West Lothian Council

CW1802

INTERNAL AUDIT REPORT

COUNCIL WIDE

INFORMATION SECURITY

15 March 2019

CONTENTS

1.0 EXECUTIVE SUMMARY

1.1 In accordance with the annual audit plan for 2018/19 we have undertaken a review of the management of information security breaches within the council and conclude that the level of control is **unsound**.

1.2 The audit remit is set out in section two. In relation to the follow up of our previous information security audit issued in December 2016, which concluded that control was unsound, we consider that control remains unsound and that the findings of our previous audit have therefore not been effectively addressed.

1.3 West Lothian Council is registered as a data controller with the Information Commissioner's Office (ICO), registration number Z6925127.

1.4 During the financial years 2017/18 and 2018/19 (to 30th November) there were 931 and 514 information security incidents logged respectively. The majority of these were considered low impact, mainly relating to 'phishing' attempts and computer viruses.

1.5 A number of cases are considered to be information security breaches, which require the completion of a risk assessment. Consideration is also given as to whether the case should be reported to the ICO. The council's process for the administration of information security breaches at the time of the audit fieldwork in November 2018 is detailed in Appendix B.

1.6 In 2017/18 and 2018/19 (to 30th November) there were 25 and 26 incidents respectively where a risk assessment was required to be completed. No incidents were deemed serious enough to be reported to the ICO in 2017/18 and two cases have been reported in 2018/19 to date.

1.7 There are policies and procedures in place for dealing with security incidents, including a security incident process, risk assessment templates and an escalation process for higher impact cases. However the audit found issues with all of these processes.

1.8 The following findings ranked as being of 'High' importance were found:

- the IT Security Incident process is not being fully followed in line with procedures, and does not reflect the revised corporate procedures (finding 3.2);
- two risk assessment templates are available for use, and there is uncertainty across services as to which should be used (finding 3.3);
- risk assessments are not being signed off and completed within the correct timescales (finding 3.4);
- we identified a duplicated case reference on a risk assessment resulting in one incident not being fully completed and correctly considered, and therefore a potential referral to the ICO being missed (finding 3.5);
- we identified inconsistencies in the data provided in the 2017/18 Annual Compliance Statement and to the Information Management Working Group (IMWG) and ICT Programme Board (finding 3.6);
- out of date Data Protection policy and Information Handling procedures are in use (finding 3.8).

1.9 Whilst there are several findings relating to the Security Incident process, through enquiry with officers in the service areas it is apparent that when new cases arise risk assessments are completed and senior management are advised. However e-mails and risk assessments are not being retained within an appropriate Security Incident folder in Objective by services and procedures are not being fully complied with. It has

therefore not been possible to review any of the most recent cases, and provide assurance that they have been dealt with effectively (finding 3.2).

1.10 The action plan in section three details our findings, grades their importance (Appendix A) and includes agreed actions. The implementation of agreed actions will help improve control.

1.11 We appreciate the assistance of all staff who contributed to the conduct of our audit. Should you require any further information please contact Kenny Wilson.

Kenneth Ribbons
Audit, Risk and Counter Fraud Manager

2.0 REMIT

2.1 The audit objectives were to determine whether controls are in place which ensure that satisfactory process and procedures for recording information security breaches and completing risk assessments are in place and being followed.

2.2 We have also followed up the agreed actions arising from information security audit CW1605, completed in December 2016.

2.3 No internal audit report can provide absolute assurance as to the effectiveness of the system of internal control. Our review concentrated on the key controls and our testing was undertaken on a sample basis. Therefore, the weaknesses we have identified are not necessarily all those which exist.

2.4 We agreed the draft report for factual accuracy with Julie Whitelaw, Head of Corporate Services on 11th March, 2019.

2.5 The Head of Corporate Services is responsible for both the implementation of agreed actions and the risk arising from not acting on any agreed actions in this report.

2.6 We carry out follow-up reviews on a risk based approach. The Audit, Risk and Counter Fraud Manager will determine the need for a follow-up review of this report.

2.7 In accordance with the council's risk management arrangements services are required to record internal audit findings graded as being of 'high' importance in Pentana (formerly Covalent) as risk actions, and to link these to the corresponding risks.

2.8 Audit findings ranked as being of 'high' importance that are not implemented will be reported to the Governance and Risk Board and Audit Committee and considered for inclusion in the Annual Governance Statement.

