding basis) and/or the potential significance of suspicions that have been raised.
- Gaining assurance that providers awarded contracts with NHS Kernow have suitable security management arrangements (e.g. Workplan and Annual Report) as reviewed and reported by the LSMS.

The Head of Corporate Governance supports the Deputy Director in her role providing operational support to the LSMS on a regular basis.

Individual members of staff are required to:

- Actively co-operate with managers to achieve the aims and objectives of this policy, and to familiarise themselves with:
    - Any special security requirements relating to their place of work; and
    - The action to take in the event of a security incident.
- Safeguard themselves, colleagues, visitors and other people so far as is reasonably practicable and ensure that equipment and property are not put in jeopardy by their actions or omissions, either by instruction, example or behaviour.
- Comply with all training requirements concerning security issues.

- Ensure that NHS Kernow ID is worn and visible whenever on NHS Kernow premises or on NHS Kernow business.
- Notify their line manager of any potential security problems and report all incidents involving criminal activity to the appropriate manager.
- Report any crime or breach of security.

Managers at all levels have a responsibility to:

- Ensure that an adequate system of internal control exists within their areas of responsibility and that controls operate effectively.
- Complete any risk assessments required in relation to the security of staff, premises or assets.
- Ensure that security issues known to them are reported accordingly.
- Ensuring that every member of staff obtains a security ID badge and that the badge is worn and visible at all times whilst the staff members is on NHS Kernow premises or on NHS Kernow business.
- Ensure that all employees for whom they are accountable for, are made aware of the requirements of the policy.

Local Security Management Specialist (LSMS)

NHS Kernow’s nominated LSMS is provided by ASW Assurance. The overall objective of the LSMS will be to work on behalf of NHS Kernow to provide a safe and secure working environment with a pro-security culture. The LSMS will:

- Report to the Deputy Director of Corporate Governance on security management work locally.
- Lead on day to day work within NHS Kernow to tackle violence against staff and professionals in accordance with national guidance.
- Ensure that lessons are learned from security incidents, and that actions to mitigate the risks arising from incidents are carried out promptly.
- Investigate security incidents, as directed by the CFO, in a fair, objective and professional manner so that appropriate sanctions and preventative action can be taken.
- Ensure that the Security Management policy addresses all relevant, identified risks within NHS Kernow and contains useful guidance.
- Assist managers with completion of risk assessments.
- Produce an annual Security Management Workplan aligned to the resource made available.

4. Security procedures

4.1 Staff Identification

Every employee, including employees on short/fixed term contracts will be issued with an identification badge on commencement of employment with NHS Kernow, which must be worn and made visible at all times whilst on NHS Kernow premises or on official business.

Each member of staff is personally responsible for their badge and its validity. Any radical changes in physical appearance, job title or department must result in the issue of a new ID badge.

Identification badges must be returned to the employee's line manager when a member of staff leaves the employment of NHS Kernow. It is the responsibility of the line manager to recover the identity badge from the member of staff concerned.

Lost or missing ID badges should be reported immediately via kccg.incidents@nhs.net. Should a reported lost badge be subsequently found; the original must be returned to NHS Kernow and the incident report updated.

4.2 Visitors and contractors

External visitors and contractors, should be escorted while on site. Regular visitors, who are known to staff and familiar with the site may not require escort. The member of staff who is responsible for the visitor/contractor should notify the reception staff that they are expecting a visitor and, where not a regular visitor, arrange for the individual(s) to be met at reception. Visitor badges must be signed in upon issue and signed out upon return.

4.3 Access and Egress

Access to NHS Kernow offices is restricted via the use of electronic ID badges and/or coded key pads.

Electronic ID badges must not be swapped, loaned or given to unauthorised personnel at any time.

Tailgating - All staff must challenge any unknown/unfamiliar person attempting to gain access, in particular if an ID badge or visitor permit is not visible.

4.4 Security of Goods

Goods received into the organisation must be checked against delivery notes prior to signing for acceptance.

