Bromley
THE LONDON BOROUGH
www.bromley.gov.uk

FINAL INTERNAL AUDIT REPORT

CHIEF EXECUTIVE'S DEPARTMENT

REVIEW OF INTERNET USAGE AUDIT 2016-17

Issued to:	**Stuart Elsey, Head of ICT** **Dee Jackson, Contract Monitoring ISD Manager**
Cc	**Mark Bowen, Director of Corporate Services**
Prepared by:	**Principal Auditor**
Date of Issue:	**2nd August 2017**
Report No:	**CX/071/01/2016-17**

INTRODUCTION

1. This report sets out the results of our audit of Internet Usage. The audit was carried out in quarter 3-4 as part of the programmed work specified in the 2016/17 Internal Audit Plan agreed by the Section 151 Officer and Audit Sub-Committee. The controls we expect to see in place are designed to minimise the department's exposure to a range of risks. Weaknesses in controls that have been highlighted will increase the associated risks and should therefore be corrected to assist overall effective operations.

2 The original scope of the audit was outlined in the Terms of Reference issued on 13th August 2015, however due to the change of contractor it was postponed until the 16th March 2017, when the TOR was reissued. The period covered by this report is from March 2015 to April 2017.

3. In June 2016 the authority used 394.88GB of internet data, with 2074 users of the Internet.

AUDIT SCOPE

4. The scope of the audit was outlined in the Terms of Reference issued on the 13th August 2015 and then reissued on the 16th March 2017.

AUDIT OPINION

5. Overall, the conclusion of this audit was that substantial assurance can be placed on the effectiveness of the overall controls. Definitions of the audit opinions can be found in Appendix C.

MANAGEMENT SUMMARY

6. Controls were in place and working well in the areas of: Policies covering internet usage are sufficiently detailed, extensive, up to date and available to staff. Information was eventually provided which shows a summary of staff’s internet usage and the sites accessed.

7. Our testing identified the following issues which we would like to draw to management's attention:-

- Staff are not undertaking Mandatory Information Governance Training.
- Monitoring is not undertaken of staff emails as per the Code of Conduct
- There are no controls to prevent Blackberry users from accessing inappropriate sites.

SIGNIFICANT FINDINGS (PRIORITY 1)

8. There were no significant findings identified during this review.

DETAILED FINDINGS / MANAGEMENT ACTION PLAN

9. The findings of this report, together with an assessment of the risk associated with any control weaknesses identified, are detailed in Appendix A. Any recommendations to management are raised and prioritised at Appendix B.

ACKNOWLEDGEMENT

10. Internal Audit would like to thank all staff contacted during this review for their help and co-operation.

DETAILED FINDINGS

No.	Findings	Risk	Recommendation
1	From the sample selected for testing of the top ten blocked users it was found that there were 5 staff, 1 councillor who had not completed the Information Assurance Training and 2 other generic user accounts detailed that do not identify the individual users. For the sample of top ten users by activity tested it was found that there were 6 staff, 1 contractor, 1 councillor and 2 generic accounts. The councillor and 1 member of staff had not undertaken Information Assurance training. The Internet and Email code of conduct was introduced in 2004. It cannot be confirmed that staff who joined before this date would have read the policy. It is made available to new starters.	Bromley does not comply with Data Protection requirements by staff accessing the internet who have not undertaken Information Governance training.	**All staff should undertake information assurance training.** **Staff should be reminded of the need to comply with the Internet and email Code of Conduct.** **[Priority 2]**
2	It was discussed with the Head of ICT that potentially controls weren't in place to prevent Blackberry users from accessing inappropriate sites as is the case with people accessing the internet through the Authority's PCs or laptops. This was then tested on the Head of ICT's Blackberry and found to be the case that inappropriate sites can be accessed. The authority has approximately 581 Blackberries.	Staff with Blackberries may access inappropriate internet sites.	**Software should be installed or the contract amended to prevent users from accessing inappropriate sites if technically possible.** **[Priority 2]**

DETAILED FINDINGS

No.	Findings	Risk	Recommendation
3	The Head of ICT confirmed to the Auditor that there is no monitoring or email monitoring unless this is requested by HR or a line manager. The Code of Conduct states that from time to time a sample of emails will be taken and monitored to make sure compliance with the code of Conduct. A protocol is in place should Managers need to request access to their staff's emails or should an investigation need be undertaken. This is not mentioned in the code of conduct.	Staff may send inappropriate emails which breach Bromley's policies and Information Governance Legislation.	**The Code of Conduct should be updated to mention the protocol in place should Managers or others wish to review a member of staff's emails and approval needed.** **[Priority 2]**

Priority 1
Required to address major weaknesses and should be implemented as soon as possible

Priority 2
Required to address issues which do not represent good practice

Priority 3
Identification of suggested areas for improvement

MANAGEMENT ACTION PLAN

Finding No.	Recommendation	Priority *Raised in Previous Audit	Management Comment	Responsibility	Agreed Timescale
1	All staff should undertake information assurance training.	2	This is being worked on by our Information assurance officer and HR / Training.	Head of ICT/ Human Resources	January 2018
2	Software should be installed or the contract amended to prevent Blackberry users from accessing inappropriate sites if technically possible.	2	There is limited software that will work with blackberry. We will explore options where we route internet traffic back through the LBB proxy servers so that it is filtered, however this may not be possible.	Head of ICT	October 2017
3	The Code of Conduct should be updated to mention the protocol in place should Managers or others wish to review a member of staff's emails and the approval needed.	2	Several policies are being reviewed and worked on with HR, we will make this one a priority	Head of ICT/ Human Resources	January 2018

Priority 1
Required to address major weaknesses and should be implemented as soon as possible

Priority 2
Required to address issues which do not represent good practice

Priority 3
Identification of suggested areas for improvement

OPINION DEFINITIONS

APPENDIX C

As a result of their audit work auditors should form an overall opinion on the extent that actual controls in existence provide assurance that significant risks are being managed. They grade the control system accordingly. Absolute assurance cannot be given as internal control systems, no matter how sophisticated, cannot prevent or detect all errors or irregularities.

Assurance Level — **Definition**

Full Assurance

There is a sound system of control designed to achieve all the objectives tested.

Substantial Assurance

While there is a basically sound systems and procedures in place, there are weaknesses, which put some of these objectives at risk. It is possible to give substantial assurance even in circumstances where there may be a priority one recommendation that is not considered to be a fundamental control system weakness. Fundamental control systems are considered to be crucial to the overall integrity of the system under review. Examples would include no regular bank reconciliation, non-compliance with legislation, substantial lack of documentation to support expenditure, inaccurate and untimely reporting to management, material income losses and material inaccurate data collection or recording.

Limited Assurance

Weaknesses in the system of controls and procedures are such as to put the objectives at risk. This opinion is given in circumstances where there are priority one recommendations considered to be fundamental control system weaknesses and/or several priority two recommendations relating to control and procedural weaknesses.

No Assurance

Control is generally weak leaving the systems and procedures open to significant error or abuse. There will be a number of fundamental control weaknesses highlighted.