C:\Documents and Settings\helen.sanderson\Local Settings\Temporary Internet Files\Content.Outlook\6UXB7KOT\NLlogo.png

**Mobile Working Policy and Guidelines**

|  |  |
| --- | --- |
| **Authorship:** | Information Governance Team |
| **Committee Approved:** | Integrated Audit & Governance Committee |
| **Approved date:** | 6 January 2021 |
| **Review Date:** | 2 Years from approval date |
| **Equality Impact Assessment**  **Sustainability Impact Assessment**  **Data Protection Impact Assessment**  **Target Audience:** | **Screening**  **Completed**  **Not Required**  **All staff** |
| **Policy Reference No:** | **N/A** |
| **Version Number:** | **2.0** |

**The on-line version is the only version that is maintained. Any printed copies should, therefore, be viewed as ‘uncontrolled’ and as such may not necessarily contain the latest updates and amendments.**

**POLICY AMENDMENTS**

Amendments to the Policy will be issued from time to time. A new amendment history will

be issued with each change.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **New Version Number** | **Issued by** | **Nature of Amendment** | **Approved by & Date** | **Date on Intranet** |
| 1 | C Wallace | Document created |  |  |
| 1.1 | M Culling | Amendments to reflect the Data Protection Act 1998 (expected to be superseded by a Data Protection Act 2017 incorporating the requirements of the General Data Protection Regulation). |  |  |
| 2.0 | H Gillingwater | GDPR  Updates to Bribery Act  Reasonable adjustments – disability / mental wellbeing  Communication Tools  Responding to Information Requests | IA&GC 6 Jan 2021 |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**CONTENTS**

|  |  |  |
| --- | --- | --- |
|  |  | **Page** |
| **1** | **Introduction** | 4 - 5 |
|  |  |  |
| **2**  **3** | **Engagement**  **Impact Analyses**  **3.1 Equality**  **3.2 Sustainability**  **3.3 GDPR**  **3.4 Bribery Act 2010** | 5  5 |
| **4** | **Scope** | 7 |
| **5** | **Policy Purpose and Aims** | 7 |
| **6**  **7**  **8** | **Roles / Responsibilities / Duties**  **Implementation**  **Training and Awareness** | 11  11  11 |
| **9** | **Monitoring and Audit** | 11 |
| **10** | **Policy Review** | 11 |
| **11** | **References** | 12 |
| **13** | **Appendices – Appendix 1 – Equality Impact Analysis**  **Appendix 2 – Sustainability Impact Assessment** | 13  23 |

**1 INTRODUCTION**

Mobile working allows North Lincolnshire Clinical Commissioning Group (thereby known as the CCG) to make cost savings while ensure that staff remains interconnected and able to work from almost anywhere.

The CCG has therefore adopted three levels of agile working with all staff falling into one of these categories:-

**Fixed**

Fixed workers will:

* Spend most of their time working at one fixed site.
* May have specific, individual equipment / furniture needs to be able to perform their role and work effectively
* Seldom away from their desk except for meetings with colleagues in the office
* Do not need to work from non-CCG sites.

**Equipment**

* + Use of Fixed Phone on Desk or mobile phone
  + Use of Fixed Desktop Computer, or laptop which can sit in a docking station on the desk.

**Flexible**

Flexible workers will:

* + Have the ability to effectively deliver their work utilising space across a range of CCG buildings or locations where Wi-Fi is available
  + May also spend time attending meetings or working at other Trust, partner, or client sites
  + Spend a large percentage of their time attending meetings/other similar events and/or delivering business across a range of internal and external sites
  + Have the option and ability to work from any site or location where Wi-Fi is enabled

**Equipment**

* + Standard mobile phone
  + Laptop computer with standard carry case
  + Laptop peripherals - ie., plug in mouse, keyboard, screen if required
  + External network access

**Flexible Plus**

Flexible Plus workers will:

* + Have the ability to effectively deliver their work utilising space across a range of CCG buildings or locations where Wi-Fi is available
  + Spend most of their time working 'on the move'; accessing information or conducting community/client/patient based activities, working across a range of operational / business sites and coming into offices only for meetings or other specific events
  + Have the option and ability to work from any site or location regardless of whether there is Wi-Fi.

