REMOTE WORKING AND PORTABLE DEVICES POLICY

Policy Type	Non Clinical
Directorate	Corporate
Policy Owner	Director of Finance, Estates and IM&T
Policy Author	Information Security Manager
Next Author Review Date	1st February 2024
Approving Body	Policy Management Sub-Committee 31st July 2020
Version No.	4.0
Policy Valid from date	1st August 2020
Policy Valid to date:	31st July 2024

'During the COVID19 crisis, please read the policies in conjunction with any updates provided by National Guidance, which we are actively seeking to incorporate into policies through the Clinical Ethics Advisory Group and where necessary other relevant Oversight Groups'

This document forms part of the suite of documents for Isle of Wight NHS Trust's ISO|IEC27001:2013 Information Security Management System (ISMS). As such, it is continuously monitored via the Information Governance Sub-Committee (IGSC) and is subject to annual review.

DOCUMENT HISTORY

(Procedural document version numbering convention will follow the following format. Whole numbers for approved versions, e.g. 1.0, 2.0, 3.0 etc. With decimals being used to represent the current working draft version, e.g. 1.1, 1.2, 1.3, 1.4 etc. For example, when writing a procedural document for the first time – the initial draft will be version 0.1)

Date of Issue	Version No.	Date Approved	Director Responsible for Change	Nature of Change	Ratification / Approval
19 Mar 16	0.1		Executive Director of Transformation and Integration	New Policy	
24 Mar 16	1		Executive Director of Transformation and Integration	Approved at	Trust Executive Committee
25 Jan 17	1.1		Director of Strategy and Planning	Reviewed and Amended	
9 Feb 17	1.1		Director of Strategy and Planning	Ratification at	Information Governance Steering Group
14 Feb 17	2.0		Director of Strategy and Planning	Approval at	Corporate Governance & Risk Sub-Committee
08 Feb 18	2.1		Director of Integration and Transformation	Ratified at	Information Governance Sub-Committee
13 Feb 2018	3.0	13 Feb 2018	Director of Integration and Transformation	Approved at	Policy Management Sub-Committee
March 2020	3.1		Director of Finance, Estates and IM&T	Policy review	
26 March 2020	3.1		Director of Finance, Estates and IM&T	Contents agreed at	Information Governance Sub-Committee
31 July 2020	4.0	31 July 2020	Director of Finance, Estates and IM&T	approved at	Policy Management Sub-Committee
29 Jan 2021	4.0	31 July 2020	Director of Finance, Estates and IM&T	12 month blanket policy extension due to covid 19 applied with author review date set 6 months prior to Valid to Date.	Quality & Performance Committee
20 May 2021	4.0	31 July 2020	Director of Finance, Estates and IM&T	Extended policy uploaded and linked back with new cover sheet	Corporate Governance

Uncontrolled when printed

NB This policy is applicable to the Isle of Wight NHS Trust, hereafter referred to as the Trust

Contents

Uncontrolled when printed

1 Executive Summary

Information security breaches may cause real harm and distress to the individuals they affect. Lives may even be put at risk.

This policy has been created to allow the Trust to derive the benefits of increased efficiency from the use of mobile systems and flexible working whilst ensuring the protection of its assets, the integrity of the data, employee rights and Health and Safety as well as Information Governance and legal requirements.

2 Introduction

This policy describes the Trusts expectations and requirements for remote working and the use of portable devices. The policy applies to all staff working directly for the Trust, and any organisation that has entered into an agreement to work remotely for the Trust.

3 Definitions

Remote Working – includes all handling of Trust information and its information assets.

Portable Equipment – includes, but is not limited to, Laptops, Mobile Phones and Smart phones, Tablet devices, PC's, USB Memory devices and other forms of digital storage.

Technology continues to evolve and thus this is not intended to be an exhaustive definition/list however, it includes all battery powered and mains adapted personal computing and storage devices.

