

Agile Working Policy

DOCUMENT CONTROL SHEET

Document Information:

Title / Version Number	Smart Working Policy v1.0
Document Status and timescale	
Accountable Executive	
Responsible post holder/Policy Owner	
Date Approved	
Approved By	
Publication Date	
Review Date	
Author	
Stakeholders engaged in development or review	All CCG Staff
Equality Impact Assessment	<p>EQUALITY IMPACT ASSESSMENT</p> <p>This document has been assessed for equality impact on the protected groups, as set out in the Equality Act 2010. This policy is applicable to every member of staff within the CCG irrespective of their age, disability, sex, gender reassignment, pregnancy, maternity, race (which includes colour, nationality and ethnic or national origins), sexual orientation, religion or belief, marriage or civil partnership, and those who work on behalf of the CCG</p>
Contact details for further information	

Amendment History:

Version	Date	Reviewer Name(s)	Comments
0.1		Victoria Medhurst	Initial Draft
0.2	26/11/2018	Victoria Medhurst	Second draft following all staff consultation and feedback

Table of Contents

Contents

DOCUMENT CONTROL SHEET	2
------------------------------	---

Document Information: 2

Table of Contents.....	3
2.0 Scope	4
3.0 Definitions.....	5
4.0 Policy Statement	5
5.1 Roles and Responsibilities.....	5
5.3 Line Managers.....	5
5.4 All Employees.....	6
6.0 Eligibility and Exclusions.....	7
7.0 Process for Agreeing Agile Working	7
8.0 Information Security and Confidentiality	8
9.0 HMRC	9
10.0 Insurance	9
11.0 Use and care of equipment	9
12.0 Remote Network Connection and Video / Teleconferencing.....	9
13.0 Dissemination	10
14.0 Review	10
Appendix 1 Equality Impact Assessment Stage 1 Screening	11
Appendix 2: Work Station Risk Assessment.....	14
Appendix 3: Additional Workstation Guidance – 12 Steps to Workstation Set-up.....	15
Appendix 4: Remote Working Risk Self Assessment Checklist	17
Appendix 5: <i>Information Security and Confidentiality</i>	22
Appendix 6: Security Procedures for CCG Staff Using Remote Access	24
Appendix 7: Application for Agile working outside of Base	25

1.0 Introduction

- 1.1 NHS Lewisham Clinical Commissioning Group (respectively referred to as 'the CCG') recognises that there is a need to develop modern working practices through the use of supportive technology, enabling employees to maximise their performance and the fact that space is becoming an increasing challenge.
- 1.2 Agile working is the term used to describe how employees can work flexibly from any location; this could include CCG headquarters or other NHS locations, offices of Partners, Stakeholders or Shared Service providers, at home on occasion, or in any combination of these.
- 1.3 The concept of agile working gives employees the ability and the equipment to carry out their role securely, efficiently and successfully in different locations across the geographical area in which they work.
- 1.4 The aim of this policy is to support agile working for staff employed by the CCG. This policy does not negate or supersede the CCG's flexible working policy that already exists for use in individual circumstances by all employees. This policy is not appropriate for instances where regular flexibility of working patterns is required for personal reasons; instead the CCG's Flexible Working Policy should be considered.
- 1.5 It is accepted that not all jobs or employees may be suitable for agile working. Some jobs are intrinsically not suitable (e.g. staff whose role requires them to be office based) and some proposed arrangements may not be considered safe and secure. Line managers should consider each situation on its own merits, applying the principles of fairness and consistency whilst ensuring that overriding business needs and other requirements can be appropriately met.
- 1.6 This policy provides a framework for consistent and fair practice on the issues to be taken into account when considering agile working arrangements. The policy also sign-posts managers and employees to other relevant policies, not unique to agile working that should be considered when making decisions about new ways of working.

2.0 Scope

- 2.1 This policy applies to all CCG staff members including temporary or fixed term contract, and also including Governing Body Members.

