

Essex County Council

PO Box 11,

County Hall,  
Chelmsford,  
Essex  
CM1 1QH

Our Ref: Information  
GovernanceS201704/01

Your Ref: ECC/Essex Fire  
Authority01-17

Date 28/4/2017

Dear Tracy

**Information Governance Support Information Governance Audit Report and  
Recommendations: Executive Summary**

We attended ECFRS HQ on the 12<sup>th</sup> and 13<sup>th</sup> of April 2017 and conducted 16 interviews with members of staff identified by the Performance & Data Manager.

We had received a pre-audit proforma from the Authority prior to the audit and an initial review of documentation was undertaken to inform activities onsite. This also highlighted issues already of concern to the Authority which are a focus for this report.

The audit highlighted the following key areas of non-compliance, and further below we provide highlights of those areas with the detailed findings for each area presented in the full audit report with recommendations on how compliance can be improved.

We have provided recommendations on compliance with the current Data Protection Act (1998), and in blue text we have further provided recommendations for complying with the General Data Protection Regulations (2016).

Whilst the outcome of the audit is 'No Assurance' it should be recognised that the staff interviewed demonstrated a clear drive to improve information governance within their own areas but appeared to lack the organisational framework, tools and resources to effect change.

**Main Audit Findings:**

*Governance Framework*

There was no evidence of a clear framework to support information governance within the Authority. This is a key building block for ensuring appropriate action resource and support is provided for compliance with information legislation.

*Reporting*

There is a lack of reporting to Service Leadership Team on areas of information governance compliance which means there is insufficient understanding of the current risk position to inform an effective strategy. Information risk is not therefore appropriately managed in line with the organisational risk appetite.

*Security Incidents*

There is no clear process or facility for effective centralised logging of security incidents. The Senior Information Risk Owner provided a copy of a Security Incident Policy during our interview however no other staff interviewed were aware of the policy. If there is no robust logging and analysing of security incidents and alignment to any relevant information risk it is difficult for the Authority to evidence effective management of risk to the regulator.

### *Records Management*

There was no evidence of a corporate approach ensure information is being recorded and managed according to a consistent and compliant set of standards. Starters with the Authority are not given adequate training on this expectation and processes for record keeping are learned 'on the job' without written processes and each team will have created its own practices independent of a central requirement.

### *Training*

Whilst there is good focus on operational training, this does not extend to information governance. There is a blend of eLearning and some face-to-face training but there is no evidence of a corporate strategy/ policy or procedures with regard to managing completion of training.

Key staff processing statutory requests appear to lack any appropriate training to enable them to carry out their roles effectively in meeting compliance

### *Risk Management*

There was no evidence provided of a risk management framework. As Service Leadership Team receives limited reporting on information governance activities, the associated risks cannot be properly managed. There is limited access to the risk management tool (software from JC Applications Development) and risks do not seem to be appropriately defined. We were advised that information risk was categorised as being 'reputational damage', however this is an impact rather than a risk.

Please review the report in full and provide your comments back to us by Friday 12<sup>th</sup> May or advise of any extension required in order to complete your review. If you would like to informally discuss these findings, please contact us to arrange a discussion.

Once we have your response we will provide you with a final report within 2 weeks

Our engagement is inclusive of template provision to support compliance and these will be made available once this report has been finalised and agreed.

Thank you for the opportunity to assist you in reviewing your current information governance compliance level. We hope the issues and recommendations provided can be used to improve information governance within the Authority. We are able to offer further support if required for example training and consultancy tailored to meet your identified needs. If you would like to discuss any further needs that we may be to assist you with, please contact us at [informationgovernancesupport@essex.gov.uk](mailto:informationgovernancesupport@essex.gov.uk)