4 Scope

This policy applies to all users of Trust information assets, when used remotely. All users must agree to adhere to this policy before a Trust portable device is provided and before using any computing or storage device in conjunction with Trust assets.

5 Purpose

The purpose of this Policy is to set out the process to be used to enable staff to use portable devices and information assets in a responsible and appropriate way, including:-

- Understanding their responsibilities when accessing the network
- Understanding the possible implications and risk of information misuse

6 Roles and Responsibilities

6.1 Senior Information Risk Officer (SIRO)

The SIRO is responsible for managing information risk in the Trust and will implement and lead the NHS IG risk assessment and management of information risk via the Information Risk Management Structure. They will also advise the Trust Board and other relevant committees on the effectiveness of the Trusts Information Governance Framework and provide written advice to the Accountable Officer regarding the information risk elements of their Annual Governance Statement.

The SIRO will advise the Trust on matters relating to IG Risk and Information Security.

Uncontrolled when printed

They will ensure that all staff provided with mobile/agile technology are aware of the inherent risks and how to mitigate them.

6.2 Director of Finance, Estates and IM&T

The Director of Finance, Estates and IM&T has ultimate responsibility for ensuring compliance with this policy.

6.3 Deputy Director of IM&T

The Deputy Director of IM&T has responsibility for overseeing the implementation of IT related security processes and procedures within the Information Communication Technology department, and ensure that appropriate documentation is in place to this effect, for example this policy.

6.4 Information Security Manager

The responsibilities of the Information Security Manager will include:

- Acting as a central point of contact on information security within the organisation and for external organisations that has entered into an agreement for the provision of ICT services by the Trust.
- Implementing an effective framework for the management of information security.
- Assisting in the formulation of Information Security Policy and related policies.
- Advise on the content and implementation of the Information Security Programme.
- Co-ordinate information security activities particularly those related to shared information systems or IT infrastructures.
- Liaise with external organisations on information security matters, including representing the organisation on cross-community committees.
- Advising users of information systems, applications and Networks of their responsibilities.
- Creating, maintaining, giving guidance on and overseeing the implementation of IT Security.
- Ensuring that risks to IT systems are reduced to an acceptable level by applying security countermeasures identified following an assessment of the risk, or where risks are identified these are managed in line with the Trusts Risk Management Strategy and Policy.
- Ensure breaches of policy and recommended actions are reported in line with organisation's procedures.

6.5 Information Asset Owners (IAOs)

Information Asset Owners (IAOs) are senior members of staff (Service Leads) responsible for information risks within their service areas. They are responsible for providing assurance to the SIRO that information risks are recorded and that controls are in place to mitigate those risks. IAOs will work closely with the Trust's Information, Communication Technology Team, Information Governance Team and Information Security Manager to ensure that:

- Security of the Network used by their staff and, where appropriate, by third parties is consistent with legal and management requirements and obligations.

Uncontrolled when printed

- Their staff are made aware of their security responsibilities.
- Their staff have had suitable security training.
- An action plan and action outcome is developed in the event of a breach to the Trust's Networks and/or Information.

6.6 Information Asset Administrators (IAA's)

IAOs can appoint an IAA to support the delivery of information risk management responsibilities within their service areas. IAA's, where appointed should ensure that:

- Staff within their areas aware of the Trust's policies and procedures and their responsibilities for the secure use of the Trusts ICT systems.
- They recognise actual or potential security incidents and take steps to report & mitigate those risks.
- They consult with their IAOs on incident management and ensure that information asset registers are accurate and up to date.

6.7 All Remote Workers

All Remote workers agree:

- To be bound by the terms of this policy, ensuring care & compliance at all times;
- The proper use, care, maintenance and safekeeping of information assets & allocated device(s);
- To ensure that they return the mobile device(s) to their line manager or to the ICT Servicedesk when they leave the organisation;
- To ensure that they follow the process detailed in section 7.3 in the event that a device is lost or stolen;
- To ensure the appropriate use of mobile devices whilst conducting their work;
- To ensure that passwords are not stored with the device.
- To ensure that remote access VPN password is not stored with the device.
- To ensure that data kept on the mobile device is backed up into corporate systems.

