Updated Management Action Plan – IT theft from Jubilee House 11 June 2009 – as at 31st August 2010

Recommendation	Implementation		Position as at 31 August 2010
	Date	By Whom	
Property Security			
1. Review of contract with security company	30/09/09	Facilities Manager	The contract with the new security firm has been in place since early December 2009. Since then the new contractor has responded to a number of alarm activations across the five main council sites. These have been handled effectively and professionally. The company's performance is being monitored on an on going basis to ensure that the Council continues to receive an adequate level of service.
2. Review of both Council and staff responsibilities and of general awareness, especially re flexible working hours and out of hours working	30/09/09	Director of HR	The revised acceptable use policy (AUP) was signed off by the Executive Member for Resources on 8 October 2009, following an update carried out as part of the GovConnect project. To date the policy has been rolled out to all staff who have been identified as users of the GovConnect secure exchange network. The policy has been revised to streamline it, remove unnecessary detail and address concerns raised by staff from the initial roll out. It is currently with the unions for consultation prior to Executive Member approval. It is planned to roll out the policy to all Council staff by October 2010 along with supporting guidance to staff regarding password security, the use of emails and the classification of information.

Recommendation	Implementation		Position as at 31 August 2010
	Date	By Whom	
			Network access will be disabled for any staff not signing up to the AUP and will only be restored after they have signed up. The AUP includes areas such as IT access, passwords, safe disposal of IT equipment, security of PCs and removable data devices, and storage of computers and devices. The Corporate Health & Safety Unit has published updated advice to staff on lone working and the provision of general personal security advice via Teamtalk and the intranet. This covers authorised employees transporting or utilising computers on or off site (e.g. transporting lap tops or use of PDAs in public areas such as car parks, etc), outside of busy public working hours. It also covers people working outside normal office hours on Council premises and the provision of personal safety advice.
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.	30/09/09	Facilities Manager / Managers of satellite establishments	Following the results of the building security audits, directors have confirmed that appropriate work has been taken to address any weaknesses or remedial actions that need to be undertaken. Children's Services staff also wrote to head teachers regarding Information Security before the summer closure. This included recommendations for schools on checking building security and secure storage of equipment and data. It is planned to include this area on the School Governors agenda for the Autumn meetings. In addition, the E-Learning Service is continuing to post key messages to schools about E-Safety and Data Security on their Learning Platform.

Recommendation	Implementation		Position as at 31 August 2010
	Date	By Whom	
			A sample of eight spot check building security audits has now been completed. These were done when Building Liaison Officers visited the sites for other works. They have reviewed the building security to ensure no issues have been overlooked and checked that the required works to address any security issues has been undertaken. The checks did not reveal any addition improvements required to strengthen building security.
Use of IT			
4. A new data centre with improved security and resilience.	**Scheduled to be delivered April 2010**	Director of BT&IT	The work is ongoing for the strip out and rebuild for the data centre. The building works, plus the fit-out of the mechanical and electrical equipment will be completed by end Jan 2011. The other data centre work, separate to the original Data Centre project, is the core infrastructure programme, which will comprise of the installation of a storage and backup solution, Active Directory, a server virtualisation environment, a monitoring & management solution etc. All these items are required before any of the IT services are migrated into the Data Centre. The date provided for the completion of this programme is estimated for May 2011 at this stage.
5. New core infrastructure design and build, which will include: • Redesign of Active directory to support the delivery of flexible and partnership working, ensuring that high levels of	**Scheduled to complete in 3rd quarter 2010.**	Director of BT&IT	Date is on track; however this is being delivered as part of the transformation agenda.

Recommendation	Implementation		Position as at 31 August 2010
	Date	**By Whom**	
security of systems and information. • 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 currently being reviewed to bring forward areas such as Adult Social Care and Children's Services.	**This project has commenced with key areas being addressed in 2009/2010**	Director of BT&IT	Children's and Elevate PCs have been refreshed. Some discussion outstanding whether this is a role based refresh. In addition to security implementation measures implemented as part of GovConnect, additional PC security enhancements are under review. With regards to encryption of machines, a number of products were evaluated by BT&IT. One has been selected for deployment across the Council's IT estate. The project to deploy encryption started on 7 June 2010. The encryption of our IT estate is now over 82% completed. The remainder will be encrypted via the 'refresh' programme as the current encryption software cannot be installed on these older machines. These machines will be given priority and will be replaced by the end of 2010. All our laptops have now been encrypted. All BwD employees who have been identified as GC mail users by the business now have GC mail accounts. Procurement of PCs for the refresh programme is underway
• Flexible work project – This project will deliver solutions to enable flexible working throughout the authority in a secure manner.	**Scheduled to deliver throughout 2010/2011**. **A further**	Director of BT&IT	There are a number of projects currently underway which will help to facilitate flexible working. These include piloting new mobile phone technology, the Refresh project, which will include secure client access, and the planned use of encrypted memory sticks.