# Information Governance Audit Report

## 1. Summary

|   |   |   |                   |  |          |   |   |                           |              |
|---|---|---|-------------------|--|----------|---|---|---------------------------|--------------|
| Organisation:   | Essex County Fire & Rescue Service  | Overall Opinion   | No Assurance      | Number of Governance Framework issues identified |          | Number of Privacy by Design issues identified |   | Number of Recommendations |              |
| Audit Sponsor:  | Tracey King   |   |                   | 4  | Critical | 1   | Critical  |                           | Made         |
| Distribution List:  | Tracey King, Mike Clayton, Shirley Jarlett  | Direction of Travel   | No previous audit | 5  | Major    | 3   | Major   | 124                       | tbc          |
| Final Report Issued:  | [Date]  |   |                   | 0  | Moderate | 4   | Moderate  |                           | N/A Rejected |
| Date of last review:  | N/A   |   |                   | 1  | Low      | 0   | Low   |                           | Major N/A    |
| Scope of the Review and Limitations:  | This audit assessed the level of compliance of the organisation with the requirements of relevant applicable statutory provisions of legislation governing the management of and access to data; namely the Data Protection Act 1998 (superseded by the General Data Protection Regulations 2016), the Freedom of Information Act 2000, the Environmental Information Regulations 2004 and the Privacy of Electronic Communications Regulations 2003. |   |                   |  |          |   |   |                           |              |
| Critical and Major Findings and Recommendations <ul style="list-style-type: none"><li>Governance Framework</li><li>Reporting</li><li>Security Incidents</li><li>Records Management</li><li>Training</li><li>Risk Management</li></ul> |   | Governance Framework  |                   |  |          |   | Each risk area for this review is shown as a segment The key to the colours on the wheel is as follows: <div><div></div>Critical priority Control Design or Control Operating in Practice issues identified</div> <div><div></div>Major priority Control Design or Control Operating in Practice issues identified</div> <div><div></div>Moderate priority Control Design or Control Operating in Practice issues identified</div> <div><div></div>No / Minor Control Design or Control Operating in Practice Issues identified</div> |                           |              |
|   |   | <div><div>Roles</div><div>Policy</div><div>Report</div><div>Notify</div><div>Assets</div><div>ROPA</div><div>Training</div><div>Records</div><div>Risk</div><div>Commercial</div></div> |                   |  |          |   |   |                           |              |
|   |   | Privacy By Design   |                   |  |          |   |   |                           |              |
|   |   | <div><div>Requests</div><div>Incidents</div><div>Assessments</div><div>Notices</div><div>Consent</div><div>Photo/Video</div><div>CCTV</div><div>Security</div></div>                    |                   |  |          |   |   |                           |              |
|   |   |   |                   |  |          |   |   |                           |              |





|   |   |
|---|---|
| <b>Auditor:</b> Lauri Almond/ David Humphreys<br><br><b>Fieldwork Completed:</b> 13/4/2017<br><br><b>Draft Report Issued:</b> 28/4/2017<br><br><b>Management Comments Expected:</b> 12/5/2017<br><br><b>Management Comments Received:</b> [Date]<br><br><b>Final Report:</b> [Date] | <b>Releasing Audit Reports:</b> Draft and final reports are retained by Essex County Council for 6 years and only distributed outside the Council's Information Governance Team to the named individuals on the distribution list above. Approval for distributing this report wider should be sought from the relevant Audit sponsor. Care must be taken to protect the control issues identified in this report.<br><br><b>Risk Management:</b> The management of the following risks has been reviewed in this audit. Where appropriate, the Audit Sponsor is responsible for adding new risks identified to the organisation's risk register. |
|---|---|

## Risks Reviewed

| Risk Ref: | Risk:   | Risk already identified? | Impact:      | Likelihood:  | Risk Rating: | Risk managed   |
|-----------|---|--------------------------|--------------|--------------|--------------|--|
| 01        | Immature information governance cannot effectively evidence current practices to the regulator <ul style="list-style-type: none"> <li>Regulator would interpret as systemic failing and would increase likelihood of high monetary penalty in the event of scrutiny</li> </ul>  | No                       | Critical (4) | Major (3)    | Critical     |   |
| 02        | Authority data is lost/ processed in a non-compliant manner due to gaps in policy and processes <ul style="list-style-type: none"> <li>Deriving from vulnerabilities in mover/ leaver processes, Authority device management and access from personal devices</li> </ul>  | No                       | Major (3)    | Major (3)    | Major        |   |
| 03        | Breach of Information Governance policies due to lack of awareness, communication and training <ul style="list-style-type: none"> <li>Where employee education needs are not effectively analysed and met, practice will not be compliant with policy</li> </ul>  | No                       | Major (3)    | Major (3)    | Major        |   |
| 04        | Authority data is shared inappropriately/ illegally due to insufficient understanding of legislation <ul style="list-style-type: none"> <li>Deriving from insufficient knowledge of legislation to develop effective sharing process which provide employees with confidence in disclosing data through legitimised routes</li> </ul> | No                       | Major (3)    | Moderate (2) | Moderate     |   |
| 05        | Suppliers breach information legislation through lack of contractual controls <ul style="list-style-type: none"> <li>Deriving from lack of clarity on compliance expectations in contracts and agreements and ineffective controls over third party access</li> </ul>   | No                       | Major (3)    | Moderate (2) | Moderate     |  |