**Equipment**

* + Smart Phone
  + Laptop computer with standard carry case
  + External network access
  + 3G dongle (SIM) - One off initial cost as well as monthly charge

While there are differences between these staffing groups any CCG member of staff can, at the discretion of their line manager request remote access. Willful or negligent disregard of this policy will be investigated and may be treated as a disciplinary offence.

**2 ENGAGEMENT**

This policy has been developed based on the knowledge and experience of the Information Governance team. It is derived from a number of national codes and policies which are considered as best practice and have been used across many public sector organisations.

**3 IMPACT ANALYSES**

**3.1 Equality**

An equality impact screening analysis has been carried out on this policy and is attached at Appendix 1.

As a result of performing the analysis, the policy, project or function does not appear to have any adverse effects on people who share *Protected Characteristics* and no further actions are recommended at this stage.

**3.2 Sustainability**

A sustainability assessment has been completed and is attached at Appendix 2. The assessment does not identify and benefits or negative effects of implementing this document.

**3.3 General Data Protection Regulation (GDPR)**

The CCG is committed to ensuring that all personal information is managed in accordance with current data protection legislation, professional codes of practice and records management and confidentiality guidance. More detailed information can be found in the CCGs Data Protection and Confidentiality and related policies and procedures.

If you are commissioning a project or undertaking work that requires the processing of personal data you must complete a Data Protection Impact Assessment. Please see the CCG’s Data Protection Impact Assessment Procedure and Data Protection by Design & Default procedure available on the website for guidance.

**3.4 Bribery Act 2010**

The Bribery Act is particularly relevant to this policy.  North Lincolnshire CCG has a responsibility to ensure that all staff are made aware of their duties and responsibilities arising from the Bribery Act 2010.  Under the Bribery Act 2010 there are four criminal offences:

•           Bribing or offering to bribe another person (Section 1)

•           Requesting, agreeing to receive or accepting a bribe (Section 2);

•           Bribing, or offering to bribe, a foreign public official (Section 6);

•           Failing to prevent bribery (Section 7).

These offences can be committed directly or by and through a third person and, in many cases, it does not matter whether the person knows or believes that the performance of the function or activity is improper.

It should be noted that there need not be any actual giving and receiving for financial or other advantage to be gained, to commit an offence.

All individuals should be aware that in committing an act of bribery they may be subject to a penalty of up to 10 years imprisonment, an unlimited fine, or both.  They may also expose the organisation to a conviction punishable with an unlimited fine because the organisation may be liable where a person associated with it commits an act of bribery.

Individuals should also be aware that a breach of this Act renders them liable to disciplinary action by NLCCG, whether or not the breach leads to prosecution.  Where a material breach is found to have occurred, the likely sanction will be loss of employment and pension rights.

It is the duty of every member of staff to speak up about any genuine concerns in relation to criminal activity, breach of a legal obligation, miscarriage of justice, danger to health and safety or the environment and the suspected cover up of any of these in the workplace.  To raise any suspicions of bribery and/or corruption please contact the Chief Finance Officer.  Staff may also contact the Local Counter Fraud Specialist (LCFS) at – Audit Yorkshire, 01482 866800 email:  [nikki.cooper1@nhs.net](mailto:nikki.cooper1@nhs.net)  or mobile 07872 988939.

The LCFS or Chief Finance Officer should be the contact for any suspicions of fraud. The LCFS will inform the Chief Finance Officer if the suspicion seems well founded and will conduct a thorough investigation.  Concerns may also be discussed with the Chief Finance Officer or the Audit & Integrated Governance Committee Chair.