All NHS Kernow departments receiving goods must ensure that there are procedures in place to monitor the receipt of goods and safe/secure systems are in place to protect goods from theft or misappropriation.

4.5 Security of Personal Belongings

All staff should ensure that personal belongings are stored in a secure location, for example in locked cupboards, desks or drawers. In the absence of negligence, NHS Kernow cannot be held responsible for the theft of personal items, and cannot accept responsibility for loss or damage to staff property.

4.6 Security of Motor Vehicles

In the absence of negligence, NHS Kernow cannot accept liability for any private motor vehicle or its contents when parked on a NHS Kernow occupied site or when the car is being used by an employee on NHS Kernow business.

4.7 Property and Assets

. Managers should review NHS Kernow property held by their department on a regular basis to ensure that all items are securely managed. Changes in allocation or status of assets, such as laptops and mobile phones, should be reported to the NHS Kernow information management and technology team.

All managers and staff should take reasonable steps to safeguard NHS Kernow property whilst it is in their care. It is an offence for members of staff to remove or fail to return property belonging to NHS Kernow without prior authority from their line manager or the custodian of the equipment. Failure to seek authority could result in disciplinary action and/or criminal proceedings being undertaken.

4.8 Lone Working

Working alone can bring additional risks to an activity. NHS Kernow has developed policies and procedures to control the risks and protect employees and staff should refer to the NHS Kernow Lone Working Policy.

The three most important aspects of lone working are that:

- The lone worker has full knowledge of the hazards and risks to which they are exposed.
- The lone worker knows what to do if something goes wrong.
- Someone else knows the whereabouts of the lone worker, the type of work they are doing and the expected time of completion.

5. Violence and aggression

NHS Kernow has a duty to provide a safe and secure environment for all employees and visitors and will not tolerate violence and abusive behaviour.

NHS Kernow takes a very serious view of violence, abuse and aggression at work and realises its responsibility to protect employees and others who may be subjected to action of violence, abuse or aggression whether or not the act results in physical or non-physical assault.

Any member of the public, person who uses the services we commission or otherwise who are violent towards NHS Kernow staff may have sanctions taken against them, be refused treatment, and/or taken to court by NHS Kernow in line with national guidance.

Staff should report any incidence of violence and aggression to their line manager and via kccg.incidents@nhs.net and refer to the Acceptable Behaviour policy.

6. CCTV

External CCTV is in place on CCG premises. This is managed by the landlord who owns the building and CCTV system. Requests for access to CCTV images are deemed to be a subject access request and as such should be made via the corporate governance team (kccg.corporategovernance@nhs.net) who will then approach NHS Property Services. For any request other than subject access, the requestor must state a lawful basis which would allow the processing of CCTV images. A decision will be made by the corporate governance team and / or LSMS to determine whether the CCTV images can be disclosed. This would also include requests made by police officers or other law enforcement agencies.

7. Emergency preparedness, resilience and response

A significant incident or emergency can be described as any event that cannot be managed within routine service arrangements. Each required the implementation of special procedures and may involve one or more of the emergency services, the wider NHS or a local authority. Please refer to the Incident Response Plan and Business Continuity Plan.

8. Bomb threats

The vast majority of bomb threats are hoaxes. Making such malicious calls is an offence contrary to Section 51 of the Criminal Law Act 1977 and should always be reported to the police. Any member of staff receiving such a call should seek the immediate advice of the most senior manager available.

For immediate guidance on how to deal with bomb threats, go to the gov.uk website. This can be found at: https://www.gov.uk/government/publications/bomb-threats-guidance

A bomb threat checklist for action to be taken on receipt of a bomb threat is also available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/552301/Bomb_Threats_Form_5474.pdf

9. Reporting of security incidents

All employees have a responsibility to report all crimes and breaches of security and should refer to the Incident Reporting and Management Policy.