**All issues identified above carry the risk of monetary penalties and/ or publication of failings by the regulator, with the strong likelihood of loss of confidence from the public and partner organisations in providing and sharing data; which will have implications for the Authority's ability to successfully deliver services.**

## 2. Basis of our opinion and assurance statement

| Risk rating  | Assessment rationale   |
|--|--|
| <br><b>Critical</b> | <p>Major financial loss – Large increase on project budget/cost: (Greater of <b>£1.0M</b> of the total Budget or more than <b>15 to 30%</b> of the organisational budget). Statutory intervention triggered. Impacts the whole Organisation. Cessation of core activities. Strategies not consistent with government's agenda, trends show service is degraded.</p> <p>Failure of major projects – Senior Managers/ Governing bodies are required to intervene. Intense political and media scrutiny i.e. front-page headlines, TV. Possible criminal, or high profile, civil action against the organisation and its employees.</p> <p>Life threatening or multiple serious injuries or prolonged work place stress. Severe impact on morale &amp; service performance. Strike actions etc.</p> |
| <br><b>Major</b>    | <p>High financial loss – Significant increase on project budget/cost: (Greater of <b>£0.5M</b> of the total Budget or more than <b>6 to 15%</b> of the organisational budget). Service budgets exceeded. Significant disruption of core activities. Key targets missed, some services compromised. Management action required to overcome medium term difficulties.</p> <p>Scrutiny required by external agencies, Audit Commission etc. Unfavourable external media coverage. Noticeable impact on public opinion.</p> <p>Serious injuries or stressful experience requiring medical treatment, many workdays lost. Major impact on morale &amp; performance of more than 50 staff.</p>   |
| <br><b>Moderate</b> | <p>Medium financial loss – Small increase on project budget/cost: (Greater of <b>£0.3M</b> of the total Budget or more than <b>3 to 6%</b> of the organisational budget). Handled within the team. Significant short-term disruption of non-core activities. Standing Orders occasionally not complied with, or services do not fully meet needs. Service action will be required.</p> <p>Scrutiny required by internal board to prevent escalation. Probable limited unfavourable media coverage.</p> <p>Injuries or stress level requiring some medical treatment, potentially some workdays lost. Some impact on morale &amp; performance of up to 50 staff.</p>  |
| <br><b>Low</b>      | <p>Minimal financial loss – Minimal effect on project budget/cost: (<b>&lt; 3%</b> Negligible effect on total Budget or <b>&lt;1%</b> of organisational budget)</p> <p>Minor errors in systems/operations or processes requiring action or minor delay without impact on overall schedule. Handled within normal day-to-day routines.</p> <p>Internal review, unlikely to have impact on the corporate image.</p> <p>Minor injuries or stress with no workdays lost or minimal medical treatment. No impact on staff morale.</p>   |
| Level of assurance   | Description  |
| <b>Good</b>  | <b>Good assurance</b> – there is a sound system of internal control designed to achieve the objectives of the system/process and manage the risks to achieving those objectives. Recommendations will normally only be of Low risk rating. Any Moderate recommendations would need to be mitigated by significant strengths elsewhere.   |
| <b>Adequate</b>  | <b>Adequate assurance</b> – whilst there is basically a sound system of control, there are some areas of weakness, which may put the system/process objectives at risk. There are Moderate recommendations indicating weaknesses but these do not undermine the system's overall integrity. Any Critical recommendation will prevent this assessment, and any Major recommendations relating to part of the system would need to be mitigated by significant strengths elsewhere.  |
| <b>Limited</b>   | <b>Limited assurance</b> – there are significant weaknesses in key areas in the systems of control, which put the system/process objectives at risk. There are Major recommendations or a number of moderate recommendations indicating significant failings. Any Critical recommendations relating to part of the system would need to be mitigated by significant strengths elsewhere.   |
| <b>No</b>  | <b>No assurance</b> – internal controls are generally weak leaving the system/process open to significant error or abuse or reputational damage. There are Critical recommendations indicating major failings  |