Failure to backup data to corporate systems will result in unrecoverable data loss if the device storage fails.

Failure to comply with this policy will be investigated and might lead to disciplinary action being taken

7 Policy detail/Course of Action

7.1 Issue of Devices

Only portable or mobile devices approved by the Trust are permitted to access the network and systems.

Line managers or senior staff holding departmental budgets can request devices be assigned to staff for remote working. This request must be made in writing to the ICT Servicedesk (via email to iow.ict@nhs.net).

Uncontrolled when printed

- The line manager must provide budgetary sign-off for licences where existing devices are being deployed.
- The mobile registration form must be signed upon collection of remote working devices from ICT.
- All applications for remote access and mobile registration forms for devices for remote use are kept by ICT.

All equipment issued by the Trust remains the property of the Trust.

7.2 Digital Security

When taking digital images or audio recordings using portable devices it is important to consider your responsibilities regarding patient consent; the security of the image; professional responsibilities and legal obligations and ensuring that where appropriate that the image becomes part of the patient record to allow auditability of digital images or audio recordings taken.

All public sector organisations are now directed to ensure all digital information that is either person identifiable or otherwise sensitive, is encrypted to appropriate NHS standards. This mandate applies to both the storage of, and transfer of any such digitally held information. If you are concerned or unsure how to secure digital images or audio recordings in this way, please contact the ICT Servicedesk iow.ict@nhs.net for further guidance.

Please see **Appendix A** for Clinical photography guidelines.

7.3 Physical Security

Staff shall accept full responsibility for the security of any portable devices issued to them, taking all necessary precautions to avoid loss, theft or damage. In the event of loss, theft or damage, it must be reported immediately to your departments Information Asset Owner (IAO), The Information Governance Team, the ICT Servicedesk, and also via the Trusts Incident Reporting system DATIX (using the incident module).

In the event of the portable device having been stolen, the incident must also be reported to the police and a crime reference number obtained.

Staff working remotely must:

- Take all reasonable care to assess the risks in their given environment and take reasonable steps to prevent the theft or loss of portable devices. Do not leave portable devices unattended in a public place or in vehicles on view - secured out of sight in the boot is acceptable, provided that there is no risk from heat/sunlight. When transporting, ensure that the device is safely stowed out of sight e.g. in a case or bag.
- Take extra vigilance if using any portable computing device during journeys on public transport, or in public spaces to avoid the risk of theft of the device or unauthorised disclosure of the Trust's stored information by a third party "overlooking" content displayed on screen. There are security measures such as screen covers that ensure that items on screen can only be seen when viewed from a certain angle, which can be deployed to support this risk if travel is common to the role, staff should enquire through the ICT Servicedesk.
- Not leave the device unattended for any reason unless the session is "locked" and it is in a safe working place. If it is anticipated that the device is to be left unattended, it must be logged out and powered off in order to secure the device, if it is possible staff should take the device with them. E.g. it is acceptable to lock the device while

Uncontrolled when printed

taking a shower in your hotel room, but if leaving the room to go for a meal, the device must be powered off.

- It is not acceptable to lock the keyboard and leave the device unattended in a public place or conference/meeting area.
- Ensure that other 'non' authorised users are not given access to the device or the data it contains e.g. members of family, visitors etc.

Portable devices must be returned to the IT Servicedesk for a health check if requested.

7.4 Backups

Data stored on local drives (e.g. laptop hard disk, tablet device storage etc.) is vulnerable to loss or corruption. In addition, if data is saved to a local drive and the device is lost or stolen, then so is the data. Due to this it is highly important that only the minimum amount of data required is carried on mobile devices, to reduce the potential impacts of an unforeseen event. Master copies of documents should never be stored on portable devices unless being created remotely and even then only until the very first opportunity to move the master copy to the network drive. Where possible, only copies of information should be taken off-site.

