Health Education East of England

Public Health Training Programme

Agile Working Policy

Version	Date	Author	Contributors/Comments
1.0 Draft	14/12/2017	John Battersby	First draft
1.1 Draft	24/01/2018	John Battersby	Celia Shohet, Linda Mercy
1.2 Final	07/02/2018	John Battersby	Bernadette Nazareth

Policy due for revision: 3 years from date of approval by STC

1. Introduction

1.1 The last few years have seen considerable changes in the way that many organisations work. Staff are routinely expected to work remotely for part of the working week and organisations now plan their office infrastructure and facilities accordingly.

1.2 The organisations that make up the public health system in the East of England have undergone these types of change. For example:

Public Health England (PHE) works on a desk:employee ratio of 4:5. Extensive use is made of Skype and other collaborative tools and teams are made up of individuals based all over the country, both at PHE locations and working from home.

Many local authority placements have similar policies in and practices in place.

1.3 If the training programme is to successfully train individuals who work effectively at consultant can level in these environments, it must expose them to these ways of working during training.

1.4 Moreover, these practices are so embedded in many organisations that it is not possible to offer 'special arrangements' to trainees; they should not be treated differently to other members of staff. For example it is not possible to justify why a trainee should be exempt from an organisation's hot-desking policy on educational grounds alone.

1.5 Nevertheless, the learning environment is an important element of training and so a balance needs to be achieved between the learning needs of the individual and the business needs of the organisation in which they are undertaking a placement.

2. Scope of policy

2.1 This policy applies to all registrars on the East of England Public Health Speciality Training Programme.

2.2 The organisations which offer training placements have a range of policies that will also apply. This includes policies covering:

- IT security
- Information governance and information security
- Health and Safety

This policy is NOT intended to override the policies of individual organisations.

3. Definition of agile working

3.1 For the purpose of this policy '*agile working*' covers situations where registrars work at a different location from their main training base on an ad hoc basis. Different locations may include satellite offices, working whilst travelling, working from other organisation's offices and working from home.

3.2 Full time home working arrangements are unlikely to be relevant in a training setting and are not covered by this policy.

3.3 This policy may be of relevance to those working from home as part of a reasonable adjustment or phased return to work but must not replace recommendations from occupational health services. Registrars requiring reasonable adjustments or phased returns to work should refer to the relevant policies published by the training programme lead employer.

4. When is agile working appropriate?

4.1 The agreement to allow agile working must be made between the registrar, their clinical and educational supervisors. In considering this, the clinical supervisor should consider the impact on the specific placement (e.g. ability to complete work, requirement to engage with colleagues and stakeholders etc.) and the educational supervisor should consider the broader impact on the registrar's training.

4.2 Agile working will not be appropriate at all stages of training or in all placements. In general agile working will not be appropriate during ST1, particularly during the MPhil course when attendance is required (in accordance with the relevant programme policies). Agreement for agile working is more likely to be given to registrars who are in phase 2 of training.

4.3 Agile working should only be considered where it is part of accepted practice for public health staff within the hosting organisation and where that organisation has planned its policies and infrastructure to allow for agile working. It would not be appropriate to agree to agile working for a registrar undertaking a placement where other staff are not expected to work in that manner; agile working is not an alternative to other forms of flexible or less than full time working.

5. Considerations for agile working

5.1 Agile working arrangements must take into account the following:

Educational factors

5.2 Agile working arrangements must not impact adversely on the registrar's ability to benefit from training. Evidence indicates that learning is largely experiential and enhanced by collaboration. Factors to consider include the ability of the registrar to consult informally with peers or other staff, the ability to access specific resources that are only available in the workplace. To ensure high quality training, the GMC requires that registrars work no more than one day per week at 'non-approved' locations, this includes working from home.

Health and safety

5.3 Employees who work at home have duties under the Health and Safety at Work Act in the same way as other employees. Registrars who work at home on an ad hoc basis as part of agile working arrangements will, therefore, need to be aware of their responsibilities and should undertake the appropriate self-assessment of their work environment.

Equipment (including computer equipment)

5.4 Registrars that are expected to work in an agile manner will need to be provided with the appropriate means to do so. In general this will mean that the host organisation will need to provide a laptop that is equipped with the necessary functionality to connect to the corporate systems that the registrar is required to access to do their work.