**Auditors' Responsibilities** It is management's responsibility to develop and maintain sound systems of risk management, internal control and governance and for the prevention and detection of irregularities and fraud. Audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems. We shall endeavour to plan our work so that we have a reasonable expectation of detecting significant control weaknesses. However, Audit procedures alone, even when carried out with due professional care, do not guarantee that non-compliance will be detected. Accordingly, our examinations as auditors should not be relied upon solely to disclose non –compliant practices, unless we are requested to carry out a special investigation for such activities in a particular area.

### 3. Recommendations

| Matters Arising  | Recommendations   | Priority & Risk   | Management Response and Agreed Actions  |
|--|---|---|---|
| <b>3.1. Governance Framework</b>   |   |   |   |
| <b>a) Roles &amp; Responsibilities</b>   |   |   |   |
| <ol style="list-style-type: none"> <li>1. No Information Governance Framework is in place. An effective framework provides for effective reporting to strategic leaders with clear roles and accountability. This informs strategy for risk tolerance, policy and training whose effectiveness is reflected in the reporting. The current lack of a framework results in no visibility of risks by the leadership, decision makers or data handlers</li> <li>2. Role holders have not received formal training for their role</li> <li>3. Job Descriptions do not specify the responsibilities aligned to Information Governance roles, e.g. Senior Information Risk Owner's job description for substantive role does not reference the Senior Information Risk Owner role</li> <li>4. No clear terms of reference for group or board role in the information governance framework</li> <li>5. <a href="#">No appointment made to the Data Protection Officer role (a statutory role under the General Data Protection Regulation)</a></li> </ol> | <ol style="list-style-type: none"> <li>1.1. An Information Governance Framework is required to ensure that roles and responsibilities are defined, and all staff have clarity on how to handle and escalate information risks</li> <li>1.2. Ensure clear routes to Service Leadership Team for raising information related concerns – Senior Information Risk Owner <a href="#">Senior Information Risk Owner responsibilities</a> should be incorporated into the relevant officer's job description</li> <li>2.1. Senior Information Risk Owner role training and annual refresher training</li> <li>2.2. Ensure staff with responsibility for information management and compliance are appropriately trained and experienced</li> <li>4. Job descriptions to be updated to fully capture responsibilities of Information Governance additional roles</li> <li>5.1. Establish a Terms of Reference for the Service Leadership Team Information Governance sub group to support this work.</li> <li>5.2. Amend terms of reference for existing</li> </ol> | <br>Critical | <b>Agreed:</b> Mike Clayton   |
|  |   | <b>Link to Risk(s):</b><br>1  | <b>Action to be taken:</b><br>Information Governance Framework to be drawn up, FD&T Job Description to be amended to reflect SIRO responsibilities, and longer term placing of the role to be agreed. Information Asset Owners in each department to be identified and a development plan for them put in place. Information Asset Owners to have Job Descriptions amended to reflect role. |
|  |   |   | <b>Additional Resources Required for implementation:</b> Use of external specialist to help develop information asset owners.   |

|  |   |  |   |
|--|---|--|---|
|  | groups to incorporate their role within the Information Governance framework  |  | <b>Responsible Officer:</b> Mike Clayton FD&T |
|  | 6. <a href="#">General Data Protection Regulation Data Protection Officer</a> must be assigned with full account taken of the statutory requirements as regards knowledge, skills and conflicts of interest (e.g. there is a clear conflict if the role is assigned to a person with strategy-setting focus)... |  | <b>Target Date:</b> 31 December 2017          |