Recommendation	Implementation		Position as at 31 August 2010
	Date	By Whom	
• 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.	**piece of work scheduled for 2010/2011 will be the implementation of electronic document management**	Director of BT&IT	This area is part of the core infrastructure and will be in place by May 2011. BT&IT are working with strategic IT partners on the infrastructure and storage solution. New PCs store on the new device by default. Users can change where data is stored. However, data storage needs to be covered in individual departmental induction processes. The acceptable use policy will reinforce Council policy on data storage. Back up tapes are NOT stored off site and this is unlikely to change until the new Data Centre is operational.
• 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.	**Scheduled for delivery throughout 2009/2011**	Director of BT&IT	Work on this area will be undertaken as part of the 'Flexible Working' project.
• All of the above will link directly and be aligned to and support delivery of the Information security strategy.		Director of BT&IT	
<u>Information Security</u> 6. That the Council appoint a Senior Information Risk Owner (SIRO) at Executive Director level.	By end of October 2009	CESG	At its meeting on 6 October, CESG agreed that the Strategic Director, Resources would be the SIRO.

Recommendation	Implementation		Position as at 31 August 2010
	Date	By Whom	
(This would show the Council's commitment to the management of the information risks the Council faces and that senior management support is given to the concept of compliance.)			SIRO now appointed and attended training in role.
7. That Information Governance training becomes mandatory for : ○ all staff who handle personal data ○ 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.) ○ Directors ○ Members 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.)	By end of October 2009	CESG	A staff awareness raising and training programme, co-ordinated by Audit and Assurance staff, nearing completion. Formal 30 minute training courses have been provided for all staff who handle personal data. In addition, all staff have been given access to 'Do's and don'ts' guidance regarding information security and data protection via the intranet and February's Team Talk. Mop up sessions are scheduled for the end of September 2010. Information security training will be included as part of the staff induction training. Other awareness raising will be carried out on an ongoing basis, which includes Directors being asked to include this area as a standing item on DMT agendas. An e learning package has been evaluated as to consider its suitability to provide the mandatory training programme, renewable every three years. The data protection awareness training provided by major partners has been reviewed and assessed. Their training, both in terms of content and frequency meets the Council's standard to be considered fit for purpose.
8. That the exchange of personal and/or confidential information between the Council and its many partners be controlled and carried out	By end of October 2009	CESG	The Director of BT & IT has led on this. This area is covered by the GovConnect Code of Connection requirements, which were implemented by the

Recommendation	Implementation		Position as at 31 August 2010
	Date	By Whom	
via secure links rather than by using existing email systems.			Council with effect from 30 September 2009. We now have a protocol which has been signed by ourselves, our NHS Partners and other local councils and public sector authorities. The PCT and Adult Services merged recently to form a 'Care Trust Plus' and as part of the councils larger organisation have signed up to the protocol as well. This protocol is now implemented across the authorities.
9. That the Council adopts the Local Government Association's guidelines on Data Handling and incorporates them into its Information Governance Strategy and all its related policies, including Data Protection, Data Quality & Records Management.	*ditto*	*ditto*	The Information Governance working group has been established to review the information governance strategy and, where these are not already in place, develop appropriate policies and procedures. The IGS group now meets on a regular basis to progress the strategy.
10. That the role of Information Governance Officers (IGO) in each Department and the Terms of Reference of the Corporate Information Governance Group (IGG) are reviewed.	By end of November 2009	ditto	The draft Terms of Reference for IGOs and for the IGG which were part of the report considered by the Committee in September have been provided to the SIRO. The reconstituted IGG, chaired by the SIRO, meet in February. The links to the corporate Risk Management Group will also be made closer. The IGG now forms part of the Risk Management structure within the Council's Risk management Structure lead by the Head of Risk and Safety.
11. That the risks re Information Governance generally and Data Protection in particularly are revised and that the SIRO is the corporate risk owner in this area.	By end of October 2009	ditto	Up dated risk register entries for both Corporate Governance and Information Governance have been prepared. The SIRO and the Risk Management group will own and manage the risks identified.

Recommendation	Implementation		Position as at 31 August 2010
	Date	By Whom	
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 involved in holding such data, reporting the outcomes to Audit & Assurance.	ditto	ditto	See 9 above.
Summary & Conclusion			
13. That the system of MAF be extended to cover the implementation of Information management and ICT policies.	By end of October 2009	CESG	See 9 above.
14. That Departmental Management Teams' Agendas include regular reviews of Information Management and ICT policies and that key risk areas are identified and mitigated.	ditto	ditto	See 9 above.
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.	By end of November 2009	ditto	This will be considered by the SIRO as part of reviewing the role of the IGG.
16. The intranet must be used to provide an accessible set of policy documents and guidance.	By end of October 2009	ditto	The Council's Data Protection and Records Management Policies have been updated to ensure they are robust and fit for purpose. These were approved by Cllr Rigby in November and are now available on the intranet site. Members of the Information Governance Group have been informed and have direct access to the policies. Directors have also been informed. As part of the work of the

Recommendation	Implementation		Position as at 31 August 2010
	Date	By Whom	
			Information Governance working group, additional policies will be published on the intranet as and when they are developed and communicated to staff to ensure that they are aware of their responsibilities.