Any crimes in progress should be reported to the police immediately and subsequently reported via kccg.incidents@nhs.net. The corporate governance team will report these and any other reported crimes, security related incidents or near misses to the LSMS as soon as possible.

If a security incident involves the **assault or abuse of a staff member of visitor**, this should be reported via kccg.incidents@nhs.net as soon as possible. Managers must offer any staff assaulted support via a meeting to identify any needs, such as counselling. Visitors should be signposted to an organisation such as victim support (www.victimsupport.org.uk / Freephone 0808 16 89 111).

If the security incident involves the **theft of person identifiable or corporate confidential information** (eg theft of records, data storage, laptop etc) this should be reported immediately to the Data Protection Officer or Head of Information Governance and an information governance breach proforma completed. Please refer to the Data Protection policy or contact the corporate governance team for further information.

Other security incidents to be reported might include large crowds demonstrating outside NHS Kernow property; unauthorised access to staff areas; and suspicious packages.

10. Assisting the police or other law enforcement agencies

Occasionally, the police or other law enforcement agencies may contact NHS Kernow for information relating to an ongoing investigation. Any individual who is contacted in such a manner should refer the police to the LSMS or Deputy Director of Corporate Governance as the initial point of contact.

Staff should obtain guidance from the information governance team should they be asked to disclose confidential information to the police

11. Fire

The overlapping interests of security and fire safety policies are fully recognised. There is full co-operation between fire and security staff.

12. PREVENT

NHS Kernow has due regard to compliance with the requirements of the PREVENT guidance for England and Wales. Regarding security management this will include:

- Ensuring that if there are concerns around rooms or buildings being used for radicalisation or terrorism, that these are reported immediately to the Safeguarding Adults team, who take the lead on PREVENT.
- Ensuring relevant staff have received PREVENT training as per the PREVENT policy, and that as a result of this training, staff report issues to relevant managers for escalation.
- Ensuring that there is an identified PREVENT lead. Within NHS Kernow the Safeguarding Adults team take the lead on PREVENT.

Please refer to the NHS Kernow Prevent policy for more details.

13. Counter fraud

The overlapping interests of security management and counter fraud are fully recognised. The LSMS will liaise closely with the Local Counter Fraud Specialist (LCFS) to ensure incidents which could be constituted as theft or fraud are appropriately investigated.

14. Monitoring compliance and effectiveness

The Deputy Director of Corporate Governance and the LSMS will agree annual and specific measures of the effectiveness of this policy.

As a minimum, the LSMS will report annually on the number and nature of instances of security incidents. This report will include details of outcomes and consequences to the individuals involved.

The LSMS will, through the annual programme of work, determine the effectiveness of NHS Kernow‘s controls and other efforts to prevent and deter security breaches.

The results of these risk assessments will be reported in the LSMS annual report to the Health and Safety sub-committee. Delivery of actions agreed to address weaknesses and lapses identified in the implementation of the policy will be monitored by the Health and Safety sub-committee.

15. Training

All staff should be made aware of the policy and their responsibility to report security incidents and crime in the NHS through a mixture of targeted security awareness items in staff bulletins and the staff intranet.

16. Associated policies

Acceptable behaviour policy
Business continuity plan
Data Protection policy
Dignity at work policy
Disciplinary policy
Health and safety policy
Incident reporting and management policy
Incident response plan
Lone working policy
Prevent policy
Safeguarding children and adults policy
Subject access policy