## b) Policy

|   |  |  |  |
|---|--|--|--|
| <ol style="list-style-type: none"> <li>1. Policies are presented in a variety of formats with little corporate consistency. Focus is on expressing detail and not on ease of consumption for staff. Inaccessible policy messages result in lack of understanding and unwillingness to commit to engaging with the documents.</li> <li>2. Information Policies do not all sit with the team with information management responsibilities, they are shared out with other teams, e.g. Human Resources, Health &amp; Safety etc which results in policy reviews not capturing the necessary input from specialists. This results in policies not covering all points required to achieve compliance with the legislation.</li> <li>3. There is no corporate record of policy changes to support policy reviews and to understand changes over time to support breach investigations. This means the Authority will find difficulty in pinpointing when policy changed and will struggle to police breaches effectively over time.</li> </ol> | <ol style="list-style-type: none"> <li>1. Move to the 'Policy on a Page' model (template supplied) to ensure your policies are easy for your staff to understand and consume; and conform to a corporate template</li> <li>2. All information management focussed policies to be owned and managed by the Performance and Data Team</li> <li>3. A policy review log should be initiated, capturing version changes, and providing the opportunity to collate issues/resolutions ahead of the policy review</li> <li>4. Create and implement a defined process to identify gaps in policy, draft changes and review. This to include clear approval routes</li> <li>5. Ensure the organisation drafts and approves policies in the following areas: <ul style="list-style-type: none"> <li>• Data Protection</li> <li>• Freedom of</li> </ul> </li> </ol> | <br>Major | <b>Agreed:</b> Tracy King  |
|   |  | <b>Link to Risk(s):</b><br>2,3   | <b>Action to be taken:</b> All policies to be reviewed, amended and aligned to corporate policy template through policy review processes. Policies to be held in JCAD as controls for specific risks. Following Information Policies to be agreed: • Data Protection<br>Freedom of Information/Environmental Information Regulation; Consent; Privacy Notices; Records Management; Communications; Social Media; Security Incident |



|   |  |  |   |
|---|--|--|---|
| <p>4. There is no clear corporate approach to creating and amending policy.</p> <p>5. A number of key policies are currently in draft form. These are not new versions of existing policies, but are designed to fill policy 'gaps'. There is therefore currently no policy control in those areas to provide to a regulator or the public to provide assurance</p> | <p>Information/Environmental Information Regulation</p> <ul style="list-style-type: none"> <li>• Consent</li> <li>• Privacy Notices</li> <li>• Records Management</li> <li>• Communications</li> <li>• Social Media</li> <li>• Security Incident Handling</li> <li>• Privacy Impact Assessment</li> <li>• Information Asset Management</li> <li>• Electronic Imaging (Video/Drones/Body Worn Cameras)</li> </ul> |  | <p>Handling; Privacy Impact Assessment; Information Asset Management; Electronic Imaging (Video/Drones/Body Worn Cameras).</p>            |
|   |  |  | <p><b>Additional Resources Required for implementation:</b> 3-Days per week planned for in Performance and Data Structure for 2017/18</p> |
|   |  |  | <p><b>Responsible Officer:</b> Tracy King AD Performance</p> <p><b>Target Date:</b> 31 December 2017</p>                                  |


### c) Reporting

|  |  |  |   |
|--|--|--|---|
| <p>1. There are some areas of the business who do routinely report into Service Leadership Team regarding compliance issues, e.g. Safeguarding &amp; Health &amp; Safety. There was no evidence of regular reporting to Service Leadership Team or Senior Information Risk Owner on compliance regimes, e.g. Freedom of Information/Environmental Information Regulations compliance, Subject Access Requests compliance, information risk management and Security Incidents. The lack of visibility this leads to for Service Leadership Team does not allow them to fully appreciate the information risks, or form effective plans to</p> | <p>1. Incorporate reporting on the following areas into the Organisation Performance report, at a minimum containing statistical representation of performance across the following regimes:</p> <ul style="list-style-type: none"> <li>• Freedom of Information/Environmental Information Regulations compliance</li> <li>• Subject Access Requests compliance</li> <li>• Information Security</li> <li>• Security Incidents</li> <li>• Complaints</li> </ul> |  <p>Critical</p> | <p><b>Agreed:</b> Tracy King</p>  |
|  |  | <p><b>Link to Risk(s):</b> 1,3</p>   | <p><b>Action to be taken:</b> Quarterly reporting to include data on information related requests, and information security. Targets to be agreed for reporting metrics. Quarterly and Annual report to Service Leadership Team.</p> <p><b>Additional Resources</b></p> |