3.0 ACTION PLAN

Ref	Findings and Risk	Agreed Action	Importance Level
3.1	**Information Security Incidents: IT Procedures** IT Services' Security Incident procedures are not dated therefore we were unable to verify when they were last reviewed. Security Incidents are logged by IT Services in the Supportworks system, where a series of predetermined steps are set up to deal with the reported incident. It was noted that the following steps within the IT Procedures differ from the corresponding steps in the "new" risk assessment process implemented in May 2017: • IT Procedures: Advise Information Liaison Officer and Depute Chief Executive of the incident. "New" risk assessment process: Service Desk will notify the Head of Service and Depute Chief Executive. • IT Procedure: Advise Information Liaison Officer, Head of Service and Chief Solicitor of requirement to complete a risk assessment. "New" risk assessment process: Head of Service or nominated officer to complete Stage 1 risk assessment template. It was established through discussions with the Solutions Architect Manager that he was not aware of the "new" steps within the risk assessment process, and therefore IT Services procedures had not been amended to reflect the changes. **Risk** *Failure to correctly deal with an information security breach.*	In order to ensure a consistent approach to risk assessment of data security breaches is being conducted, an Objective workflow has been implemented from January 2019. A copy of the flowchart for the workflow is attached (Appendix F). The Objective system is the Council's electronic content management system. IT Services will commence/activate the workflow which immediately sends a notification to the Chief Solicitor to advise that a data breach has been lodged. The workflow contains alarms/alerts which are set to trigger at stages through the process to ensure that appropriate attention is being given to the completion of the risk assessment to allow reporting to the ICO within 72 hours where that is considered necessary. IT Security incident procedures have been updated to reflect the new workflow procedure.	Medium **Responsible Officer** Head of Corporate Services **Risk Identifier** WLC007 **Action Date** Completed

Ref	Findings and Risk	Agreed Action	Importance Level
3.2	**IT Security Incident Process** Once an information security breach has been reported to the IT Service Desk the main steps detailed on the IT Incident procedures are: • Inform the Information Liaison Officer (ILO) and Depute Chief Executive (DCE) of the incident • Advise the ILO, Head of Service and Chief Solicitor if there is a requirement to complete a risk assessment • Escalate to the Information Security Officer and DCE if no risk assessment is received within 7 days. A sample of 20 Security Incidents, 12 from 2017/18 and 8 from 2018/19 were reviewed and a number of findings identified, details of which are provided in Appendix C. IT Services confirmed it is their responsibility to open a file in Objective for each security incident logged. However we found that for 2017/18 and 2018/19 to date, 25 and 26 incidents required the completion of a risk assessment, and only 17 and 8 incident case folders respectively have been opened within Security Incidents in Objective. Enquiries with services did find that local records of security incidents were available; however in contravention of procedures, these were not located in the relevant incident files in Objective. There is a significant level of non-compliance with procedures and instances where we were unable to establish compliance due to a lack of an audit trail. **Risk** *Security incidents are not being properly resolved, or are not resolved within required timescales.*	In order to ensure a consistent approach to risk assessment of data security breaches is being conducted, an Objective workflow has been implemented from January 2019. A copy of the flowchart for the workflow is attached (Appendix F). The Objective system is the Council's electronic content management system. The Objective workflow automatically creates a separate file in Objective for all cases. The workflow has alerts which are set to trigger at stages through the process to ensure that appropriate attention is being given to the completion of the risk assessment to allow reporting to the ICO within 72 hours where that is considered necessary. The workflow retains/logs the risk assessment in the unique file in Objective. There is a clear audit trail to follow which officers have completed actions and what those actions were. IT Security incident procedures have been updated to reflect the new workflow procedure.	High **Responsible Officer** Head of Corporate Services **Risk Identifier** WLC007 **Action Date** Completed