NHS
Kernow
Clinical Commissioning Group

Equality Impact Assessment

Name of policy to be assessed	Security Policy		
Section	Corporate Governance	**Date of Assessment**	15/05/2019
Officer responsible for the assessment	Head of Corporate Governance	**Is this a new or existing policy?**	New
1. Describe the aims, objectives and purpose of the policy.			
This policy relates to all matters of security including the security of staff, property and assets. The overall aims of this policy are to: • Improve the knowledge and understanding of all NHS Kernow employees irrespective of their position, about security within the organisation. • Assist in promoting a climate of openness and a pro-security culture where staff feel able to raise concerns sensibly and responsibly. • Ensure the appropriate sanctions are considered following an investigation.			
2. Are there any associated objectives of the policy? Please explain.			
None			
3. Who is intended to benefit from this policy, and in what way?			
Staff, visitors, members of public, people who use the services we commission, through increased safety and security, protection from harm, loss, theft etc.			
4. What outcomes are wanted from this policy?			
Improved awareness of structures and process in place for security management in NHS Kernow..			
5. What factors/ forces could contribute/ detract from the outcomes?			
Lack of staff awareness of policy and processes involved. Colleagues unfamiliar with systems (this will be mitigated through regular reminders through weekly bulletin)			
6. Who are the main stakeholders in relation to the policy?			

This policy applies to all employees of NHS Kernow, regardless of position held, as well as consultants, vendors, contractors, and/or any other parties who have a business relationship with the CCG.
7. Who implements the policy, and who is responsible for the policy
Corporate Governance team and Local Security Management Specialist.
8. What is the impact on people from Black and Minority Ethnic Groups (BME) (positive or negative)?
Consider relevance to eliminating unlawful discrimination, promoting equality of opportunity and promoting good race relations between people of different racial groups. Issues to consider include people's race, colour and nationality, Gypsy, Roma, Traveller communities, employment issues relating to refugees, asylum seekers, ethnic minorities, language barriers, providing translation and interpreting services, cultural issues and customs, access to services.
No differential impact is anticipated on these groups.
How will any negative impact be mitigated?
Not applicable.
9. What is the differential impact for male or female people (positive or negative)?
Consider what issues there are for men and women e.g. responsibilities for dependants, issues for carers, access to training and employment issues, attitudes towards accessing healthcare.
No differential impact is anticipated.
How will any negative impact be mitigated?
Not applicable
10. What is the differential impact on disabled people (positive or negative)?
Consider what issues there are around each of the disabilities e.g. access to building and services, how we provide services and the way we do this, producing information in alternative formats and employment issues. Consider the requirements of the NHS Accessible Information Standard. Consider attitudinal, physical and social barriers. This can include physical disability, learning disability, people with long term conditions, communication needs arising from a disability.
No differential impact is anticipated.

How will any negative impact be mitigated?
Not applicable
11. What is the differential impact on sexual orientation?
Consider what issues there are for the employment process and training and differential health outcomes amongst lesbian and gay people. Also consider provision of services for e.g. older and younger people from lesbian, gay, bi-sexual. Consider heterosexual people as well as lesbian, gay and bisexual people.
No differential impact is anticpated.
How will any negative impact be mitigated?
Not applicable
12. What is the differential impact on people of different ages (positive or negative)?
Consider what issues there are for the employment process and training. Some of our services impact on our community in relation to age e.g. how do we engage with older and younger people about access to our services? Consider safeguarding, consent and child welfare.
No differential impact is anticipated
How will any negative impact be mitigated?
Not applicable
13. What differential impact will there be due religion or belief (positive or negative)?
Consider what issues there are for the employment process and training. Also consider the likely impact around the way services are provided e.g. dietary issues, religious holidays, days associated with religious observance, cultural issues and customs, places to worship.
No differential impact is anticipated
How will any negative impact be mitigated?
Not applicable
14. What is the impact on marriage of civil partnership (positive or negative)? NB: this is particularly relevant for