|   |   |  |  |
|---|---|--|--|
| <p>mitigate.</p> <p>2. The organisation does not set expectations around performance in order to demonstrate Information Governance compliance. Information Governance staff therefore do not have strategic goals to work towards and wider staff whose cooperation the Information Governance staff rely on to meet compliance are not made aware of corporate expectation</p> <p>3. In the event of an information security incident the regulator (Information Commissioner's Office) may require you to produce compliance figures and your risk and strategic approach in order to inform their decision making process. At present, the organisation could produce some data on demand, but there is low confidence in its inaccuracy, would present an accurate picture and would not provide assurance of well monitored activity and a strategic approach</p> | <ul style="list-style-type: none"> <li>Records Management</li> <li>Information risk management</li> </ul> <p>2. Service Leadership Team to set Service Level Agreements for reporting activities to drive performance and to enable summarised reports to focus on areas of activity falling outside of the risk acceptance range</p> <p>3. Introduce an annual report to Senior Information Risk Owner in all information risks and assets in order to support annual improvement plans within the strategic objective setting cycle</p> |  | <b>Required for implementation:</b> Requirement for additional resources not known at this time. |
|   |   |  | <b>Responsible Officer:</b> [Tracy King AD Performance   |
|   |   |  | <b>Target Date:</b> 31 December 2017   |

#### d) Notifying

|   |   |  |   |
|---|---|--|---|
| <p>1. Currently notified to the Information Commissioners Office. Performance and Data service's awareness of the requirement has resulted in timely compliance and there is awareness that the current notification is due to expire</p> | <p>1. Due for renewal in June 2017, however be aware that notification arrangements will change under the General Data Protection Regulation so monitor messages sent out by the ICO to ensure compliance in this area.</p> | <br>Low | <b>Agreed:</b> Tracy King   |
|   |   | <b>Link to Risk(s):</b><br>-   | <b>Action to be taken:</b><br>Registration to be reviewed with Information Asset Owners and as and when ICO guidance changes. |
|   |   |  | <b>Additional Resources Required for implementation:</b> None   |

|  |  |  |  |
|--|--|--|--|
|  |  |  | <b>Responsible Officer</b> Tracy King AD Performance |
|  |  |  | <b>Target Date:</b> 31 December 2017                 |

#### e) Asset Registers


|   |   |   |   |
|---|---|---|---|
| <p>1. There is no evidence of an information asset register. The lack of such a register creates risks for effective information management.</p> <p>2. As there is no asset register it follows that there are no recorded or assigned asset owners or managers who can manage any related risks to those assets, and there is no process to maintain a register.</p> | <p>1. Compile Information Asset Register</p> <p>2.1. Assign Information Asset Owners and Managers</p> <p>2.2. Ensure training is given to IAO/Ms</p> <p>2.3. Ensure regular reporting to IAO/Ms to verify accuracy of their asset entries in the register</p> <p>2.4. Ensure regular review process to ensure the register remains accurate</p> |  | <b>Agreed:</b> Tracy King   |
|   |   | Critical  |   |
|   |   | <b>Link to Risk(s):</b><br>1  | <b>Action to be taken:</b><br>Departmental Asset Owners to be identified. Work with them to identify information held and compile information asset register. Information Asset Owners to receive development in their role |
|   |   |   | <b>Additional Resources Required for implementation:</b> External support for development   |
|   |   |   | <b>Responsible Officer:</b> Tracy King AD Performance   |
|   |   |   | <b>Target Date:</b> 31 December 2017  |

#### f) Records of Processing Activity

|  |  |   |                           |
|--|--|---|---------------------------|
| 1. No current records meeting the evidential requirements of the General Data Protection | 1.1 Review existing regulator guidance and the detail in the General Data Protection Regulation. Further |  | <b>Agreed:</b> Tracy King |
|--|--|---|---------------------------|


