

## Management Action Plan

| Recommendation   | Implementation   |   | Comments |
|--|--|---|----------|
|  | Date   | By Whom   |          |
| <p><b><u>Property Security</u></b></p> <ol style="list-style-type: none"> <li>1. Review of contract with security company</li> <li>2. Review of both Council and staff responsibilities and of general awareness, especially re flexible working hours and out of hours working</li> <li>3. Audit and actions of buildings to cover matters such as the strength of doors and windows to be undertaken – Facilities Manager for the Council's main offices and each manager of a satellite establishment within the organisation.</li> </ol>   | 30/09/09   | Facilities Manager  |          |
|  | 30/09/09   | Director of HR  |          |
|  | 30/09/09   | Facilities Manager / Managers of satellite Establishments |          |
| <p><b><u>Use of IT</u></b></p> <ol style="list-style-type: none"> <li>4. A new data centre with improved security and resilience.</li> <li>5. New core infrastructure design and build, which will include: <ul style="list-style-type: none"> <li>• Redesign of Active directory to support the delivery of flexible and partnership working, ensuring that high levels of security of systems and information.</li> <li>• PC refresh programme – The Council has a 5-year refresh programme. The current approach is to refresh PCs based on age. This programme will deliver enhanced security (including encryption, where appropriate, and enhanced e-mail security, delivered via GovConnect, and the use of GCMail) on PCs. However, in light of this incident, the implementation schedule is</li> </ul> </li> </ol> | <p><b>Scheduled to be delivered April 2010</b></p>                                   | Director of BT&IT   |          |
|  | <p><b>Scheduled to complete in 3<sup>rd</sup> quarter 2010.</b></p>                  | Director of BT&IT   |          |
|  | <p><b>This project has commenced with key areas being addressed in 2009/2010</b></p> | Director of BT&IT   |          |

|  |   |   |  |
|--|---|---|--|
| <p>currently being reviewed to bring forward areas such as Adult Social Care and Children's Services..</p> <ul style="list-style-type: none"> <li>• Flexible work project – This project will deliver solutions to enable flexible working throughout the authority in a secure manner. This project is currently being</li> <li>• Storage – A new scalable and secure storage solution was implemented in 2008. All new PCs being rolled out are configured to store data on this device as the default. This device is backed up regularly and tapes stored off site</li> <li>• Partnership working – This project will build on the work already undertaken under GovConnect to further strengthen the security, policies and protocols required to enable effective partnership working, whilst addressing the need to protect and secure Council information. – scheduled for delivery throughout 2009/2010.</li> <li>• All of the above will link directly and be aligned to and support delivery of the Information security strategy.</li> </ul> | <p><b>Scheduled to deliver throughout 2010/2011.</b></p> <p><b>A further piece of work scheduled for 2010/2011 will be the implementation of electronic document management</b></p> <p><b>Scheduled for delivery throughout 2009/2010</b></p> | <p>Director of BT&amp;IT</p> <p>Director of BT&amp;IT</p> <p>Director of BT&amp;IT</p> <p>Director of BT&amp;IT</p> |  |
| <p><b><u>Information Security</u></b></p> <p>6. That the Council appoint a Senior Information Risk Owner (SIRO) at Executive Director level. (This would show the Council's commitment to the management of the information risks the Council</p>  | <p>By end of October</p>  | <p>CESG</p>   |  |

|  |       |       |  |
|--|-------|-------|--|
| <p>faces and that senior management support is given to the concept of compliance.)</p>  |       |       |  |
| <p>7. That Information Governance training becomes mandatory for:</p> <ul style="list-style-type: none"> <li>○ all staff</li> <li>○ staff of partner organisations that handle personal data for which BwD is accountable (An acceptable equivalent level of training could be provided by the employing organisation.)</li> <li>○ Directors</li> <li>○ Members</li> </ul> | ditto | ditto |  |
| <p>and that this is renewed every three years. (This should become part of the appraisal system in such a way managers will know who has and who has not had recent training.)</p>   |       |       |  |
| <p>8. That the exchange of personal and/or confidential information between the Council and its many partners be controlled and carried out via secure links rather than by using existing email systems.</p>  | ditto | ditto |  |
| <p>9. That the Council adopts the Local Government Association's guidelines on Data Handling (see checklist in the attached appendix 14) and incorporates them into its Information Governance Strategy and all its related policies, including Data Protection, Data Quality &amp; Records Management.</p>  | ditto | ditto |  |
| <p>10. That the role of Information Governance Officers in each Department and the Terms of Reference of the Corporate Information Governance Group are reviewed.</p>  | ditto | ditto |  |
| <p>11. That the risks re Information Governance generally and Data Protection in particular are revised and that the SIRO is the corporate risk owner in this area.</p>  | ditto | ditto |  |
| <p>12. That each Department and Council partners, immediately, review the personal data they hold, outside secure server systems (in whatever format), and assess the risks and controls</p>   | ditto | ditto |  |

|   |       |       |  |
|---|-------|-------|--|
| <p>involved in holding such data, reporting the outcomes to Audit &amp; Assurance.</p>  |       |       |  |
| <p><b><u>Summary &amp; Conclusion</u></b></p>   |       |       |  |
| <p>13. That the system of MAF be extended to cover the implementation of Information management and ICT policies.</p>   | ditto | ditto |  |
| <p>14. That Departmental Management Teams' Agendas include regular reviews of Information Management and ICT policies and that key risk areas are identified and mitigated.</p>   | ditto | ditto |  |
| <p>15. That each Department appoints an "Information Champion" who reports to the Director on key information management issues, with the corporate centre maintaining policies and providing support and guidance.</p> | ditto | ditto |  |
| <p>16. The intranet must be used to provide an accessible set of policy documents and guidance.</p>   | ditto | ditto |  |