APPENDIX 2 ITSOG highlight report: Information security management

January 2012

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

1.1 Statistical summary of incidents

1.1.1 Incidents since 2009

The table below gives a breakdown of all incidents that have come to the attention of the Information Management Team since January 2009. This also includes current active cases, further statistics on which can be found in section 1.1.2:

Dept	2009			2010			2011		
	L	I	Sub-Total	L	I	Sub-Total	L	I	Sub-Total
CHS	9	1	10	12	7	19	3*	3	6
CSD	4	4	8	1	4	4	3*	1	4
Env	0	1	1	2	2	4	1	0	1
FCS	5	6	11	1	9	10	0	4	4
HFH/HRD	0	1	1	0	1	1	2	5	7
RSD	1	1	2	0	0	0	0	0	0
HFBP	1	0	1	0	0	0	0	0	0
All Depts	0	0	0	0	0	0	0	2	2
Unknown	2	0	2	0	0	0	0	0	0
Total H&F:	23	13	36	16	21	33	8*	15	23

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 for the council.

1.1.2 Current active incidents

The table below gives a breakdown by department of all current active incidents in 2011 to date on the H&F Incident Log:

Dept	Live	Open	Closed
CHS	1	4*	1
CSD	2	1*	1
Env	0	0	1
FCS	0	1	3
HRD	2	2	3
RSD	0	0	0
Cross-department	0	1	1
Total H&F	5	8*	10

To note:

Live = Active incidents with priority tasks still outstanding
Open = Priority tasks completed, residual risks being monitored
* 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 for the council.

From January 2012, any incidents with outstanding actions will be compiled and presented by the Information Manager to the next ITSOG meeting for escalation.

1.2 Top 5 risks

1. Potential for data to be sent via webmail with no method of monitoring.
   MITIGATION – Webmail access to be switched off and staff to be informed via Message of the Day
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:
   MITIGATION - planned preparation and roll-out of Data Protection online training plus “classroom” sessions in high-risk service areas.
4. Forwarding of potentially sensitive information via Councillors auto-forwarding emails sent to their council accounts over the internet to their webmail accounts:
   MITIGATION – Councillors have signed their own Personal Commitment Statement and undertake to manage the risk by advising their constituents that auto-forwarding takes place. All newly elected or returning Councillors were trained in data protection and information security management as part of their induction.

5. Paper records and documents containing sensitive information stored insecurely for considerable periods of time whilst being prepared for transit:
   MITIGATION – data protection training, Offsite Records Storage Service standards and awareness raising that will be rolled-out as part of communication the new confidential waste arrangements.

2 Government Connect Project

2.1 GCSx mandatory information security awareness training

It has been brought to light, through the provision of statistics by Learning Pool, our e-learning provider, that as a result of personnel changes there has been a marked drop in the number of current staff within H&F who have completed this training. This is even taking into account the additional staff from the Housing and Regeneration Department (HRD) who have yet to complete this.

Percentage completion per department is as follows:

Department	% completion to date
Children's Services	44%
Community Services	48%
Environment Services	36%
Finance & Corporate Services	46%
Housing & Regeneration	2%
Resident Services Dept	71%
Grand Total	42%

To address the fall in figures, due to H&F reorganisation and high staff turnover, IMT, HR and Organisational Development will be rolling-out the e-learning to HRD in January 2012. This roll-out will focus on HRD in the first instance and act as a pilot for the roll-out across the remainder of the council by March 2012.

The intention thereafter is to ensure that all staff will complete refresher training every 2 years, with the e-learning also embedded into the induction process for new starters.

2.2 Personal commitment statement (PCS)

2.2.1 Existing staff

In light of the drop in the proportion of current staff who have completed the e-learning package (see 2.1), there will have been a concomitant and similar drop in the proportion of current staff who have signed the PCS. IMT are currently carrying out a gap analysis to ascertain the exact scale of this.

In order to ensure that all staff are captured going forward, a new round of PCS sign-ups will be incorporated into the roll-out programme for the e-

learning (see 2.1). HR have also committed to ensure that all new starters to H&F complete a PCS upon accepting a job offer from H&F.

2.2.2 Business partners (including the voluntary sector)

A new version of the PCS has been drafted for business partners. Moving forward we will need to ensure that all current business partners have signed this, focusing initially on areas involved in tri-borough work. This will also be added to all new contract procurement procedures.

3 Information security policy

The information security policy is in the process of being reviewed. As part of this process ITSOG, HR and other key stakeholders will be consulted prior to its submission to the Joint Management Group. The reviewed and updated policy will then be published on the Intranet to replace the current version: http://theintranet.lbhf.gov.uk/Council_Business/Business_Technology/Information_Security/159654_Information_Security_Policy_May_2011.asp

As part of the review of the information security policy, the communications plan (previous version attached below) will be updated. This will ensure that all officers are regularly advised of the policy's importance and applicability, through regular "message of the day" and email updates.

\\LBHF\Root1\
FCS-Procurement-and