

**IMPLEMENTATION EXECUTIVE
13 MAY 2009**

INFORMATION SECURITY POLICIES AND PROCEDURES

Executive Summary

This report is a brief interim summary of the current status of Wiltshire Council's information security policies and procedures, and the effectiveness of their promulgation to users (staff, members and contractors). As the documentation and processes are currently in a state of flux, a further conclusive report will be submitted to Cabinet.

Proposal

That the Implementation Executive:

- a) Note the contents of this interim report.

Reason for Proposal

Not only is there a significant risk of reputational damage to the authority were there to be a breach of information security (ie. unauthorised disclosure of confidential or personal data), there is a potentially much greater risk of harm to the citizens of Wiltshire should their data be compromised.

DR CARLTON BRAND

Corporate Director, Resources

Contact Details: 01225 718088

INFORMATION SECURITY POLICIES AND PROCEDURES

Purpose of Report

1. To inform the IE of the current status of the Council's policies and procedures covering information security and the arrangements for their dissemination to staff, members and contractors.

Background

2. Following the loss in the post of an encrypted USB memory stick (also known as a pendrive) containing personal information relating to a significant number of benefit claimants in the Salisbury area, the Chief Executive commissioned this review of policies and procedures. The encryption level of the memory stick was high, with negligible risk of the data on it being accessible. The review was carried out jointly by Internal Audit and IT Security. The review is focussing on the adequacy of policies and procedures governing information security in Wiltshire Council and the dissemination of these to users of our information systems.

Main Considerations for the Implementation Executive

3. This is a brief interim report on the progress to date by Wiltshire Council's ICT Security section (and others) to enhance existing policies and procedures governing information security for the new authority, and the means by which these policies and procedures are disseminated to users. A further report will be submitted to the new Wiltshire Council Cabinet at its meeting in June.
4. A number of detailed and technical issues have been identified, and these are actively being addressed by the Corporate ICT Unit and others. These relate to (a) responsibility for formally adopting relevant policies, (b) making the policies available to users via The Wire and other appropriate avenues, and (c) ensuring that users are aware of the policies and of their responsibilities.
5. Policies and procedures governing information security have been written over recent years and are being developed and updated in the context of the new authority. These are being loaded onto the new authority's intranet (The Wire). However, considerable work needs to be undertaken to consolidate these documents, as there are discrepancies in naming conventions; for example there are references to the 'Internet, E-mail and Computer Usage Policy', which no longer exists and has been replaced with a document entitled the 'Acceptable Usage Policy'. Although these are essentially the same document, there is a risk of confusion for users as to which policy is in effect.
6. Information security policies and procedures are developed by the Corporate ICT Unit. There are no clear, definitive governance arrangements for the formal clearance and adoption of these documents. As a result, policies have been issued without accompanying consultation with non-IT functions. An example of this is the management of the Acceptable Usage Policy, which is currently required to be signed by the user and logged by HR. Work is being carried out

to refine administrative processes thus ensuring a lean and efficient means of communicating policies to users, possibly using a software solution.

Environmental Impact of the Proposal

7. None.

Equality and Diversity Impact of the Proposal

8. None

Risk Assessment

9. The over-arching risk to the Authority is that of data loss, primarily confidential and/or personal information being accidentally disclosed to unauthorised people.
10. The first contributory risk to the above is that policies and procedures are not sufficiently robust to address the increasingly complex IT environment in which Wiltshire Council now operates.
11. The second risk is that the policies and procedures are not adequately communicated to colleagues.
12. The third risk is that there is inadequate monitoring of adherence to and compliance with the policies and procedures.
13. As the authority is currently in a transitional phase, the above risks must be (and are being) addressed.

Financial Implications

14. None

Legal Implications

15. Information security has a close correlation with the Data Protection Act 1998. Security breaches of this Act are rightly taken extremely seriously by the Information Commissioner, the media and most importantly the citizens of Wiltshire.

Conclusion

16. The authority is in a period of major change, and, whilst some areas of information security remain to be fully addressed from a corporate governance perspective, the IE should recognise that extensive steps are being taken to address outstanding issues.

Background Papers

None.

Appendices

None.