3.0 Definitions

- 3.1 Agile working is based on the concept that 'work' is an activity that we undertake, rather than a place to which we go. Agile working allows organisations to work smartly and to take advantage of the opportunities available as a result of technology and situations where staff travel as a requirement of their role.
- 3.2 Teams and individuals may wish to review how they work and collaborate when working in an agile way, ensuring that communication channels are not lost.
- 3.3 Nominal Base describes the contractual base of the employee for HMRC, mileage/travel claims, and other expenses purposes.
- 3.4 Remote working is when an employee works from a location other than the nominal base remaining in contact electronically and via telephone.

4.0 Policy Statement

- 4.1 The CCG is committed to adopting agile working practices, where appropriate in the context of business needs, and empowering employees to maximise their performance.
- 4.2 This policy should be read in conjunction with other CCG policies, including but not exclusive to:
- The staff handbook, including the CCG values
 - Lone Worker policy
 - Flexible working policy
 - Health and safety policy

5.1 Roles and Responsibilities

5.2 Managing Director

The Managing Director has overall responsibility for this policy.

5.3 Line Managers

Line Managers are required to:

- Consider and, where appropriate, encourage agile working across their teams.
- Ensure fairness and consistency in applying this policy, especially when working within matrix management structures (e.g. line managing staff from different organisations).
- Ensure flexibility, openness and constructiveness in all discussions and agreements about agile working with employees within their area of responsibility, remaining focused on the needs of the service.
- Consider any health and safety implications when agreeing to agile working

arrangements. In particular, line managers may wish to discuss Display Screen Equipment (DSE) Assessments.

- Arrange for the provision of any appropriate equipment needed by the employee to ensure they can work securely, effectively and safely when working agilely.
- Periodically review agile working arrangements for employees within their area of responsibility, in line with the policy and guidance.
- Ensure employees working in an agile way are clear of the expectations on them and that effective communication and an effective managerial relationship is maintained.
- Consider any information governance and security implications associated with agile working and seek advice as appropriate.
- Ensure the employee takes responsibility for the security of CCG equipment and sensitive, confidential data and complies with the Data Protection Act, reporting data breaches or loss or theft of such to the CCG immediately.
- Ensure that the employee is aware of and agrees to other appropriately associated policy's e.g. the CCG's Lone Worker Policy, Health and Safety at Work, listed in Section 4.
- Consider how they can model agile working in their daily practice

5.4 All Employees

All employees are required to:

- Familiarise themselves with the content of this document, and with health and safety requirements relating to agile working, ensuring that they protect their own health and safety when working agilely.
- Comply with all conditions contained within this document, and any other policies or guidance referred to within this document.
- Ensure their line manager has authorised (in writing) the agile working arrangements in advance of undertaking any agile working.
- Ensure their line manager is advised of any changes to agreed agile working arrangements in a timely manner.
- Raise any concerns arising from agile working arrangements, including health and safety and information governance concerns to their line manager.
- Ensure flexibility, openness and constructiveness in all discussions with their line manager about agile working remaining focused on the needs of the service.
- Ensure the security of CCG equipment and data complying with the Data Protection Act and the CCG information governance policy.
- Report the loss or theft of any CCG equipment or data or breaches of the information governance policy and/or Data Protection Act in line with local policy as soon as is reasonable practicable.
- Report the damage of any CCG equipment as soon as is reasonable practicable.
- Ensure that when working agilely, they are contactable via telephone and email at a minimum. Frequency should be agreed between the member

of staff and the line manager.

- Ensure that when working agilely, their Outlook calendar is up-to-date and that appropriate staff can view the details of the calendar.
- Liaise with their line manager for advice or clarification as required.

6.0 Eligibility and Exclusions

- 6.1 Line managers are responsible for determining appropriateness for the roles and eligibility for agile working and have the ultimate responsibility for deciding whether an employee is authorised to undertake agile working.
- 6.2 The SMT will review all applications for agile working and a decision will be provided to the employee and their line manager no later than 28 days after the date of application.
- 6.3 Agile working is not a substitute for Flexible Working, nor is it considered a contractual right or a permanent arrangement. In instances where regular flexibility of working patterns is required for personal reasons, the CCG's Flexible Working Policy should be considered.