If staff prefer, they may call the NHS Fraud & Corruption Reporting Line on 0800 028 40 60 between 8am-6pm Monday-Friday or report online at [www.reportnhsfraud.nhs.uk](http://www.reportnhsfraud.nhs.uk).  This would be the suggested contact if there is a concern that the LCFS or the Chief Finance Officer themselves may be implicated in suspected fraud, bribery or corruption.

**4 SCOPE**

This policy applies to all staff, CCG Governing Body Members, temporary staff, seconded staff, contractors and others undertaking work on behalf of the CCG etc who are permitted to use equipment of the organisation at home or other place of work, or who may use their own personal or third-party computing resources to connect to networked services of the organisation.

Such equipment includes, but is not limited to:

* + Laptop computers
  + PDA’s or other hand-held devices
  + Smartphones

**5 POLICY PURPOSE & AIMS**

# Requesting Remote Access

Remote access can be requested for any existing staff member or can be requested as part of the setup of a new account.

Requests for remote access should be directed to the IT Service Desk and should originate from the Line Manager of the individual requiring the access. Once logged the IT department will process the request.

# Guidelines

### Health and Safety

In principle the same considerations should be given to the remote working environment as to the working in the normal office environment. You should ensure your immediate working environment is free of trip hazards, electrical connections are safe etc. It is the employee’s duty to always consider the risks surrounding their working environment, and take steps where appropriate. If staff require reasonable adjustments to their remote working due to a disability, this should be raised with your line manager. Line managers should respond to requests promptly and where necessary refer to the Occupational Health service. The CCG is committed to supporting the mental health and wellbeing of employees who are working remotely. The HR team can provide employees and managers with links to appropriate resources.

### Theft

A laptop or other mobile device is a prime target for theft, as they are small, expensive, and generally easy to dispose of.

* + You should never leave devices unattended
  + You should never leave devices on view in a motor vehicle. Ideally always take equipment with you, however if you have no choice but leave equipment in a vehicle ensure it is locked in the boot and not visible.
  + Such equipment can also be an issue in a high-risk environment, an individual carrying what is clearly a laptop bag is a prime target, so wherever possible ensure you are aware of the risks surrounding you. The use of rucksacks or other non-obvious bags to carry a laptop may be advisable in some circumstances.

### Privacy and Information Governance

The rules applying to information governance in the workplace similarly apply to remote working using IT equipment. You should take all steps that are necessary to ensure that information is not disclosed.

In particular, ensure that you are not overlooked when using any system. If you are in a public place, then find a location where it is not possible for anyone to see over your shoulder. CCTV is also prevalent in today’s world, particularly in the UK, so it is advisable to be aware of any cameras overlooking your point of work that might be able to see information on your screen. Privacy screens are available on request from the Information Governance Team. These screens fit over the laptop’s monitor and reduce the viewing angle of the screen so that it is only visible when looked at squarely to the screen.

The risks associated with a breach of the information governance rules are:

* + accidental breach of patient confidentiality
  + disclosure of other sensitive data of the organisation to unauthorised individuals
  + loss or damage to critical business data
  + damage to the organisation’s infrastructure and e-services through spread of un-trapped malicious code such as viruses
  + the creation of a hacking opportunity through an unauthorised internet access point
  + misuse of data through uncontrolled use of removable media such as digital memory sticks and other media
  + other operational or reputational damage

Any staff member using alternative communication tools for business purposes must follow the below rules. This applies to any information that is created or received as part of a CCG task, be that communication between teams on work matters, contacting your manager or service delivery.

Before use please ensure:

* you only use alternative communication tools after consulting with your line manager or if in doubt the Information Governance team.
* alternative communication tools are only used where the CCG recommended options are not available and it is critical to service delivery.

