

**ELECTORAL OFFICE FOR NORTHERN IRELAND
MANAGEMENT BOARD PAPER**

Date of Meeting: 28 January 2010

Prepared by: Lisa Cherry, HR Officer

Home Working Policy

(a) The Management Board is asked to approve the attached draft policy for occasional one-off home working.

(b) **Background**

The HR Officer was requested by the August 09 Management Board to consider the practicalities of home working for all staff taking account of broadband availability and the need for direct access to EONI network. Following a survey of all staff no adverse impact was identified for any particular group by introducing home working procedures. The HR Officer met with the Senior IT Officer to discuss security. Given the security implications it was not permissible to use a home PC/laptop to connect to EONI network, however, most staff have access to an EONI laptop which is the only suitable arrangement where remote access connection is required. However, where direct access to the network is not necessary, a non-EONI laptop was recommended for home working use in respect of material that is not protectively marked data. The October Board agreed that the HR Officer would prepare a home working policy based on the recommendations.

(c) **Summary of Existing Policy and Practice**

Arrangements for home working were implemented as a contingency arrangement in respect of the swine flu pandemic. A formal home working policy for all staff has never been introduced although senior management have, on occasion, worked from home with the approval of CEO.

(d) **There are no options to consider in respect of access to the network for home working - due to security considerations, this is only permitted on EONI laptop. However, where access to the network is not required the following are options:**

1. Home Working Policy which prohibits the use of personal laptops and only permits the use of encrypted EONI laps regardless of nature of work.
2. Home Working Policy which permits occasional use a personal laptop for material which is not protectively marked, sensitive or personal.

(e) **Advantages and Disadvantages of each option**

Option 1

Advantages:

- Maximum security.

Disadvantages:

- Expensive encrypted laptops would be used regardless of the nature of the work, increasing unnecessary risks and increasing the responsibility on staff in respect of EONI assets eg carrying laptops on public transport etc.
- There is only a small number of EONI laptops available; the policy is applicable to all staff.

Option 2

Advantages:

- Minimises the risk of lost or stolen laptops, which would be a major embarrassment to EONI.
- Material worked on at home could be emailed and scanned through a 3 level security Mailmarshal and EONI server.
- Complies with NIO Code of Practice on working from home.

Disadvantages

- IT has no control over staff personal laptops which may contain viruses..

(f) **Evaluation of options**

Without argument, all staff must use an EONI laptop when processing protectively marked data or need access to EONI network but there is a balance to be struck in relation to working on material at home which is not sensitive or personal, and would give no cause for concern in terms of data protection. A personal PC is not a 100% secure environment to process non-protectively marked data but the security risk is minimal if data is scanned through EONI mail server. The current practice of working from home informally and emailing non protectively marked, sensitive or personal data has not produced any problems to date, and there is no reason why it would cause any difficulties in the future given the robust IT security system currently in place which ensures all data is scanned at network entry level, server level and client level ie Mailmarshal, Exchange and PC.

(g) **Recommendation**

To strictly enforce a mandatory measure as outlined in Option 1 is excessive and places EONI assets at an unnecessary risk due to the transportation of the equipment and increased responsibility placed on staff. I would recommend Option 2 but a strict restriction on USB devices – see Annex A (Concerns from IT).