7.0 Process for Agreeing Agile Working

- 7.1 Either the line manager or the employee can initiate a discussion about the possibility of agile working. The line manager should give appropriate consideration to a request made by an employee to work in an agile way and employees should similarly give appropriate consideration to management requests to work agilely.
- 7.2 The line manager and employee should consider the following points before agreeing an agile working arrangement:
- Whether this policy is applicable or whether an alternative policy may be more appropriate, for example, the flexible working policy;
 - Whether the business needs of the CCG can be best met if an agile working arrangement were to be agreed;
 - Whether there are any health and safety implications or information governance implications, consulting the information governance lead or the CCG's Health and Safety manager/provider and undertaking assessments such as Risk Assessments and Display Screen Equipment (DSE) Assessments, as appropriate;
 - Whether there are any other risks associated with agile working, for example, risks to equipment and the CCG's obligations in relation to the Data Protection Act in line with information governance requirements. Where risks are identified, the line manager and employee should discuss whether these can be adequately mitigated to ensure that the CCG continues to comply with any legal or other obligations;
 - Whether any additional equipment may be required and whether this is financially feasible;

- Whether the employee will be adequately contactable. As a minimum staff should be contactable by email and telephone;
- Whether the manager has full view of the staff member's calendar and
- Whether HR or other advice may be required.

7.3 If agreed, the line manager should:

- Confirm agreement to the principle of working agilely to the individual in writing.;
- Confirm any particulars of the agreement, for example, in relation to management supervision and communication, or other specific arrangements, including how the employee will be contactable and their location known to their manager, their team and others;
- Ensure that all specific expectations of the agile working arrangement are clear to the employee, including the delivery of outcomes whilst working agilely; and
- Regularly review the agile working agreement and update this where necessary.

7.4 The SMT will review all applications for agile working and a decision will be provided to the employee and their line manager no later than 28 days after the date of application

7.5 If an employee does not agree to a manager's request to work agilely, the line manager should ascertain the reasons for the employee's refusal and discuss the reasonableness of this, the reasonableness of the request and all other relevant circumstances with their HR Business Partner. In some cases where there is a critical business need to transition staff to working more agilely, it may be necessary to consult with employees and HR advice should be sought from the appropriate HR Business Partner to determine the best course of action in the circumstances.

7.6 Any agreement to work agilely will not constitute a change to an employee's nominal base.

8.0 Information Security and Confidentiality

8.1 The Data Protection Act (1998), the General Data Protection Regulation (GDPR, 2018) the Freedom of Information Act (2000), and the Environmental Information Regulations (2004) all give the public rights of access to information held by the CCG. This right of access includes information held on the CCG's main sites and it also covers information held by staff at home or those working remotely.

8.2 Smart workers must ensure the security and safekeeping of all work related information. Any documentation of a confidential nature, particularly where it contains person confidential data (on patients or employees), should be kept in a lockable cabinet, box or briefcase only accessible to the employee. When finished

with, such documentation should be returned to the organisation to be disposed of appropriately.

8.3 All staff should be aware of the CCG's information governance policies relating to the handling of both patient and corporate confidential information and records. Specific Do and Don't instructions for this in relation to smart working are summarised in Appendix 5. This guidance MUST be followed by all staff working for or on behalf of the CCG away from the organisation premises on either an occasional or regular basis (remote or at home). Appendix 6 details security procedures for CCG staff using remote access

8.4 Staff should also be aware that rights of access by the public to the information held by the CCG under the Data Protection Act (1998) (DPA) and the Freedom of Information Act (2005) (FOI) legislation includes information held by staff at home or those working remotely at various destinations (see FOI and DPA policy).

9.0 HMRC

9.1 HMRC states that, providing that private use of an employer's equipment is insignificant when equipment is provided for business purposes, no benefits charge (tax) would arise. The CCG has issued staff with a mobile computing device which it considers essential for staff to carry out their work duties; in this case, a reasonable amount of additional personal use is permitted without attracting a benefits charge.

10.0 Insurance

10.1 Home insurers may need to be aware of agile working intentions e.g. if an individual is regularly working from home, as this may require a change in premium or policy terms. Staff should ensure that they have adequate home insurance cover.