While using please ensure:

* Any correspondence created for business purposes is kept separate from any personal conversations that you have. You can do this by creating a new group and adding any relevant officers or partners to it.
* Where possible you should avoid using any alternative to send personal or sensitive data. However, should this be a necessity you will be allowed to do so using secure domains only but you should ensure that you provide only the minimum amount of information needed.

After using please ensure:

* If a conversation contains any decision-making, employee or patient data it should be exported from application and uploaded to the relevant filing system on the Network.
* Once a conversation is no longer required, all parties in the conversation must clear chat / clear messages to remove all versions of it from every device.

**Responding to Information Requests**

In carrying out CCG business please be aware that any information, even which stored on external applications, is subject to statutory information requests that the CCG may receive such as Freedom of Information requests or Subject Access Requests. This includes:

* any messages between you and your staff,
* any correspondence you created from a personal mobile number for a work purpose.

### Use of Public Computers or Publicly Available Networks

Great care should be taken using publicly-available equipment, such as an Internet café or hotel PC.

* Ensure that controls exist such that access is controlled. Avoid ‘free use’ facilities where someone could just walk up and use the device. Most Internet cafés have systems which issue a ‘one time’ password, which allows access only for a prescribed period of time. If this is the case, also ensure you have allowed sufficient time at the end of your period for ‘clearing down’ any information you may leave behind.
* If you have any doubts that the device is not properly secured (e.g. does not appear to have any anti-virus software installed), then do not use such equipment
* Facilities will be limited when using public equipment, generally to using Outlook Web Access for reviewing and sending emails
* When you have finished, before closing Internet Explorer make sure you clear the browsing history (depending on the version of Explorer, generally Tools->Internet Options->Clear History), and also remove temporary files (generally Tools->Internet Options->Delete Files). Ensure that the ‘Delete All Offline Content’ box is ticked.
* If you are using a publicly available network or ‘hotspot’, make sure that is a secured network (i.e. requires you to put in a pass key). If it is unsecured, do NOT use it, as any data passing between your PC and the network can be captured.

### Storage of Data

* + You should never store any data on a non-CCG supplied device. This applies to home PCs or PCs used in hotels or Internet cafes
  + Do not store data on diskette, CD or other similar storage device

### Memory Sticks

* + If data does need to be stored, then use ONLY a CCG-supplied encrypted memory stick .These are available by request from the IMT department, subject to a manager’s approval.
  + Each encrypted memory stick has a unique serial number and password. Information cannot be accessed unless the password is known. Do not write the password down, and if it needs to be shared with other member of staff, inform the other individual verbally.
  + Memory sticks should not be labelled with any sort of NHS identification. They are secure, and without the password they are useless. It should not be possible to determine that the memory stick is the property of the NHS.

### Data and Device Encryption

* + All mobile devices MUST be equipped with encryption software
  + Laptops supplied by the CCG will have this pre-installed
  + Other devices, such as Smartphones should also be encrypted. Any device supplied by the IT department will already be encrypted, however devices ordered directly from the manufacturer or distributor may not. If you are in any doubt, please contact the IT Service Desk. As a guide an encrypted device will require a password at power-on, whereas an unencrypted one will not.

### Identifying Labels

Remote devices should not carry any identifying labels which immediately indicate they are NHS property. You should make a note of any serial or asset numbers on the devices you have been issued with. These will be required when any loss or theft is reported.

You should also not carry any other identifying paperwork with the laptop, which identifies it as an NHS machine. If possible, always carry paperwork separate from the laptop.

### Confidentiality

As the NHS net is a closed network and access from other networks is very strictly controlled, staff should be aware that the greatest risk to security is posed by those within the network, and not by outsiders. The NHS net cannot protect systems from the actions, legitimate or otherwise, of other users. Therefore, all staff should be especially aware of the CCG's security and Internet and E-mail policies. Staff should also ensure that they are meeting the requirements of the Data Protection Acts 2018 incorporating the requirements of the General Data Protection Regulation, and at all times behave in accordance with UK law.