employment policies
This characteristic is relevant in law only to employment, however, NHS Kernow will strive to consider this characteristic in all aspects of its work. Consider what issues there may be for someone who is married or in a civil partnership. Are they likely to be different to those faced by a single person? What, if any are the likely implications for employment and does it differ according to marital status?
No differential impact is anticipated
How will any negative impact be mitigated?
Not applicable
15. What is the differential impact who have gone through or are going through gender reassignment, or who identify as transgender?
Consider what issues there are for people who have been through or a going through transition from one sex to another. How is this going to affect their access to services and their treatment when receiving NHS care? What are the likely implications for employment of a transgender person? This can include issues such as privacy of data and harassment.
No differential impact is anticipated
How will any negative impact be mitigated?
Not applicable
16. What is the differential impact on people who are pregnant or breast feeding mothers, or those on maternity leave?
This characteristic applies to pregnant and breast feeding mothers with babies of up to six months, in employment and when accessing services. When developing a policy or services consider how a nursing mother will be able to nurse her baby in a particular facility and what staff may need to do to enable the baby to be nursed. Consider working arrangements, part-time working, infant caring responsibilities.
No differential impact is anticipated
How will any negative impact be mitigated?

Not applicable

17. Other identified groups:

Consider carers, veterans, different socio-economic groups, people living in poverty, area inequality, income, resident status (migrants), people who are homeless, long-term unemployed, people who are geographically isolated, people who misuse drugs, those who are in stigmatised occupations, people with limited family or social networks, and other groups experiencing disadvantage and barriers to access.

No differential impact is anticipated

How will any negative impact be mitigated?

Not applicable

18. How have the Core Human Rights Values been considered in the formulation of this policy/strategy? If they haven’t please reconsider the document and amend to incorporate these values.

- **Fairness;**
- **Respect;**
- **Equality;**
- **Dignity;**
- **Autonomy**

The policy has been written to ensure that people are treated with dignity and respect by protecting them from harm and loss.

19. Which of the Human Rights Articles does this document impact?

The right:	**Yes / No:**
• To life	Yes
• Not to be tortured or treated in an inhuman or degrading way	Choose an item.
• To liberty and security	Yes
• To a fair trial	Choose an item.
• To respect for home and family life, and correspondence	No
• To freedom of thought, conscience and religion	Choose an item.
• To freedom of expression	Choose an item.
• To freedom of assembly and association	Choose an item.

• To marry and found a family	Choose an item.
• Not to be discriminated against in relation to the enjoyment of any of the rights contained in the European Convention	Choose an item.
• To peaceful enjoyment of possessions	Yes
a) What existing evidence (either presumed or otherwise) do you have for this?	
Policy covers processes around personal safety and security and that of possessions.	
20. How will you ensure that those responsible for implementing the Policy are aware of the Human Rights implications and equipped to deal with them?	
The Human Rights Statement and Guidance accompanies the Equality Impact Assessment guidance and Comprehensive Impact Assessment guidance, to provide comprehensive information for staff. These policies are available for staff on the NHS Kernow website and have been proactively disseminated via the staff bulletin.	
21. Describe how the policy contributes towards eliminating discrimination, harassment and victimisation.	
Policy cross references with the Acceptable Behaviour Policy and the Incident Management Policy both of which contribute towards eliminating discrimination, harassment and victimisation.	
22. Describe how the policy contributes towards advancing equality of opportunity.	
Policy contributes to equality of opportunity by seeking to provide a safe, secure working environment for all our staff.	
23. Describe how the policy contributes towards promoting good relations between people with protected characteristics.	
Policy contributes to promoting good relations by seeking to provide a safe, secure working environment, and cross references the Acceptable Behaviour Policy and the Incident Management Policy both of which contribute towards eliminating discrimination, harassment and victimisation.	
24. If the differential impacts identified are positive, explain how this policy is legitimate positive action and will improve outcomes, services or the working environment for that group of people.	
No differential impacts identified.	
25. Explain what amendments have been made to the policy or mitigating actions have been taken, and when they were made.	

None
26. If the negative impacts identified have been unable to be mitigated through amendment to the policy or mitigating actions, explain what your next steps are.
Not applicable

Signed (completing officer): …………Jess James ……………………………………………..

Date: …………………14/5/19……………………………………..

Signed (Head of Section): ………………………………………………………..

Date: ………………………………………………………..

Please ensure that a signed copy of this form is sent to both the Policies Officer with the policy and the Equality and Diversity lead.