11.0 Use and care of equipment

11.1 Staff are expected to take reasonable care of equipment provided to keep the risk of theft, data breach and personal safety concerns to a minimum. Equipment should be regularly charged, synchronised and software updated. Problems with the equipment should be reported to IT and the line manager at soon as possible.

12.0 Remote Network Connection and Video / Teleconferencing

12.1 CCG has invested in technology to allow smart working in it's offices. At the most basic

level, conference telephones, which allow multiple users to dial in, are available in meeting rooms. In addition, full videoconferencing facilities are available which allow visual contact and sharing of documents and media between all parties. Thirdly, sufficient access and bandwidth is provided over the wired and wireless networks to allow individuals to use services such as Skype for Business, FaceTime or Skype.

13.0 Dissemination

13.1 This Policy will be publicised in line with the framework for the development and management policy and procedural documents. Any future amendments/revisions to this policy will be brought to the attention of staff via internal communications. Managers will arrange for this policy and any subsequent amendments to be brought to the attention of all staff and ensure that it is accessible to them.

14.0 Review

14.1 This policy will be reviewed every three years.

Appendix 1 Equality Impact Assessment Stage 1 Screening

Title of policy, service, proposal etc being assessed:
Agile Working Policy

<p>What are the intended outcomes of this work? Include outline of objectives and function aims</p> <p>The aim of this policy is to support agile working for staff employed by the CCG. This policy does not negate or supersede the CCG's flexible working policy that already exists for use by all employees. This policy is not appropriate for instances where regular flexibility of working patterns is required for personal reasons; instead the CCG's Flexible Working Policy should be considered.</p>
<p>How will these outcomes be achieved? What is it that will actually be done?</p> <p>The CCG is committed to adopting agile working practices, where appropriate in the context of business needs, and empowering employees to maximise their performance.</p>
<p>Who will be affected by this work? e.g. staff, patients, service users, partner organisations etc. If you believe that there is no likely impact on people explain how you've reached that decision and send the form to the equality and diversity manager for agreement and sign off</p> <p>Staff</p>

<p>Evidence</p> <p>What evidence have you considered? Against each of the protected characteristics categories below list the main sources of data, research and other sources of evidence (including full references) reviewed to determine impact on each equality group (protected characteristic).</p> <p>This can include national research, surveys, reports, research interviews, focus groups, pilot activity evaluations or other Equality Analyses. If there are gaps in evidence, state what you will do to mitigate them in the Evidence based decision making section on page 9 of this template.</p> <p>If you are submitting no evidence against a protected characteristic, please explain why.</p>
<p>Age Consider and detail age related evidence. This can include safeguarding, consent and welfare issues.</p> <p>No local assessment. Policy based on other organisation's policies and best practice.</p>
<p>Disability Detail and consider disability related evidence. This can include attitudinal, physical and social barriers as well as mental health/ learning disabilities.</p>

<p>local assessment. Policy based on other organisation's policies and best practice. Potential for agile working to be a positive, reasonable adjustment. Also potential for agile working requirements need to take account of reasonable adjustments.</p>
<p>Gender reassignment (including transgender) Detail and consider evidence on transgender people. This can include issues such as privacy of data and harassment. No local assessment. Policy based on other organisation's policies and best practice.</p>
<p>Marriage and civil partnership Detail and consider evidence on marriage and civil partnership. This can include working arrangements, part-time working, caring responsibilities. No local assessment. Policy based on other organisation's policies and best practice.</p>
<p>Pregnancy and maternity Detail and consider evidence on pregnancy and maternity. This can include working arrangements, part-time working, caring responsibilities. No local assessment. Policy based on other organisation's policies and best practice. Potential need to assess agile working arrangements' suitability during pregnancy and for breastfeeding women. Potential to enable better flexibility and therefore a positive impact. DSE requirements will need to be fulfilled.</p>
<p>Race Detail and consider race related evidence. This can include information on difference ethnic groups, Roma gypsies, Irish travellers, nationalities, cultures, and language barriers. No local assessment. Policy based on other organisation's policies and best practice.</p>
<p>Religion or belief Detail and consider evidence on people with different religions, beliefs or no belief. This can include consent and end of life issues. No local assessment. Policy based on other organisation's policies and best practice.</p>
<p>Sex Detail and consider evidence on men and women. This could include access to services and employment. No local assessment. Policy based on other organisation's policies and best practice.</p>
<p>Sexual orientation Detail and consider evidence on heterosexual people as well as lesbian, gay and bisexual people. This could include access to services and employment, attitudinal and social barriers. No local assessment. Policy based on other organisation's policies and best practice.</p>
<p>Carers Detail and consider evidence on part-time working, shift-patterns, general</p>

caring responsibilities.