Ref	Findings & Risk	Agreed Action	Importance Level
3.3	**Risk Assessment Process / Templates** A comprehensive risk assessment is required to record all appropriate information of the incident, allowing informed and objective decisions to be made. There are two risk assessment templates currently available to council officers on the intranet and there is uncertainty across services as to which should be used; both are used intermittently. An entry in Pentana indicates a pilot of the "two part" process was to start and this was reported to the ICT Programme Board on 22 May 2017. New templates for the "two part" process are available, however no evidence is available to confirm if and when this process was formally implemented. A review of the completed risk assessments available in the Security Incident folders since 22nd May 2017 show that 14 "old" and 8 "new" templates have been completed. The templates are not dated or version controlled and the available guidance notes are out of date. Both processes appear to be cumbersome and unwieldy with duplication of information/data being requested, particularly in the two stage process, and there is scope for the process and templates to be reviewed and streamlined. **Risk** *Confusion over which risk assessment process to follow resulting in potential delays in the initial assessment, progression and resolution of information security incidents.*	The 2 stage process was implemented to recognise that not all data incidents require to be categorised as data breaches and therefore not all incidents require to have the full risk assessment completed. The 2 stage process did not differ greatly from the 1 stage process, other than allowing an assessment of whether a full risk assessment was required. Where the "old" 1 part template has been used in error, the incident will have been fully assessed, rather than taking the opportunity to conduct an initial short assessment and close the case at that stage, where appropriate. In order to ensure a consistent approach to risk assessment of data security breaches is being conducted, an Objective workflow has been implemented from January 2019. A copy of the flowchart for the workflow is attached (Appendix F). The Objective system is the Council's electronic content management system. The Objective workflow implemented from January 2019 determines the process to be followed. A single risk assessment template is commenced/activated and is required to be completed in respect of all data breach incidents. Outstanding Risk Assessments will be considered and reviewed at each meeting of the Information Management Working Group. In addition, where outstanding risk assessments fail to be progressed, this will be reported as a risk to the Governance and Risk Board.	High **Responsible Officer** Head of Corporate Services **Risk Identifier** WLC007 **Action Date** Objective Workflow 1 stage process Completed IMWG from 3 April 2019 Reporting to Governance and Risk Board 13 May 2019

Ref	Findings and Risk	Agreed Action	Importance Level
3.4	**Risk Assessment Review** A sample of 20 risk assessments from 2017/18 (12) and 2018/19 (8) were reviewed with a number of findings identified. Details are provided in Appendix D. There is a significant level of non-compliance with procedures and a lack of an audit trail over key stages in the process e.g. risk assessments not fully signed off, required timescales not met or no evidence of sign off, and we are therefore unable to establish timescales. The sign off process appears to be overly complicated with too many officers required to sign the risk assessment resulting in delays in cases being formally closed. Consideration should be given to simplifying the risk assessment process. For example; final sign off being delegated to a Legal Services officer (within 72 hours); the service nominated officer/manager and final sign off by Head of Service (within a timescale to be agreed). With the exception of high risk / ICO cases, Depute Chief Executive and Chief Solicitor involvement should therefore be for reporting purposes only. **Risk** *The process for resolving an information security incident is unnecessarily cumbersome, resulting in security incidents not being properly resolved with required timescales.*	In order to ensure a consistent approach to risk assessment of data security breaches is being conducted, an Objective workflow has been implemented from January 2019. A copy of the flowchart for the workflow is attached (Appendix F). The Objective system is the Council's electronic content management system. The Objective Workflow requires sign off by Head of Service, Chief Solicitor and Data Protection Officer. All these officers are required to be involved in the risk assessment process to ensure all appropriate information is being captured; all cases are being appropriately risk assessed and considered and all appropriate remedial actions are being identified and progressed. Outstanding Risk Assessments will be considered and reviewed at each meeting of the Information Management Working Group. In addition, where outstanding risk assessments fail to be progressed, this will be reported as a risk to the Governance and Risk Board.	High **Responsible Officer** Head of Corporate Services/Heads of Service **Risk Identifier** WLC007 **Action Date** Completed IWMG from 3 April 2019 Reporting to Governance and Risk Board from 13 May 2019