7.5 Passwords, Passphrases and Pin Codes

Passwords are an integral part of the Access Control mechanisms which are enforced by the Operating System, (e.g. Microsoft Windows).

Passwords and/or PINs must not be written down unless it is in a secure place e.g. under contact in Outlook.

Passwords and/or PINs must not be communicated to another person under any circumstance.

7.6 Cyber Security

Unauthorised use of portable devices can be gained through the inappropriate application of technical means, e.g. through capturing data transmissions or guessing passwords on unattended devices.

Encrypting data, good use of passwords, dual factor authentication and secured wireless networks all help to counter opportunist technical attacks.

Some forms of attack are executed remotely, therefore care must be taken to ensure that all portable device anti-virus & anti-spyware software is regularly updated to protect against these types of attacks. Connecting to the Trust network regularly will ensure this happens.

On access file scanning is enabled within Trust anti-virus software, to help detect email messages containing malicious code, or infected files transferred from portable storage media.

7.7 User-provided Portable Devices

User provided mobile phones and tablets that are used to access the Trust environment will only do so with the consent of the user's line manager and ICT, and will require to be correctly licensed and that licensing paid for by the service budget holder.

The user is responsible for maintaining anti-virus and anti-malware software on the device, which will be a pre-requisite for successful connection. Also the user will be responsible for notifying ICT of loss or change to the device and liable for outcomes in the event that they do not follow the Information Governance rules around data handling and storage.

Uncontrolled when printed

8 Remote Working

8.1 Eavesdropping

Take all reasonable care not to be eavesdropped upon when talking in public places e.g. while chatting in café's, on the telephone, talking with colleagues etc.

8.2 Wireless Connections

It is important that only secured Wireless (Wi-Fi) connections are utilised. These connections are typically announced as, and secured by, WPA/WPA2.

The following connection types should be avoided

- **WEP** (wired equivalent privacy) secured – known to be insecure; easy to gain unauthorised access to the network.
- **Public Hotspots**- These should be avoided due to the uncertainty of the security of the provided network.
- **Certificate Errors** – If a certificate error is displayed upon connection, then your device should be disconnected immediately and an alternative Wireless access point found, as the security of the connection cannot be guaranteed.

8.3 The use of Portable Devices

Any portable devices used by staff MUST have encryption enabled if they store Trust information.

- Sensitive corporate and personal identifiable information MUST NOT be stored or transferred using any unencrypted USB Memory device.
- Non-sensitive or non-personal information may be stored and transferred using non-encrypted USB Memory devices. Whilst the security of data is greatly increase when using encrypted "USB Memory" devices it does not remove responsibility from the user who must exercise due care and attention at all times when using these devices.

Applications for Encrypted Memory Sticks should be made to the Information Governance Team or via your departments Information Asset Owner.

Where it is not possible to encrypt sensitive/personal information, the advice of the assigned Data Custodian and Information Governance Team is to be sought and, where no solution can be found, the risk is to be articulated to SIRO for their consideration and decision.

Where available, only ICT approved encryption products are to be utilised to secure sensitive/personal information. Where no such product exists, the advice of the assigned Data Custodian and the Information Governance Team is to be sought in all cases.

Portable devices should only be used to transport confidential or sensitive information when other more secure methods are not available. Information must not be stored permanently on portable devices. Always transfer documents back to their normal network storage area as soon as possible. Failure to do so may result in problems with version control or loss of information if the portable device is lost or corrupted.

Staff must ensure that any suspected or actual breaches of security are reported to your departments Information Asset Owner (IAO), The Information Governance Team, the ICT Servicedesk, and also via the Trusts Incident Reporting system DATIX (using the incident module).