No local assessment. Policy based on other organisation's policies and best practice.

Other identified groups Detail and consider evidence on groups experiencing disadvantage and barriers to access and outcomes. This can include different socio-economic groups, geographical area inequality, income, resident status (migrants, asylum seekers).

No local assessment. Policy based on other organisation's policies and best practice.

Engagement and involvement

How have you engaged stakeholders with an interest in protected characteristics in gathering evidence or testing the evidence available?

This policy has been initiated by the need for staff to vacate Cantilever House and co-locate with the Council at Laurence House. A Building Working Group has been established as a staff stakeholder group, which has reviewed this policy.

How have you engaged stakeholders in testing the policy or programme proposals?

This policy has been initiated by the need for staff to vacate Cantilever House and co-locate with the Council at Laurence House. A Building Working Group has been established as a staff stakeholder group, which has reviewed this policy.

For each engagement activity, please state who was involved, how and when they were engaged, and the key outputs:

This policy has been initiated by the need for staff to vacate Cantilever House and co-locate with the Council at Laurence House. A Building Working Group has been established as a staff stakeholder group, which has reviewed this policy.

Summary of Analysis

Considering the evidence and engagement activity you listed above, please summarise the impact of your work. Consider whether the evidence shows potential for differential impacts, if so state whether adverse or positive and for which groups and/or individuals. How you will mitigate any negative impacts? How you will include certain protected groups in services or expand their participation in public life?

Policy based on other organisation's policies and best practice.

Appendix 2: Work Station Risk Assessment



DSE Workstation
checklist.pdf



Workstation set up &
advice.pdf

Appendix 3: Additional Workstation Guidance – 12 Steps to Workstation Set-up

1. Seated Posture	<ul style="list-style-type: none">• Adjust the chair back angle for support; this should be fairly upright when typing.• Adjust the chair back height to give support to the small of your back.• Adjust the seat height so that your elbows are just above the desk (relaxed shoulders, vertical upper arms, elbows bent at right angles).• Your wrists should be in a relaxed, neutral position over the keyboard.• Ensure arm rests do not prevent you getting close enough to the desk or obstruct your elbows whilst typing. If necessary, request that arm rests are removed.• Your thighs should be approximately horizontal.• If thighs are not horizontal or your feet are not flat on the floor, use a footrest.• Ensure that there is no undue pressure on the underside of your thighs.
2. Input Devices	<ul style="list-style-type: none">• The keyboard should be directly in front of you and at a distance to allow you to maintain relaxed shoulders, elbows at right angles and a neutral wrist posture.• Position your mouse close to the side of the keyboard and within easy reach.• Take your hand away from the mouse when not in use.• Use keyboard shortcuts as an alternative to the mouse.

3. Screen Reflection & Glare	<ul style="list-style-type: none"> • The screen viewing distance should be at approximately arms-length. • Screen height should prevent excessive movement of the head and neck. • The top of the screen should be at or just below eye level. This will depend on typing style, software used, glasses worn and tasks performed. The screen should be tilted back slightly. • Glare and reflections should be avoided by adjusting lights and closing blinds.
4. Local Environment	<ul style="list-style-type: none"> • Lighting should be sufficient for the task. • Workplace temperature should be at least 16° C. Draughts should be reported. • Noise that distracts or affects concentration should be reported.
5. Desk & Drawers	<ul style="list-style-type: none"> • Your body position should be 'squared-up' to the desk. • Avoid sitting twisted. Shoulders should be in line with your hips. • Drawers, CPUs, waste bins, etc. should not obstruct your legs.
6. Document Position	<ul style="list-style-type: none"> • Use a document holder or position documents to reduce head and neck movement, e.g. between the screen and keyboard.
7. Equipment Position & Work Area	<ul style="list-style-type: none"> • Place frequently used items within easy reach. • Don't cradle the phone between shoulder and chin. Hold the handset or consider a headset if you frequently use the phone and PC together. • Make sure the area around your desk is free from obstructions and trip hazards.
8. Workplace Organisation	<ul style="list-style-type: none"> • Organise your work so that you that you have reason to get up out of your chair and away from your workstation at least once an hour, e.g. collecting documents, filing. • As far as possible, do not locate printers on your desk or within reaching distance. • Adopt a variety of postures throughout the day.