Ref	Findings and Risk	Agreed Action	Importance Level
3.5	**Risk Assessment – Case F0194366** A review of the above IT Services case file found two risk assessments quoting the same case reference number. These related to completely different incidents from 7th November 2017 and 25th January 2018. The latter case from 25th January (reference F0202843) related to a lost phone that contained within its case a paper list of 20 young people's names, dates of birth and phone numbers. Details of the lost phone are recorded in the Legal Services Data/Security Breach Log; however no reference is made to the children's missing personal data. Investigations have been unable to confirm what information was provided to Legal Services, and discussion with the Chief Solicitor established that a recommendation to report the case to the ICO would have been made if she had been made aware of the full incident details. IT Services have closed the case and the actions covering the lost phone itself are complete. However, no Stage 2 risk assessment is available (which contains more detailed information on the review and assessment of the breach, including the actions taken), and we are unable to verify the full process has been followed and sign off has been completed. The service area Team Leader has confirmed that she discussed the loss of personal data with the colleague involved and collectively reminded the team of the importance of protecting customer data. **Risk** *The process for resolving an information security incident has not been completed properly resulting in no managerial sign off and the Chief Solicitor being unable to make informed decision to report a potential case to the ICO.*	The workflow contains alarms/alerts which are set to trigger at stages through the process to ensure that appropriate attention is being given to the completion of the risk assessment to allow reporting to the ICO within 72 hours where that is considered necessary. The Objective workflow automatically assigns a unique case reference to all cases. Cases cannot be closed until they have progressed through the sign off process – sign off by Head of Service, Chief Solicitor and Data Protection Officer. Outstanding Risk Assessments will be considered and reviewed at each meeting of the Information Management Working Group. In addition, where outstanding risk assessments fail to be progressed, this will be reported as a risk to the Governance and Risk Board.	High **Responsible Officer** Head of Corporate Services **Risk Identifier** WLC007 **Action Date** Completed IWMG from 3 April 2019 Reporting to Governance and Risk Board from 13 May 2019

Ref	Findings and Risk	Agreed Action	Importance Level
3.6	**Accuracy and Completeness of Incident Reporting Data** The audit identified inconsistencies in the data provided in the 2017/18 Annual Compliance Statement and to the IMWG and ICT Programme Board. WLC Annual Compliance Statement 2017/18 The Annual Compliance Statement was reported to the Council Executive on 25 September 2018 and the Governance and Risk Committee on 29 October 2018. The above statement advises there were 921 incidents logged with 17 Risk Assessments completed. Data provided by IT Services for the audit confirms there were 931 incidents logged and 25 Risk Assessments completed during 2017/18. Our previous audit report dated 13 December 2016 had also identified an error in the compliance statement for 2015/16. IMWG & ICT Programme Board (2018) Security Incident reporting to these groups is inconsistent with only figures for December 2017, January, May and June 2018 provided. Details for the remaining months of 2018 have not been reported. Also the figures provided to the January and February meetings (covering December 2017 and January 2018) are identical; therefore inaccurate data would appear to have been reported. The correct January figures were provided in April. See Appendix E for details. On reviewing the IMWG minutes it would also appear that outstanding risk assessments, as provided by IT Services, are not always discussed with a view to ensuring completion. **Risk** *Insufficient or incorrect data leading to a failure to properly monitor and manage the information security process.*	The risk assessment process does not record data when a decision has been taken not to progress a risk assessment, e.g. after initial investigation it is considered no data breach has occurred because the personal data has not been released out with the council. This has resulted in an inconsistency in the number of breaches reported to the IT Service desk and the number of risk assessments concluded. The Objective workflow automatically creates a separate file in Objective for all cases reported to the IT Service desk. The workflow has alerts which are set to trigger at stages through the process to ensure that appropriate attention is being given to the completion of the risk assessment to allow reporting to the ICO within 72 hours where that is considered necessary. The workflow retains/logs the risk assessment in its own file in Objective. There is a clear audit trail to follow which officers have completed actions and what those actions were. The workflow will also keep a record of any decision not to progress the risk assessment. The Objective workflow cases cannot be closed until they have progressed through the sign off process – sign off by Head of Service, Chief Solicitor and Data Protection Officer, including agreeing where a risk assessment is not required to progress Outstanding Risk Assessments will be considered and reviewed at each meeting of the Information Management Working Group. In addition, where outstanding risk assessments fail to be progressed, this will be reported as a risk to the Governance and Risk Board.	High **Responsible Officer** Head of Corporate Services **Risk Identifier** WLC007 **Action Date** Objective Workflow Completed IWMG from 3 April 2019 Reporting to Governance and Risk Board 13 May 2019