5.5 If a registrar requires additional equipment as part of reasonable adjustments, then the host organisation will need to provide this.

Security

5.6 The host organisation's information security and governance policies must be complied with at all times. Appendix 1 should be considered as a good practice guide for any areas not covered by host policies.

5.7 All registrars should have completed the appropriate mandatory training in relation to information security and governance for their host organisation.

5.8 Registrars should be aware that in all agile working situations there is an enhanced security risk. This may be through theft of equipment or information or through disclosure of information. In particular there is a risk of disclosure of personal confidential data (PCD). Personal confidential data should:

- Only be processed remotely with the agreement of the Clinical Supervisor and if it is impracticable to process it on host employer premises;
- Only be processed or stored on host employer provided IT equipment, not on personal computers or devices;
- Only be processed or stored on devices which are fully encrypted;
- Not be taken out away from host employer's premises in printed format;
- Not be emailed unless secure email accounts on the same network are used to both send and receive data (e.g. NHS.net).

5.9 Computers or other devices should be locked whenever unattended, even if only for a few minutes.

Hours worked

5.10 Registrars will be expected to work their contracted number of hours each day/week irrespective of the location at which that work is undertaken.

5.11 Arrangements for flexible working of contracted hours (e.g. starting and finishing earlier or later than usual business hours) must be discussed and agreed by the Clinical Supervisor. The discussion must be documented and must include a clear statement about the agreed core hours during which a registrar is expected to be contactable together with a record of relevant contact numbers.

5.12 Registrars should be aware that host employer IT departments may undertake software updates, equipment upgrades or other system changes which impact on the ability to work remotely. These often take place outside core working hours and registrars need to be aware of scheduled service interruptions and plan their work accordingly.

Communication

5.13 Registrars working remotely will be expected to be contactable by phone and email at all times. Diaries and calendars should be kept up to date with working arrangements and appropriate contact details.

Appendix 1: Good practice guide for areas not covered by host policies

- Users must take due care and attention of portable computer devices when moving between home and another business site
- Due to the high incidence of car thefts laptops or other portable equipment must never be left unattended in cars or taken into vulnerable areas.
- Users will not install or update any software onto a host owned portable computer device
- Users will not install any screen savers onto a host owned portable computer device
- Users will connect with a wired connection wherever possible. Where a wired connection is not possible and a wireless connection is used, this should be a secure connection. Personal, OFFICIAL-SENSITIVE or SECRET data should not be accessed via wireless connection.
- Users will not install any hardware to or inside any host owned portable computer device, unless authorised by the host's IT Services
- Users will allow the installation and maintenance of the host's installed Anti-Virus updates immediately
- Users will inform the IT Services Helpdesk of any host owned portable computer device message relating to configuration changes
- Business critical data should be stored on a host network drive and not held on the portable computer device
- All faults must be reported to the IT Services Helpdesk
- Users must not remove or deface any asset registration number
- No family members may use any host provided equipment. The host provided equipment is supplied for the registrars' sole use
- The user must ensure that reasonable care is taken of the host equipment supplied
- The user is not permitted to take any host supplied equipment outside the United Kingdom unless this is required as part of the registrar's placement and all appropriate organisational policies are followed.
- The host may at any time, and without notice, request a software and hardware audit and may be required to remove any equipment at the time of the audit for further inspection. All users must co-operate fully with any such audit
- Any user who chooses to undertake work at home or remotely in relation to their official duties using their own IT equipment must understand that they are not permitted to hold any database, or carry out any processing of OFFICIAL-SENSITVE or SECRET information relating to the host, its employees or customers. Under no circumstances should personal, OFFICIAL SENSITIVE or SECRET information be emailed to a private non-host email address.
- Any user accessing GCSx type services or facilities, or using OFFICIAL-SENSITIVE or SECRET information, must only use host-owned equipment which has appropriate technical security and advanced authentication mechanisms whilst working remotely. Connection for this device must be with a wired connection and no wireless connections must be used.
- When working on a laptop or other device, the user must ensure that the screen cannot be seen by anyone else. Personal information should never be viewed on a laptop or phone screen while travelling on public transport.