APPENDIX 3

ITSOG highlight report: Information security management July 2011

1 Information security incidents

A security incident is an event that has actual or potential adverse effect(s) on computer, network or user resources or is a compromise, damage or loss of such equipment or data. Each incident is allocated a sequential number, summary description and current status.

The new Information Security Incident procedure and toolkit is finished and is now available on the intranet: http://theintranet.lbhf.gov.uk/Council_Business/Business_Technology/Information_security/ .

1.1 Statistical summary of incidents

	2009			**2010**			**2011**		
	L	**I**	**Sub-Total**	**L**	**I****	**Sub-Total**	**L**	**I**	**Sub-Total**
CHS	9	1	10	12	7	19	0	1	1
CSD	4	4	8	1	4	4	1	0	1
Env	0	1	1	2	2	4	1	0	1
FCS	5	6	11	1	9	10	0	3	2
HFH/HRD	0	1	1	0	1	1	1	4	5
RSD	1	1	2	0	0	0	0	0	0
HFBP	1	0	1	0	0	0	0	0	0
Unknown	2	0	2	0	0	0	0	0	0
Totals:	23	13	36	16	21	33	3	6	9

Please note that from the incidents recorded above the following number of cases are still open for each department:

- CHS = 4
- CSD = 1
- ENV = 1
- FCS = 1
- HRD = 5

Key:

- L = Loss/theft
- I = all other incidents, including DP and GC breaches
- **Where incidents involve more than one department this has been counted individually against each department involved, but as a single incident in the overall total.

1.2 Top 5 risks

1. Potential for data to be sent via webmail with no method of monitoring
2. Confidential waste service is not currently fit for purpose due to a lack of internal governance and contract with companies used –

MITIGATION: new framework agreement is about to be signed up to by H&F which provides lockable containers..

3. 3rd party and internal Individuals inappropriately copied into emails containing personal data.
4. Forwarding of potentially sensitive information via Councillors auto-forwarding emails sent to their council accounts over the internet to their webmail accounts.
5. Paper records and documents containing sensitive information stored insecurely for considerable periods of time whilst being prepared for transit.

2 Government Connect Project

2.1 Accreditation

LPSN (London Public Secure Network) - Full connection to the LPSN is awaiting an LPSN policy decision regarding remote working. HFBP investigating a workaround proposed by LPSN that would avoid H&F having to issue all mobile/remote/Smart workers with Council owned equipment.

2.2 GCSx mandatory information security awareness training

The Information Manager will be reporting back to the each DMT with a final chasing list so that each DMT can chase those officers who have yet to complete the training.

Percentage completion per department is as follows:

Department	**% completion to date**
Children’s Services	86%
Community Services	86%
Residents Services	100%
Finance and Corporate Services	98%
Environment	94%

The e-learning training for information security was rolled out to H&F Homes in September of last year to very limited take-up. It was hoped that all officers who had not signed the PCS or completed the training would do so as part of their induction when they join H&F in June 2011. However, we are now informed that no such inductions took place, so a full roll-out to staff in the Housing & Regeneration Department is being prioritised with a final deadline for completion of December 2011. IMT have a preliminary meeting with HR to discuss the roll-out on Wednesday 20 July.

All other non-signees will be shortlisted by IMT and sent up to EMT to escalate action.

2.3 Personal commitment statement (PCS)

2.3.1 Existing staff

To date, 89% of h&f staff has signed up to the PCS including agency staff (includes the 395 dead accounts now deleted from Outlook). Targeted chasing of non-responders has been carried out through the roll-out of the information security management training (see 2.2).

2.3.2 Business partners (including the voluntary sector)

- Some HFBP staff and other third party individuals with council logins have also signed up to the PCS but these will now instead be captured at organisational level through Business Partner sign ups. HFBP are writing to their subcontractors and LBHF departments should similarly write to a senior contact at each external organisation with whom they exchange restricted information whether electronically or as paper.
- The Information Management Team is in the process of chasing HFBP subcontractors and LBHF departments with external business partners and will prioritise those teams that are sharing personal client data.

3 Information security policy

The reviewed and updated Information Security Policy has now been published on the Intranet:
http://theintranet.lbhf.gov.uk/Council_Business/Business_Technology/Information_Security/159654_Information_Security_Policy_May_2011.asp

Going forward we will be rolling out a communications plan to ensure that all officers are regularly advised of its importance and applicability, including a regular message of the day and email updates.