|            |  |                                |   |
|------------|--|--------------------------------|---|
| Regulation | <p>guidance will be issued by the regulator in due course</p> <p>1.2 Compile Information asset register,</p> <p>1.3 Complete data flow mapping across all areas of the business and then combine with other General Data Protection Regulation Article 30 requirements (e.g. legal basis, categories of data, recipients and subjects).</p> <p>1.4 Ensure all data flows link through to the PIA, privacy notice and any supporting contract or information sharing protocols.</p> | Major                          |   |
|            |  | <b>Link to Risk(s):</b><br>1,4 | <b>Action to be taken:</b><br>Methodology for managing information to be determined and workshops held with information assets owners to ensure a consistent approach across every department.  |
|            |  |                                | <b>Additional Resources Required for implementation:</b><br>Departments to be supported in the development of their information asset owners and managers.<br><br>Temporary Business Analyst required to assist departments with Data Flow Mapping. |
|            |  |                                | <b>Responsible Officer</b> Tracy King AD Performance<br><br><b>Target Date:</b> 31 December 2017  |

#### g) Training

|  |   |  |  |
|--|---|--|--|
| <p>1. There is no consistent policy or strategy governing all training across all elements of information governance.</p> <p>2. There is a 3-month probation process for all new staff to complete relevant training before their induction can be passed, but this is not monitored/enforced and contains little reference to</p> | <p>1.1. A clear corporate strategy, policy and guidance is required and compliance must be monitored and documented.</p> <p>1.2. Security incidents analysis and areas of concern from the Senior Information Risk Owner's report should inform areas for greater focus when planning</p> | <br>Major | <b>Agreed:</b> Claire Budgen   |
|  |   | <b>Link to Risk(s):</b>  | <b>Action to be taken:</b> Existing corporate training on information governance to be |

|  |   |   |  |
|--|---|---|--|
| <p>Information Governance matters. Consequently staff begin work with no formal expectations set on data management and confidentiality and rely on verbal undocumented process training on the job.</p> <p>3. There is no central system which can report on the successful completion of required learning across all staff and courses. The eTask system can report but is limited to training for operational staff which does not include Information Governance training. For some learning e.g. Data Protection, staff were asked to verify completion by email as proof an individual has completed the training. There was no test of the learning and some interviewees questioned its value. It was noted that an eLearning platform procurement business case is near completion.</p> <p>4. There is insufficient profiling and identification of role-specific training needs where key roles require more detailed or role-specific Information Governance training.</p> <p>5. No standard reporting to Service Leadership Team, except for operational training via eTask</p> | <p>training strategy</p> <p>3.1. Information provided at Induction needs to be reviewed and updated to reflect corporate standards and the requirements of GDPR</p> <p>3.2. Progress procurement and implementation of an eLearning platform capable of compiling statistics/ KPIs required</p> <p>3.3. Annual training on data protection is required for all staff as part of assurance evidence</p> <p>3.4. There are no consistent mechanisms in place to capture effectiveness of awareness raising</p> <p>4. Enhanced training is necessary for those staff with information management responsibilities. Such roles to be identified and matched to training needs with appropriate content then developed. Needs to be reviewed annually.</p> <p>5. Service Leadership Team to be provided with quality training completion data as part of the recommended reporting process</p> | 3 | strengthened. Departmental managers to be supported in identifying training and development needs for information asset owners and managers. Role of information governance in induction process to be reviewed. |
|  |   |   | <b>Additional Resources Required for implementation:</b> External training spend on trainers.  |
|  |   |   | <b>Responsible Officer:</b> Claire Budgen, Head of Learning and Development  |
|  |   |   | <b>Target Date:</b> 31 December 2017   |

#### h) Records Management

|  |   |  |  |
|--|---|--|--|
| <p>1. Unnecessary retention of records has been highlighted in recent internal and external audit reports and a high level retention policy has been produced to assist staff in managing review decisions. Holding onto data past retention periods adds to workload for Freedom of Information/Subject Access Requests etc</p> | <p>1. Review retention schedule to provide more detailed breakdown of record types and corresponding retention periods, highlighting any legal basis for the periods adopted as policy</p> <p>2. A Records Management policy should be introduced which clearly defines</p> | <br>Major | <b>Agreed:</b> Roy Carter  |
|  |   | <b>Link to Risk(s):</b>  | <b>Action to be taken:</b> Existing records management policy to be reviewed in the light of the |