Uncontrolled when printed

8.4 Information held on the Organisation's Portable Devices

Confidential information may only be held on the organisation's portable devices with the permission from the assigned Information Asset Owner (IAO). This should be recorded on a Service Information Asset Register and an updated copy sent to the Information Governance Team.

Information must be virus checked before transferring onto the organisations computers. This will be done automatically for information that is sent via email.

8.5 Use of Portable Devices by External Visitors

External visitors (lecturers, contractors, company representatives, etc.) may only connect portable devices, including USB sticks and laptops, to Trust assets where authorisation has been granted following consultation with the IT Servicedesk who will ensure that the device is virus- scanned before any documents are opened.

9 Mobile Telephony Devices

9.1 Issue of Smart and Mobile Devices

Only mobile devices supplied by the Trust will be permitted to access the corporate network or Trust data.

9.2 Use of Mobile Devices

It is important that the Trust demonstrates value for money in the use of mobile devices. Staff must provide assurance that the mobile devices are used appropriately at all times.

Trust staff should not use any mobile device whilst in control of a vehicle unless they are using an appropriate hands free kit.

If a member of staff is given a device in order that they are contactable then their mobile device should be on at all times during business or 'on-call' hours, except when driving or when the user deems it inappropriate due to work reasons for example when in a meeting.

All Trust staff should take all reasonable measures to prevent loss, damage or theft.

10 Return of Devices

Any person leaving the organisation must return all portable and mobile devices to their line manager or the ICT Department. Any person no longer requiring the use of a Trust issued portable or mobile device must return it to their line manager or the ICT Department.

Line managers are responsible for the mobile devices used by their staff and for ensuring that any member of their staff using a mobile device has returned it before they leave the employ of the Trust.

All portable media containing Trust information must be returned to the ICT Servicedesk for retention or appropriate destruction.

11 Working with Portable Display Screen Equipment

The Trust has a duty to ensure that the Display Screen Equipment (DSE) which the Trust owns or uses, is constructed, operated and maintained in a manner which ensures the safety of its operatives.

Uncontrolled when printed

Knowledge of the minimum Health and Safety requirements for work with DSE is regarded as a basic requirement for all staff employed defined as a “user” by the Trust. This requirement is achieved by the manager responsible ensuring that those persons receive appropriate information and guidance.

DSE guidance, applies to staff working remotely as well as when working in their conventional workplace.

If a laptop is used for prolonged periods, an attempt should be made to find a sensible compromise that retains the benefits of mobile working but removes the risk of causing harm to staff.

For prolonged use of a laptop in a fixed location, such as an office where the user is constantly present and using the laptop, the provision of docking stations should be considered because these enable full size, good quality display screens and full size keyboards and mouse to be used.

A docking station allows the laptop to be used as a portable device in the normal manner, while, when in the office, the user has access to a full size keyboard and screen[s], effectively turning the laptop into a workstation. This will offer the user the flexibility inherent in using a laptop but remove problems that can occur such as back, shoulder, neck and wrist pains.

All users of display screen equipment must carry out a DSE level 1 risk assessment on the safe use of the device and complete the DSE training on a frequency as per their individual Pro4 training profile. See link:

http://intranet.iow.nhs.uk/Home/Corporate/Health-Safety-and-Security/Back-Care-Advisory-Team/Referrals-and-Risk-Assessments

12 Laptop Handling

It is Trust policy that laptops will be used according to the following guidelines:

- When carrying to and from your place of work don’t overload your laptop bag and distribute the weight as evenly as possible
- Wherever possible the laptop should be positioned on a firm surface, which is the right height for its use
- You are advised to angle the computer screen to minimise reflections
- Ensure that you have enough space in front of the laptop to rest your wrists and forearms whilst working minimum 50mm(2 inches)
- Keep the use of a laptop to a minimum and take regular breaks, at least ten minutes in every hour
- If any discomfort is experienced whilst using a laptop, it must be reported immediately to their Manager/Supervisor.