Ref	Findings and Risk	Agreed Action	Importance Level
3.7	**<u>Risk Assessment Remedial Actions Recorded in Pentana</u>** The final step of the "new" Data Breach and Risk Assessment procedure states *"All outcomes and remedial actions to be logged in Covalent (Pentana) as risk actions".* There is no evidence that any actions have been recorded in Pentana. The remedial action taken for security incidents is recorded within the risk assessment template and is resolved locally within the team / service area. Where serious breaches have been identified there would be merit in recording the corresponding actions in Pentana. **<u>Risk</u>** *Identified action in relation to remediating security breaches is not completed.*	All Heads of Service/ILOs will be reminded that risk actions are to be logged and monitored via Pentana. Outstanding risk actions will be reported and monitored via the IMWG. The IMWG will now report via the Governance and Risk Board and outstanding risk reports will be presented to the Board on a quarterly basis	Low **Responsible Officer** Head of Corporate Services **Risk Identifier** WLC007 **Action Date** IWMG 3 April 2019 Reporting to Governance and Risk Board 13 May 2019

Ref	Findings and Risk	Agreed Action	Importance Level
3.8	**Data Protection Policy, Information Security Policy and Information Handling Procedure** The council's Data Protection Policy is out of date. Last reviewed in April 2017, the 2018 version is available in early draft form only. The Information Handling procedure, dated July 2015, has not been reviewed since March 2016. The Information Security Policy is dated June 2017 and was presented to the ICTPB in August 2018. The meeting minute states *'Board noted the update by Ian Forrest on the Information Security Policy'*. The approval history of the current Policy on the intranet is still dated 20th June 2017. The Information Handling procedure link on the IT Services Information Security page opens the Information Security Policy not the Information Handling procedure. **Risk** *Policies and procedures are outdated and fail to reflect current regulatory requirements and up to date practices. Leading to an increased likelihood of information security breaches.*	All information policies and procedures were considered during the preparations for the implementation of GDPR and high risk processes were addressed, e.g. processes reviewed, privacy notices developed. A draft revised data protection policy was developed but further review of the suite of information management policies and procedures has resulted in the creation of a short life working group. Chaired by Head of Corporate Services, the group is reviewing all Information Management Policies, Procedures and Guidance with a view to developing one overarching Policy to be supported by appropriate procedures and guidance. Revised policy to be reported to Council Executive on 25 June 2019	High **Responsible Officer** Head of Corporate Services **Risk Identifier** WLC007 **Action Date** 25/06/2019

Ref	Findings and Risk	Agreed Action	Importance Level
3.9	**Information Security Officer (ISO)** No ISO has been appointed since the previous post holder left the council in August 2018. We consider that this role is vital to ensuring ongoing compliance with Information Security requirements The absence of such a post holder may have contributed to the weaknesses identified in this report. **Risk** *Failure to maintain effective information security policies and procedures, and failure to effectively monitor and report on compliance.*	The tasks of the Information Security Officer have been absorbed into the IT Technology and Solutions Manager role, which is currently filled on an interim role. This post holder is supported, in relation to security issues, by an Advanced Technical Specialist. The operational information management tasks of the Information Security Officer have been absorbed into the role of the Records Manager.	Medium **Responsible Officer** Head of Corporate Services **Risk Identifier** WLC007 **Action Date** Completed

APPENDIX A

DEFINITIONS OF AUDIT FINDINGS & AUDIT OPINION

AUDIT IMPORTANCE LEVELS

Importance levels of '**High'**, '**Medium'** or '**Low'** are allocated to each audit finding within the action plan.

These reflect the importance of audit findings to an effective system of internal control and must be considered in the context of the business processes being audited (Section 2 – Audit Remit).

AUDIT OPINION

Our overall opinion on the controls in place is based on the level of importance attached to the findings in our audit report. The overall audit opinions are as follows:

Overall Opinion	Definition
EFFECTIVE	No findings ranked as 'High' importance. There may be a few 'Low' and 'Medium' ranked findings.
SATISFACTORY	No findings ranked as 'High' importance however there are a moderate number of 'Low' and 'Medium' ranked findings.
REQUIRES IMPROVEMENT	A few findings ranked as 'High' importance. There may also be a number of findings ranked as 'Low' and 'Medium' importance.
UNSOUND	A considerable number of findings ranked as 'High' importance resulting in an unsound system of control. There may also be a number of findings ranked as 'Low' and 'Medium' importance.