Staff working on CCG or associated organisations material/work must at all times take extreme care to ensure that confidentiality is maintained and follow appropriate Trust policies.

Sensitive and confidential material must not be taken out of the conventional workplace without prior approval by a member of staff's line manager

# Incident Reporting

Any incident which has or you believe may have compromised the integrity of the CCG information systems through remote working should be reported through the existing incident management process. This would include, but is not limited to:-

* Loss or theft of any supplied equipment
* Accidental loss or disclosure of information such as login names, passwords or PIN numbers that could cause the CCG information systems to be compromised.
* Loss or disclosure of any other confidential information.
* Loss or theft of equipment should be reported to the IT Service Desk immediately. This will ensure that steps can be taken to prevent the equipment being used on the CCG network, and in some cases allow the equipment to be disabled remotely.

**6 Roles / Responsibilities / DUTIES**

Review and Maintenance:- Senior Information Governance Specialist

Approval:- Audit & Integrated Governance Committee

Local adoption:- Line managers (in scope)

Compliance:- All staff and contractors (in scope)

Monitoring:- Service Desk, System Engineers, Audit

**7 IMPLEMENTATION**

The policy will be disseminated by being made available on the intranet and highlighted to staff through newsletters, team briefings and by managers.

*‘Breaches of this policy may be investigated and may result in the matter being treated as a disciplinary offence under the CCG’s disciplinary procedure’.*

**8 TRAINING & AWARENESS**

Staff will be made aware of the policy via the website.

**9 MONITORING & AUDIT**

Adherence to this policy will be monitored through the incident reporting system and also through standard IT monitoring KPI’s. Where there is a suspected issue an investigation will be performed and staff found to be breach guidance may be subject to disciplinary actions.

**10 POLICY REVIEW**

This policy will be reviewed in 2 years. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation/guidance, as instructed by the senior manager responsible for this policy.

**11 REFERENCES**

This policy should be used in conjunction with the following policies:

Acceptable Computer Use Policy

Data Protection and Confidentiality Policy

# 

**Appendix 1**

|  |  |
| --- | --- |
| 1. **Equality Impact Analysis** | |
| **Policy / Project / Function:** | Mobile Working Policy and Guidelines |
| **Date of Analysis:** | 18/11/2020 |
| **This Equality Impact Analysis was completed by:**  **(Name and Department**) | H Gillingwater – Senior Information Governance Specialist |
| **What are the aims and intended effects of this policy, project or**  **function ?** | This Policy defines the types of worker .e.g. fix desk or flexible and provides guidance to staff who work remotely. |
| **Please list any other policies that are related to or referred to as part of this analysis?** | Email Policy  Data Protection & Confidentiality Policy |
| **Who does the policy, project or function affect ?**    Please Tick ✔ | Employees    Service Users    Members of the Public  Other (List Below)  Any users of CCG IT equipment |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1. **Equality Impact Analysis: Screening** | | | | |  |
|  | Could this policy have a positive impact on… | | Could this policy have a negative impact on… | | Is there any evidence which already exists from previous (e.g. from previous engagement) to evidence this impact |
|  | Yes | No | Yes | No |  |
| **Race** |  |  |  |  |  |
| **Age** |  |  |  |  |  |
| **Sexual Orientation** |  |  |  |  |  |
| **Disabled People** |  |  |  |  |  |
| **Gender** |  |  |  |  |  |
| **Transgender People** |  |  |  |  |  |
| **Pregnancy and Maternity** |  |  |  |  |  |
| **Marital Status** |  |  |  |  |  |
| **Religion and Belief** |  |  |  |  |  |
| **Reasoning** |  | | | | |
| **If there is no positive or negative impact on any of the Nine Protected Characteristics go to Section 7** | | | | | |

