Appendix 4

Corporate Information Governance Group (CIGG)

Information Governance Policy Framework

End of Consultation Document

Information Security, Risk and Governance Framework and Policies

Document Control	
Title/Version	End of Consultation Document
Owner	Corporate Information Governance Group
Date Approved	2 December 2016

Description	Version		Considered by
First Draft	1.0	23 Nov 16	David Randall/ Hannah Lynch
Second Draft	2.0	25 Nov 16	David Randall/ Hannah Lynch
Final Draft	3.0	02 Dec 16	CIGG

Contents

Introduction

Consultation on the Information Security and Governance Framework and an associated suite of Information Governance Policies for Canterbury City Council, Dover District Council (including East Kent HR and East Kent Audit Partnership), Thanet District Council (including East Kent Services) and East Kent Housing commenced on 13 October 2016 and ended on 27 November 2016.

Thank you for all of the feedback during this period, it has been extremely productive and has informed the final proposals as outlined in this document and its appendices. This document should be read in conjunction with the original consultation paper.

Subject to the necessary approval at each Authority or body, the final policies will be published on the intranet site and will take effect from 1 January 2017.

Feedback summary

Feedback and comments from both the Trade Unions and staff were collected via the intranet pages and have been considered by the Corporate Information Governance Group (CIGG), which includes the SIRO and Deputy SIRO from each authority and representatives from EKS (ICT), EKHR, EKH and EKAP. These have informed the final framework and policies as outlined in this document. Some of the key themes have been collated and are included at section 4 of this document.

Responses

Feedback and comments were collated.

Changes to original proposal

The majority of the feedback received sought clarification around the application of the policies and procedures and/or suggested changes to the wording which do not significantly impact the structure or content of the policy or procedure. A summary of these are detailed below:

Policy	Feedback	Final action
Information Security, Risk and Governance Framework	None received	Adopt as drafted
Physical and Environmental Security	None received	Adopt as drafted
Password Policy	I'd place the comment about writing down/sharing passwords in the "Key message" section given how important it is. iOS allows a longer PIN that 4 characters although our current MDM policy prevents me from doing so. May be worth a caveat or clarification as, although the OS allows it, the device config does not. Typo: "Car Registration plates plates" - an extra "plates" should be removed.	Added to key message section of the policy. This is already stated within key messages in the policy so no further change required. Amended accordingly.

	Passwords not containing names - I'd argue over zealous. By the time the password is 12 characters long, the fact that 4 of those characters is my friend's name is irrelevant. I wouldn't permit a password like "Will Russell Tim 3" as it's people in the team I'm from but "Russell Parrot Building 4" would be fine (and once hashed not a problem as guessing "Russell" wouldn't give you the rest). App development standards: "Shall not store passwords in clear text or in any easily reversible form". Unfortunately this isn't achievable in a number of situations. Case in point: web application which requires a database password to be provided in a text based configuration file. A caveat to this clause along the lines of "wherever possible, shall not store passwords in clear text or in any easily reversible form" would allow both situations.	Edited the bullet point within the policy to reflect the comment. Suggested words inserted into the policy.
Internet Use Policy	None received	Adopt as drafted
E-Mail Acceptable Use Policy	Regarding the recent incident involving a member of staff clicking a link in an email. Some firms use a series of test emails sent to staff which contain links that used to monitor where additional training is required, for example the company sends a mail to staff advising a secure token is available for collection from the mailroom - the user clicks the link which flags on a report to identify which users require additional email security training. This pro-active approach can help to prevent situations where staff are negligent and also helps to ensure that all emails are treated with the same sense of cautiousness. Nothing to comment regarding emailing large attachments, can the policy clarify whether use of Dropbox/ we transfer and other such sites is okay?	References to internet policy corrected so that they now refer to the email policy. Additional wording added to bullet point to reflect this type of incident, however, not reflected the potential use of this tool in the policy itself. This has been discussed previously at the CIGG and would be a matter for the group. Added reference to secure file sharing solutions in the policy.
Wi Fi Policy	An issue here is that staff are not trained to spot a good Wi-Fi network from a malicious one. Should this come to a disciplinary I'd be querying what training the end user had to know if a network was good or bad. Additionally, they only have to	Wording amended in responsibilities section of the policy to reflect the feedback. Removed the requirement to 'satisfy' and replaced with a duty of care.

	satisfy themselves according to this policy ("you must satisfy yourself that the connection is trustworthy"). By that token, this is unenforceable as the end-user can claim they satisfied themselves and the employer would be unable to prove the employee was being neglectful. It may be better for this to be guidance/training than a policy which could be used in a disciplinary. Not sure how practical it is to require that 'you must satisfy yourself that the connection is trustworthy, before you connect to it.' In practice many public areas now offer 'free Wi-Fi', how are individuals supposed to differentiate between what is trustworthy and what is not?	
Removal Media Policy	Under "key messages" it gives the impression only "returning or visiting devices" must be AV scanned. This means I can plug my personal device in for the first time and use it without scanning the device. Perhaps simply change this to "any time a removable media device is to be connected to Organisation owned equipment it must be scanned by ICT"? The potential impacts of removable media incidents are very serious.	Edited the bullet point within the policy to reflect the comment. However, this was rejected by the CIGG as it was considered to be too draconian a control measure and would adversely impact on day to day operations. Therefore the original wording was retained. Practical procedures to be developed to balance the need for removable media risks to be mitigated, whilst allowing the business to operate effectively.
Remote Working Policy	None received	Adopt as drafted
Information Management Policy	None received	Adopt as drafted
Incident Management Policy	None received	Adopt as drafted
Payment Card Industry Data Security Standards Policy	None received	Adopt as drafted
Business Continuity Policy	None received	Adopt as drafted
Information Risk Management	None received	Adopt as drafted

Policy		
Information Sharing Policy	None received	Adopt as drafted
PSN Acceptable Usage Policy and Personal Commitment Statement	None received	Adopt as drafted
Digital Security Policy – Network Access and Availability	None received	Adopt as drafted
Digital Security – Monitoring and Standards	"All owned and managed devices must meet these criteria" - implies the same is true for servers and workstation (non-portable) computers. "The device must have the capability to detect, isolate and respond to malicious software" a switch can't. Perhaps a caveat of "capable devices must..."? Similarly on the next point. "Session Activity by User and Workstation" - paragraph is missing its ending. Might be worth not naming software we use, as if that has to change the policy has to be updated.	Edited the bullet point within the policy to reflect the comments. Edited the bullet point within the policy to reflect both comments.
Data protection Policy	I am writing in connection with the Data Protection Policy, in particular the requirement to destroy or dispose of the data when it is no longer required. I am aware that many older IT systems were not designed to be able to identify items of personal data or to delete them readily, if at all. How do we secure compliance with the Act when we cannot identify or delete data that is no longer required?	This is being addressed through the Data Protection Sub Group.

Timeline and Next Steps

Description of Activity / Action	**Date**
Formal adoption of policies and procedures by the CIGG	2 December 2016
Consideration by Cabinet for approval and adoption	9 January 2016
Framework and Policies to go live (retrospectively)	1 January 2017