APPENDIX B

Data Protection –Overview of Data Breach & Risk Assessments Process

Note: this relates to the process in place at the time the audit fieldwork was undertaken in November 2018

Process: Data Breach occurs

First 24 hours: Responsible officer - Head of Service or nominated officer.

Step 1 - identify the data which has been subject of the breach. Confirm whether this includes personal data.

Step 2 - Notify service manager and IT Service desk of the breach.

Step 3 - if personal data is involved, notify the Chief Solicitor. If not, the Chief Solicitor does not need to be involved. Service desk will notify Head of Service and Depute Chief Executive.

Within 2 days

Step 4 - identify and take any steps which require to be taken to contain the breach/recover the data and prevent further breach.

Step 5 - identify and take any steps which require to be taken to protect any individual from any effects of the breach.

Step 6 - Head of Service or nominated officer to complete Stage 1 risk assessment template (including the risk assessment table), save in the records management system and email a link to the document to the Depute Chief Executive, Chief Solicitor and Information Security Officer, for information. Where a nominated officer has conducted the risk assessment, the link to the document is also to be emailed to the Head of Service.

Step 7 - Where a breach is likely to result in a high risk to the rights and freedoms of individuals, Head of Service or nominated officer to notify those concerned directly.

Within 3 days

Step 8 - Chief Solicitor to advise the Depute Chief Executive by email whether the ICO should be notified of the breach. Depute Chief Executive to confirm by email, acceptance or otherwise of the Chief Solicitor's advice. Depute Chief Executive to provide a reason where their decision is against the recommendation of the Chief Solicitor.

Step 9 - ICO to be notified by Chief Solicitor, where appropriate.

Within 7 working days

Step 10 - Identify timeline of events which led to the data breach including names of staff involved, details of events, decisions made and actions taken in containing and recovering data at risk.

Step 11 - Identify outcomes and remedial actions which will prevent or mitigate the risk of future data breach.

Step 12 - identify any disciplinary issues to be investigated /actioned in relation to the staff involved in the breach.

Step 13 - Head of Service or nominated officer to complete the risk assessment table, save in the records management system and email a link to the document to the Depute Chief Executive, Chief Solicitor and Information Security Manager. Where a nominated officer has conducted the risk assessment, the link to the document is also to be emailed to the Head of Service.

Step 14 - Final details of incident to be notified by the Chief Solicitor to the ICO where necessary.

Within 10 working days

Step 15- Copy of risk assessment and email confirmation from Depute Chief Executive regarding notification (or not) to ICO to be saved in Meridio.

Within 14 days

Step 16 - All outcomes and remedial actions to be logged in Covalent as risk actions.

APPENDIX C

SUMMARY OF AUDIT FINDINGS

IT SECURITY INCIDENT PROCESS (FINDING 3.2)

(Review of 20 Security Incidents 2017/18 (12) and 2018/19 (8))

Main Steps – Notification and Escalation

- 3 cases appropriate notification was not sent to the relevant officers within 24 hours.
- 5 cases the requirement to complete a risk assessment was not sent to the relevant officers within 24 hours.
- 15 cases of non-receipt of a risk assessment and escalation was not followed up correctly and / or not completed within 7 days.

Call Diary / Attachments

Actions are logged in the incident Call Diary and marked complete once the appropriate e-mail is sent. There is inconsistency in saving copy e-mails in the 'Attachments' folder as evidence the task is complete.

- 16 cases the e-mail advising the ILO and DCE was not saved.
- 1 case the task requesting a risk assessment was marked complete, no e-mail was saved. It was later identified the original request had not being sent and was issued approximately 4 weeks late.
- 2 cases no actions were logged requesting a risk assessment but an assessment is on file.
- 1 case a risk assessment e-mail was available but the task had not been marked as complete.

Escalation of Outstanding Risk Assessments

The process of escalating outstanding risk assessments is not being followed correctly:

- 6 outstanding cases do not appear to have been escalated.
- 9 cases state that follow up e-mails have been sent but no evidence has been saved.
- No escalation of outstanding risk assessments has been undertaken since August.

APPENDIX D

SUMMARY OF AUDIT FINDINGS

RISK ASSESSMENT COMPLETION (FINDING 3.4)

(Review of 20 Security Incidents, 2017/18 (12) and 2018/19 (8))

Completion of Risk Assessments

Full Sign Off

- 8 forms correctly signed by the appropriate signatories.
- 7 cases only a word document on file, unable to validate sign off.
- 1 form no evidence of DCE or Chief Solicitor signature as final page missing.
- 1 case the form has not been signed by the Head of Service.
- 3 cases, no Stage 2 template on file, unable to validate sign off.