|  |  |
| --- | --- |
| 1. **Equality Impact Analysis: Local Profile Data** | |
| **Local Profile/Demography of the Groups affected** (population figures) | |
| **General** |  |
| **Age** |  |
| **Race** |  |
| **Sex** |  |
| **Gender reassignment** |  |
| **Disability** |  |
| **Sexual Orientation** |  |
| **Religion, faith and belief** |  |
| **Marriage and civil partnership** |  |
| **Pregnancy and maternity** |  |

|  |  |
| --- | --- |
| 1. **Equality Impact Analysis: Equality Data Available** | |
| **Is any Equality Data available relating to the use or implementation of this policy, project or function?**  Equality data is internal or external information that may indicate how the activity being analysed can affect different groups of people who share the nine *Protected Characteristics* – referred to hereafter as *‘Equality Groups’.*  Examples of *Equality Data* include: (this list is not definitive)   1. Application success rates *Equality Groups* 2. Complaints by *Equality Groups* 3. Service usage and withdrawal of services by *Equality Groups* 4. Grievances or decisions upheld and dismissed by *Equality Groups* 5. *Previous EIAs* | Yes    No  Where you have answered yes, please incorporate this data when performing the *Equality Impact Assessment Test* (the next section of this document). |
| **List any Consultation e.g. with employees, service users, Unions or members of the public that has taken place in the development or implementation of this policy, project or function** |  |
| **Promoting Inclusivity**  **How does the project, service or function contribute towards our aims of eliminating discrimination and promoting equality and diversity within our organisation** |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. **Equality Impact Analysis: Assessment Test** | | | | |
| **What impact will the implementation of this policy, project or function have on employees, service**  **users or other people who share characteristics protected by *The Equality Act 2010* ?** | | | | |
| **Protected**  **Characteristic:** | **No**  **Impact:** | **Positive**  **Impact:** | **Negative**  **Impact:** | **Evidence of impact and if applicable, justification**  **where a *Genuine Determining Reason* exists** |
| **Gender**  (Men and Women) | X |  |  |  |
| **Race**  (All Racial Groups) | X |  |  |  |
| **Disability**  (Mental and Physical) | X |  |  |  |
| **Religion or Belief** | X |  |  |  |
| **Sexual Orientation**  **(Heterosexual, Homosexual and Bisexual)** | X |  |  |  |
| **What impact will the implementation of this policy, project or function have on employees, service**  **users or other people who share characteristics protected by *The Equality Act 2010* ?** | | | | |
| **Protected**  **Characteristic:** | **No**  **Impact:** | **Positive**  **Impact:** | **Negative**  **Impact:** | **Evidence of impact and if applicable, justification**  **where a *Genuine Determining Reason* exists** |
| **Pregnancy and Maternity** | X |  |  |  |
| **Transgender** | X |  |  |  |
| **Marital Status** | X |  |  |  |
| **Age** | X |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. **Action Planning** | | | | |
| **As a result of performing this analysis, what actions are proposed to remove or reduce any risks of adverse outcomes identified on employees, service users or other people who share characteristics protected by *The Equality Act 2010* ?** | | | | |
| **Identified Risk:** | **Recommended Actions:** | **Responsible Lead:** | **Completion Date:** | **Review Date:** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. **Equality Impact Analysis Findings** | | | | |
| **Analysis Rating:** | * Red | * Red/Amber | * Amber | * **Green** |