It is best to avoid using a laptop and other portables if full sized equipment is available

Uncontrolled when printed

13 Related Policies

Lone Worker Policy

Health and Safety Policy

Agile Working and Space Utilisation Policy

14 Consultation

This policy has been circulated to the ICT and Information Governance Team for comment prior to final approval and ratification.

15 Training

This policy does not have a mandatory training requirement. However, further guidance or clarification will be provided by the Information Security Manager upon request.

Users should also be aware of Health & Safety 'Display Screen Equipment' requirements. There is an e-learning module available on Training Tracker. If you do not have access to Training Tracker, please contact the Development and Training team on ext.: 5409

16 Monitoring Compliance and Effectiveness

Information Asset Owners are required to undertake spot checks to ensure compliance with this policy.

17 Appendices

Appendix A - Clinical photography

Appendix B - Equality Impact Assessment (EIA) Screening Tool

Appendix C - Financial and Resourcing Impact Assessment on Policy Implementation

Uncontrolled when printed

Appendix A

Clinical photography

In 2013, the General Medical Council issued guidance on the making and using visual and audio recordings of patients, covering the principles of maintaining privacy and dignity and a patient's right to make or participate in decisions that affect them. The guidance covers the issues of consent, storage and uses of the images. Acknowledging that a clinical photograph is often a useful part of a clinical record and the Trust does not have a Medical Imaging Department, in accordance with the GMC guidance, the following practice will be adopted.

- In clinical areas and services where photographs are taken on a regular basis, digital cameras will be provided. Staff will be trained in their use and the security of images. The cameras will be recorded on the appropriate Information Asset Register.

- Images will only be taken with appropriate consent. If circumstances permit, this will be with written consent recorded on a "Consent to Photography" Form. If the patient is unable to give written consent, implied consent will be recorded in the clinical record.

- The Consent to Photography Form allows for three levels of consent:

    - for Health Record use only
    - for clinical teaching purposes
    - for use in medical publication

- All images taken of patients on the hospital site or in the wider community setting constitute a part of the patient's record irrespective of who has taken the photograph or what device it has been taken on.

- Images and scanned copies of the consent form will be downloaded on to a central password-protected drive and the original image on the camera deleted.

- Images that are not paired up with an appropriate consent form within one month of the image being taken must be deleted.

- When patients are transferred to other Trusts, it may be necessary to send medical images to their clinical teams. Clinical images should only be sent by email using the nhs.net e-mail service.

- Various diagnostic procedures incorporate cameras which are used to record findings in patient examinations. These include:

    - Colposcopy
    - Endoscopy
    - Fluorescein angiography
    - Pathology / laboratory microscopes

- The use of such cameras is permissible and therefore they are excluded from the policy, provided that they not be used to take pictures from which a patient could be identified

Uncontrolled when printed

It is **not** permitted to make clinical photography recordings on any other recording device, in particular on mobile phones and other mobile devices.

It is **not** permitted for clinicians to keep personal/private collections of any such patient recordings which are not sufficiently consented nor documented.

Uncontrolled when printed

Appendix B

Equality Impact Assessment (EIA) Screening Tool

Document Title:	Remote Working and Portable Devices Policy
Purpose of document	Set out expectations in relation to remote working.
Target Audience	All staff who work remotely or use portable devices.
Person or Committee undertaken the Equality Impact Assessment	Carl Moreira-Smith

1. To be completed and attached to all procedural/policy documents created within individual services.

2. Does the document have, or have the potential to deliver differential outcomes or affect in an adverse way any of the groups listed below?

If no confirm underneath in relevant section the data and/or research which provides evidence e.g. JSNA, Workforce Profile, Quality Improvement Framework, Commissioning Intentions, etc.

If yes please detail underneath in relevant section and provide priority rating and determine if full EIA is required.