Appendix 4: Remote Working Risk Self Assessment Checklist

This form will be used to assist you and your manager to ensure that your remote working conditions comply with current best practice.

Line manager	
Employee	
Address where assessment was undertaken	
Date completed	
Review date	

Working Practices	Yes	No	Comments / Actions Required	Date Completed
Do you use Display Screen Equipment (DSE) more than one hour per day?				
I spend 5-10 mins doing work other than DSE each hour.				
Health	Yes	No	Comments / Actions Required	
I am free of sore hands, joints or impaired grip				
I am free of aches and pains, pins and needles in the neck, back, shoulder or arms				
I am free of visual problems such as headache, focussing difficulties or eye discomfort				
I have had an eye test in the last two years.				
I have read health and				

safety information covering the safe use of DSE.				
I have arrangements for regular contact with my line manager.				
I am able to keep up to date and informed about my team and colleagues e.g. by attending team meetings.				
Workstation	Yes	No	Comments / Actions Required	
The design of my workstation allows me to work comfortably and efficiently.				
I have sufficient room around the workstation to arrange the desk and chair comfortably.				
Cords and wires are positioned safely to prevent trips and falls.				
The room had adequate lighting.				
The room is a comfortable temperature for working.				
Work Equipment	Yes	No	Comments / Actions Required	
My chair is stable with adjustable height and back support.				
My chair is properly adjusted and is comfortable for my work.				
I can rest my arms on the desk between tasks.				

The writing on the display screen is easy to read.				
The screen is free of reflection or glare from windows and lights.				
I do not need an anti-glare screen.				
I can easily read the keyboard.				
I can adjust the keyboard and screen to a comfortable position directly in front of my seating position.				
I do not need a document holder.				
When I work, my feet can rest flat on the floor or I have a foot rest to support my feet.				
My mouse is used within forearm radius from the edge of my desk.				
My mouse is used with my hand flat on the desk and directly in front of the mouse.				
I have a docking station for my laptop computer that I can use to connect to a full size keyboard and mouse.				
My screen is at the correct height i.e. the top of the screen is level with my eyes or slightly lower.				

Electrical Safety	Yes	No	Comments / Actions Required	
My equipment has been electrically tested (date).				
Security of information	Yes	No	Comments / Actions Required	
Is your home secure from intruders?				
Do other people in your accommodation have access to the area where you will be undertaking CCG business?				
Confidentiality	Yes	No	Comments / Actions Required	
I will only use encrypted equipment supplied by the CCG for work purposes.				
My passwords / PIN numbers etc are kept secure and not divulged to anyone.				
I can confirm that I will not transport any confidential data on non-encrypted storage devices e.g. memory stick or CD.				
I will shred confidential documentation.				
My computer will be locked when I am away from the workstation.				
Accidents / first Aid	Yes	No	Comments / Actions Required	
I know the procedure for reporting any accidents or work related illness				

I have a first aid kit available when working at home.				
--	--	--	--	--

Appendix 5: Information Security and Confidentiality

Do:

- Remember that as all work-related documents are the Organisation's assets, and as such fall within the scope of FOI and DPA (see CCG DPA Protocol and FOI policy).
- Work directly from the Organisation's server and save documents on the CCG network drives via CITRIX OR via a CCG issued encrypted USB data stick OR on OneDrive / SharePoint from office 365.
- Take all reasonable steps to maintain security of and prevent loss or damage to any data and/or records taken away from the organisation
- Take reasonable measures to protect work related information at home from unauthorised access, amendment or loss (this includes access by family members or pets).
- Consider what practical measures are needed to ensure the home environment is secure, i.e. not leaving papers in household areas where disclosures can take place.
- Take precautions against theft and loss, particularly on the journeys to and from work.
- Only use work email accounts for agile working. Keep home computer systems and applications virus protected and up-to-date
- Dispose of all confidential papers files in the CCG confidential bins at CCG premises only.
- Assess the risk involved with the loss of personal and business sensitive data, by addressing the following questions:
 - How serious would the consequences be if someone gained unauthorised access to this information?
 - How likely it is that someone could gain access to this information?
 - What security procedures and measures are in place and are they appropriate?
 - What is the cost of implementing appropriate security procedures and measures?
- Any person confidential data or corporate confidential data transferred to an encrypted USB data stick must:
 - be a copy of what is on your secure network drive;
 - remain encrypted and must not be transferred to any other external system, e.g. a home or other computer;
 - be worked on by opening and saving changes back to the USB data stick;
 - be returned to the appropriate location, as an updated version of the file/s on your organisation network drive and deleted from the memory stick after the work required is completed.
- Report lost or stolen device straight away even your own device if used for work related purposes
- Make sure you know how to **wipe/delete** data from your own device if it is lost/stolen so work related information is not at risk of being in the public. The CCG can provide this guidance too where appropriate but staff have to make sure they know who can provide them this assistance (from the manufacturer e.g Apple, Android) especially for devices such as tablets, phones etc.
- Ensure you have undertaken Information Governance Training
- Contact the CCG Information Governance Manager for guidance.

Don't:

- Use your home computer to store Organisation information.
- Remove a confidential paper file from the Organisation premises unless it can be stored securely.
- Leave confidential paper or electronic files where they could be accidentally viewed by others, including family members.
- Use a personal e-mail account for Organisation business or vice-versa. If you have to use your Organisation email account for personal business please keep separately and store separately to avoid possible problems with DPA or FOI requests.
- Leave confidential CCG information data or electronic media in unattended vehicles, even if locked in the boot.

Appendix 6: Security Procedures for CCG Staff Using Remote Access

Whilst high levels of security are incorporated into the remote access systems, users must comply with the following as an approved user:

- Passwords must never be written down.
- Passwords and user names must never be disclosed to unauthorised persons.
- Users must safeguard their authentication tokens.
- Output from the PC being used to connect remotely must be afforded the appropriate governance practice (see Information Security Policy) to avoid any unauthorised disclosure.
- Do not save confidential files to your computer's hard drive. All files should be saved to your network server to ensure they are secure and backed up.
- Only those staff approved and authorised are permitted to use the remote working service.
- Computers used must have proprietary anti-virus software installed with a valid licence.
- During log on and while conducting authentication users must ensure that no one can overlook the screen to view typing of passwords and also ensure that no disclosures of confidential information appear on screen during session take place.
- Computers must not be left unattended whilst logged on; if a computer is left unattended it must be secured by locking the workstation (CTRL+ALT+DEL followed by selecting the "Lock This Computer" option).
- All sessions are to be logged off when no longer required and users must ensure they receive a "termination" notice when disconnecting from the CCG network.
- Approved users must abide by the above practice as an approved user of remote working, failure to comply with best practice may result in the withdrawal of the facility.
- Applications for the use of other bespoke software should be made via your line Manager and the completion of the agreement below. The user must ensure that their line manager supports the application and provides the necessary budget code.
- Please refer to Smart Working Policy for guidance and details of the rules which apply to remote working.

Appendix 7: Application for Agile working outside of Base

Employee name	
Line Manager name	
Date of application	

Does the line manager support the application for agile working and why?	
What format will this take? (e.g. regular working from home, working from alternative organisations etc)	
How often will this occur?	
Is it anticipated that this will be on regular days? If so, when?	

Kit requirements

Laptop

4G connected device (not required if regular locations have wifi)

Mobile phone

SMT review

Date of review	
Comments from SMT	
Outcome	