|  |  |  |  |
| --- | --- | --- | --- |
|  | | Actions | Wording for Policy / Project / Function |
| **Red**  **Stop and remove the policy** | **Red:** As a result of performing the analysis, it is evident that a risk of discrimination exists (direct, indirect, unintentional or otherwise) to one or more of the nine groups of people who share *Protected Characteristics.* It is recommended that the use of the policy be suspended until further work or analysis is performed. | **Remove the policy**  Complete the action plan above to identify the areas of discrimination and the work or actions which needs to be carried out to minimise the risk of discrimination. | No wording needed as policy is being removed |
| **Red Amber**  **Continue the policy** | As a result of performing the analysis, it is evident that a risk of discrimination exists (direct, indirect, unintentional or otherwise) to one or more of the nine groups of people who share *Protected Characteristics.* However, a genuine determining reason may exist that could legitimise or justify the use of this policy and further professional advice should be taken. | **The policy can be published with the EIA**  List the justification of the discrimination and source the evidence (i.e. clinical need as advised by NICE).  Consider if there are any potential actions which would reduce the risk of discrimination.  Another EIA must be completed if the policy is changed, reviewed or if further discrimination is identified at a later date. | As a result of performing the analysis, it is evident that a risk of discrimination exists (direct, indirect, unintentional or otherwise) to one or more of the nine groups of people who share *Protected Characteristics.* However, a genuine determining reason exists which justifies the use of this policy and further professional advice.  ***[Insert what the discrimination is and the justification of the discrimination plus any actions which could help what reduce the risk]*** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Equality Impact Findings (continued):** | | | |
|  | | Actions | Wording for Policy / Project / Function |
| **Amber**  **Adjust the Policy** | As a result of performing the analysis, it is evident that a risk of discrimination (as described above) exists and this risk may be removed or reduced by implementing the actions detailed within the *Action Planning s*ection of this document. | **The policy can be published with the EIA**  The policy can still be published but the Action Plan must be monitored to ensure that work is being carried out to remove or reduce the discrimination.  Any changes identified and made to the service/policy/ strategy etc. should be included in the policy.  Another EIA must be completed if the policy is changed, reviewed or if further discrimination is identified at a later date. | As a result of performing the analysis, it is evident that a risk of discrimination (as described above) exists and this risk may be removed or reduced by implementing the actions detailed within the *Action Planning s*ection of this document.  ***[Insert what the discrimination is and what work will be carried out to reduce/eliminate the risk]*** |
| **Green**  **No major change** | As a result of performing the analysis, the policy, project or function does not appear to have any adverse effects on people who share *Protected Characteristics* and no further actions are recommended at this stage. | **The policy can be published with the EIA**  Another EIA must be completed if the policy is changed, reviewed or if any discrimination is identified at a later date | As a result of performing the analysis, the policy, project or function does not appear to have any adverse effects on people who share *Protected Characteristics* and no further actions are recommended at this stage. |

|  |  |
| --- | --- |
| **Brief Summary/Further comments** |  |

|  |  |  |
| --- | --- | --- |
| **Approved By** | | |
| Job Title: | Name: | Date: |
|  |  |  |

**Appendix 2**

**SUSTAINABILITY IMPACT ASSESSMENT**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Policy / Report / Service Plan / Project Title:** | | | | |
| **Theme (Potential impacts of the activity)** | **Positive**  **Impact** | **Negative**  **Impact** | **No specific**  **impact** | **What will the impact be? If the impact is negative, how can it be mitigated? (action)** |
| Reduce Carbon Emission from buildings by 12.5% by 2010-11 then 30% by 2020 |  |  | X |  |
| New builds and refurbishments over £2million (capital costs) comply with BREEAM Healthcare requirements. |  |  | x |  |
| Reduce the risk of pollution and avoid any breaches in legislation. |  |  | x |  |
| Goods and services are procured more sustainability. |  |  | x |  |
| Reduce carbon emissions from road vehicles. | x |  |  | Home workers have no commute. |
| Reduce water consumption by 25% by 2020. |  |  | x |  |
| Ensure legal compliance with waste legislation. |  |  | x |  |
| Reduce the amount of waste produced by 5% by 2010 and by 25% by 2020 |  |  | x |  |
| Increase the amount of waste being recycled to 40%. |  |  | x |  |
| Sustainability training and communications for employees. |  |  | x |  |
| Partnership working with local groups and organisations to support sustainable development. |  |  | x |  |
| Financial aspects of sustainable development are considered in line with policy requirements and commitments. |  |  | x |  |