Legal Services Recommended Referral to ICO
Should be 10 days (pre GDPR) / 72 hours (post GDPR)

Analysis of Legal Services Data Breach Log

Services Reporting to Legal:

- 2 cases received in correct timescales
- 2 cases unable to verify timescales
- 11 cases not received by Legal in correct timescales
- 5 cases not detailed in log at all

ICO Decision:

- 10 cases ICO decision made in correct timescale upon receipt of information by Legal Services
- 5 cases unable to verify timescale.

Chief Solicitor Sign Off

- 2 cases were signed within the required timescales.
- 4 cases were signed 11, 13, 23 and 24 days after the incident.
- 1 case was signed 7 weeks after the incident
- 1 case was signed but not dated, unable to validate timescale.
- 1 case (post GDPR) was signed within 3 working days but not 72 hours.
- 1 case no evidence of Chief Solicitor signature as final page missing
- 7 cases only a word document on file, unable to validate sign off
- 2 cases no Stage 2 template on file, unable to validate sign off
- 1 case only Stage 1 template available, e-mail from Chief Solicitor stating happy to sign off. No evidence of decision to report to ICO available.

Depute Chief Executive Sign Off (within 7 Days)

- 2 cases were signed within the required timescales.
- 3 cases were signed 10, 11 and 13 days after the incident.
- 3 cases were signed 5, 7 and 15 weeks after the incident
- 1 form no evidence of DCE signature as final page missing
- 1 case had 5 signatories but no DCE signature on the form
- 7 cases only a word document on file, unable to validate sign off
- 3 cases no Stage 2 template on file, unable to validate sign off

Overdue Risk Assessment Templates

Risk assessments should be fully completed within 10 (old template) and 7 days (new template). As at 30th November 2018 there are 40 incidents that remain open with risk assessments outstanding. The breakdown per year is:

2016/17 – 3 incidents
2017/18 – 14 incidents
2018/19 – 23 incidents

Appropriate Remedial Action Taken

The proposed remedial action as detailed on the risk assessment was reviewed:

- 17 cases the proposed actions appeared reasonable and proportionate.
- 3 cases no action plan was completed.

APPENDIX E

SUMMARY OF AUDIT FINDINGS

ACCURACY OF REPORTING DATA (FINDING 3.6)

(Review of 2018 IMWG Minutes)

IMWG Minute - 17/1/18

Outstanding risk assessments discussed and importance stressed.

Security Incidents Logged on the IT Service Desk – December 2017:

39 Security Incidents logged,
38 Resolved

Breakdown:
Unauthorised Access: 1
Equipment Loss: 1
Email/Phishing: 27
Application: 6
No incident after investigation: 3

IMWG Minute - 27/2/18 (same data as reported in January 2018)

Reminder to look for trends in incidents only.

There were 39 Security Incidents logged in January 2018 with 38 resolved. These include:

Unauthorised Access: 1
Equipment Loss: 1
Email/Phishing: 27
Application: 6
No incident after investigation: 3

IMWG Minute - 10/4/18 (correct January figure reported in April 2018)

There were 35 **Security Incidents** logged in January 2018 with 33 resolved. These include:

Unauthorised Access: 1
Equipment Loss:4
Email/Phishing: 16
Application: 7

IMWG Minute - 3/7/18
Security Calls Logged on the IT Service Desk May & June 2018

May
Total Calls Logged – 41
Total Calls Resolved – 41

Breakdown:
2nd Line Education Road Call – 1
Access – 1
Application – 6
EDRMS – 1
Email – 1
Enquiry – 1
Internet – 2
First Line Resolve – 2
Phishing/SPAM – 16
Phishing/SPAM - Not Legitimate – 9
Second Line Resolve – 1

June
Total Calls Logged – 27
Total Calls Resolved – 22

Breakdown:
Application - 4
First Line Resolve – 1
Cyber – 4
Phishing/Spam – 6
Block/Remove -> Legitimate/rectify – 2
Not Legitimate, Block 4
Second Line Resolve 1

APPENDIX F

INFORMATION SECURITY BREACH PROCESS FLOW