healthwatch Rutland

Home and Remote Working Policy

Policy objective:

To manage and prevent unacceptable risks arising to Healthwatch Rutland (HWR) from the use of unapproved or unsafe facilities and/or practices when working at home or working remotely.

Scope:

All staff/volunteers who are permitted to use HWR equipment at home or remotely, or who may use their personal computing resources to connect to networked services of HWR or produce HWR work are subject to the requirements of this Information Governance (IG) policy and procedure.

Responsibilities:

HWR Chair is responsible for the local infrastructure and computer information security requirements and for the supply and configuration of all computing equipment provided by HWR. This will include network connectivity and support for approved services if appropriate. The Chair may choose to delegate this responsibility to HWR CEO, whilst remaining accountable through line management.

Where agreement is provided that a staff member or volunteer may use their personal computing resources for business purposes connected to HWR, the CEO, with IT security advice as appropriate, must be satisfied that:

- resources concerned are configured appropriately
- the security measures are implemented and operating correctly
- that no unacceptable IG risks exist

HWR CEO is responsible for ensuring that a home risk assessment survey is conducted where necessary and for the identification of any necessary improvements or controls that affect proposed home working. In addition, the CEO, with appropriate IT security advice, will provide guidance to the home or remote worker (staff/volunteer) on all relevant security policies and responsibilities.

A home risk assessment survey will be necessary when an individual regularly works from home or remotely and has access to:

a. Documents protectively marked as 'confidential' or above in accordance with central government guidelines
b. other commercially or otherwise sensitive documents

c. any sensitive person identifiable information
d. person identifiable information deemed non-sensitive but still significant in terms of quantity (defined as 50+ records)

Unless instructed otherwise, the home or remote worker is responsible also for ensuring that their home contents insurance cover extends to any equipment provided belonging to HWR.

IG Security Procedures for home working:

- The home or remote worker's proposed working environment(s) should be considered and if necessary surveyed, and any perceived IG risks assessed to help inform consideration of home or remote working options. The findings of this consideration or survey process and any associated risks should be documented, so that appropriate control measures may be reviewed.

- Where the proposed home or remote working arrangements involve the use of personal (or shared) computing resources, it must be noted the IG risks of doing so may outweigh any operational advantage of working at home or working remotely. For all home or remote working scenarios, consideration of risks must be made and should take account of the potential to:

    - accidentally breach confidentiality
    - disclose other sensitive data of Rutland Healthwatch or associated organisations to unauthorised individuals
    - lose or damage critical business data
    - damage the organisation's infrastructure and e-services through spread of un-trapped malicious code such as viruses
    - create a hacking opportunity through an unauthorised internet access point;
    - misuse data through uncontrolled use of removable media such as digital memory sticks and other media
    - cause other operational or reputational damage

- When a home or remote working agreement is possible, the purpose, terms and conditions should be formally reviewed and agreed between HWR and the member of staff/volunteer and reference copy of this agreement must be provided to all parties. All such home or remote working agreements should be reviewed periodically for their continued applicability.

- Steps should then be taken to define, agree and implement the environmental security controls deemed necessary. HWR CEO, with appropriate IT security advice, should maintain records of all such assessments, surveys, related decisions, agreements and implementation plans.

- It is the responsibility of the staff member/volunteer to maintain their home or remote working environment ensuring compliance with HWR policies and agreements permitting their home or remote working. Where any aspect of home or remote working requires clarification or guidance this should be sought in the first instance from the HWR CEO.

- The home or remote worker (staff/volunteer) should be made fully aware of their information governance responsibilities to HWR. Training should be provided to support

any additional or special tools or functions that underpin the security of their home or remote working. Such facilities and training in their use are the responsibility of the CEO with appropriate IT security advice. This may for example include guidance on the deletion of cached information from internet browsers used to access web-based services.

- Failure by staff/volunteers to observe and maintain their home or remote working agreement may result in their home or remote working facility being withdrawn.

- It is the responsibility of the HWR CEO to ensure that the HWR infrastructure is maintained in a technically secure manner that would reasonably prevent a security breach arising from a home worker's location.

- Once all necessary steps have been satisfied, the home or remote working arrangements agreed may be made operational.

- Audit spot checks may be considered by HWR to ensure this home or remote working policy is complied with and the agreement with the staff/volunteer should clearly specify that this may occur. Any compliance issues will be reported to the HWR CEO and may subsequently be handled through a disciplinary process or contractual arrangements.

- All incidents involving the use of home or remote working facilities must be reported to the HWR CEO immediately and to the Board in a timely manner and in accordance with the organisation’s incident reporting procedures.