		Positive Impact	Negative Impact	Reasons
Gender	Men	N/A	N/A	
	Women	N/A	N/A	
Race	Asian or Asian British People	N/A	N/A	
	Black or Black British People	N/A	N/A	

Uncontrolled when printed

	Chinese people	N/A	N/A	
	People of Mixed Race	N/A	N/A	
	White people (including Irish people)	N/A	N/A	
	People with Physical Disabilities, Learning Disabilities or Mental Health Issues	N/A	N/A	
Sexual Orientation	Transgender	N/A	N/A	
	Lesbian, Gay men and bisexual	N/A	N/A	
Age	Children	N/A	N/A	
	Older People (60+)	N/A	N/A	
	Younger People (17 to 25 yrs.)	N/A	N/A	
Faith Group		N/A	N/A	
Pregnancy & Maternity		N/A	N/A	
Equal Opportunities and/or improved relations		N/A	N/A	

Uncontrolled when printed

Notes:

Faith groups cover a wide range of groupings, the most common of which are Buddhist, Christian, Hindus, Jews, Muslims and Sikhs. Consider faith categories individually and collectively when considering positive and negative impacts.

The categories used in the race section refer to those used in the 2001 Census. Consideration should be given to the specific communities within the broad categories such

as Bangladeshi people and the needs of other communities that do not appear as separate categories in the Census, for example, Polish.

3. Level of Impact

If you have indicated that there is a negative impact, is that impact:			
		YES	NO
Legal (it is not discriminatory under anti-discriminatory law)			
Intended			

If the negative impact is possibly discriminatory and not intended and/or of high impact then please complete a thorough assessment after completing the rest of this form.

3.1 Could you minimise or remove any negative impact that is of low significance? Explain how below:	
3.2 Could you improve the strategy, function or policy positive impact? Explain how below:	
3.3 If there is no evidence that this strategy, function or policy promotes equality of opportunity or improves relations – could it be adapted so it does? How? If not why not?	
Scheduled for Full Impact Assessment	Date:
Name of persons/group completing the full assessment.	Carl Moreira-Smith
Date Initial Screening completed	19/03/2016

Uncontrolled when printed

Appendix C

Financial and Resourcing Impact Assessment on Policy Implementation

NB this form must be completed where the introduction of this policy will have either a positive or negative impact on resources. Therefore this form should not be completed where the resources are already deployed and the introduction of this policy will have no further resourcing impact.

Document title	**Remote working and Portable Devices Policy** (No change in resourcing requirements)

Totals	WTE	Recurring £	Non-Recurring £
Manpower Costs	0	0	0
Training Staff	0	0	0
Equipment & Provision of resources	0	0	0

Summary of Impact:
Risk Management Issues:
Benefits / Savings to the organisation: Equality Impact Assessment

- Has this been appropriately carried out? YES/NO
- Are there any reported equality issues? YES/NO

If "YES" please specify:
Use additional sheets if necessary

Please include all associated costs where an impact on implementing this policy has been considered. A checklist is included for guidance but is not comprehensive so please ensure you have thought through the impact on staffing, training and equipment carefully and that ALL aspects are covered.

Manpower	WTE	Recurring £	Non-Recurring £
Operational running costs			
Totals:	0	0	0

Staff Training Impact	Recurring £	Non-Recurring £
Totals:	0	0

Equipment and Provision of Resources	Recurring £ *	Non-Recurring £ *
Accommodation / facilities needed	0	0
Building alterations (extensions/new)	0	0
IT Hardware / software / licences	0	0
Medical equipment	0	0

Uncontrolled when printed

Stationery / publicity	0	0
Travel costs	0	0
Utilities e.g. telephones	0	0
Process change	0	0
Rolling replacement of equipment	0	0
Equipment maintenance	0	0
Marketing – booklets/posters/handouts, etc.	0	0
Totals:	0	0

- Capital implications £5,000 with life expectancy of more than one year.

Funding /costs checked & agreed by finance:	
Signature & date of financial accountant:	
Funding / costs have been agreed and are in place:	
Signature of appropriate Executive or Associate Director:	

Uncontrolled when printed