|  |   |   |   |
|--|---|---|---|
| <p>Some staff interviewed were aware of a retention policy but not of supporting processes of recording disposition decisions. There was no clear understanding of who was authorised to approve deletion.</p> <p>Retention practice for Personal Record Files does not make provision for extended retention periods for staff in roles which require DBS checks</p> <p>2. There is no standard guidance to Asset Owners, Asset Managers or staff at any level on the Service's expectations of quality data recording, where and how records should be managed. Each department has been free to develop practices independently.</p> <p>3. There is no clear policy statement regarding the use of personal drives for storing business data, and no analysis of the amount of data held in these locations despite capacity issues and generous storage allowances</p> <p>4. Anecdotal evidence that operational environments retain duplicated paper and electronic data after being supplied to support teams for storing as definitive records. Practices with such records are not known and not documented</p> <p>5. Although there is a facility at HQ for secure paper document disposal, there is no policy statement enforcing use. Staff have no guidance on what data should be disposed of using this process.</p> <p>6. Staff interviewed could not all verify that the systems they owned had either the functionality to delete records or whether this was being actively used in a documented managed process</p> | <p>ownership of information assets and the responsibilities of all staff to create and maintain quality information in a manner which supports business continuity and ease of access to those with the appropriate rights</p> <p>3. Policy to make clear how destruction decisions need to be approved and documented.</p> <p>4. Policy to make clear how personal drives can be used and to review storage allowance, regularly reporting on usage statistics to monitor policy compliance</p> <p>5. Policy to provide clear guidance on how records should be managed in operational areas after transfer of copies of data to support teams</p> <p>6. Review the deletion capability of all systems which hold personal data and document the functionality and supporting processes to utilise this in retrospective privacy impact assessments. Ensure future new or upgraded systems have this capability.</p> | 2 | identification of information assets.                           |
|  |   |   | <b>Additional Resources Required for implementation</b><br>None |
|  |   |   | <b>Responsible Officer:</b> Roy Carter, Service Solicitor       |
|  |   |   | <b>Target Date:</b> 31 December 2017                            |

## i) Risk Management

|   |  |  |  |
|---|--|--|--|
| <p>1 ECFRS use J C Applications Development (JCAD) to record their organisational risks, however we were advised that only the H&amp;S Manager has access to JCAD. There appears to be a lack of visibility for SLT of organisational risks</p> <p>2 In interview the Senior Information advised that risks are recorded as either reputational or financial risks, however these terms are 'impacts' as opposed to 'risks', so more depth, accuracy and clarity is needed when recording risks</p> | <p>1 Risk needs to be clearly understood by staff in order that management and senior leaders are able to manage those risks, tolerating or treating according to the organisations risk appetite</p> <p>1.3. Ensure there is a clear risk framework, and staff are aware of the roles and responsibilities assigned under the framework</p> <p>1.4. Ensure adequate risk management training is provided to key staff</p> <p>1.5. Consider including information asset owners/managers as part of your risk framework</p> | <div data-bbox="1563 229 1619 288"></div> <p>Critical</p> <p><b>Link to Risk(s):</b><br/>1</p> | <p><b>Agreed:</b> Charles Thomas</p> <p><b>Action to be taken:</b> Essex Fire Authority use software from JC Applications Development to record their organisational risks. All Senior Leadership Team members, and other managers not on the Senior Leadership Team, have access to JC Applications Development software. In addition, Senior Leadership Team members have sight of every register on the recording system as part of the Senior Leadership Team Service management. The Strategic Risk Register has a risk around governance processes. Following this audit, a specific risk around information governance will be added. Risk appetite is a matter that the Senior Leadership Team will have to reconsider in the round, and not just about information governance. There is a very clear risk strategy and a day-to-day guidance document, both of which will be amended following a recent</p> |
|---|--|--|--|

|  |  |  |  |
|--|--|--|--|
|  |  |  | internal audit report, and taking account of likely changes to Service governance arrangements as we move towards new governance arrangements under the PCC. |
|  |  |  | <b>Additional Resources Required for implementation:</b> None  |
|  |  |  | <b>Responsible Officer:</b> [Charles Thomas, Risk and Business Continuity Manager  |
|  |  |  | <b>Target Date:</b> 31 December 2017   |

#### j) Commercial


|   |   |  |  |
|---|---|--|--|
| <p>1 There are Framework contracts as well as individual service contracts, and a mix of Information Technology suppliers and service delivery suppliers. It is good that risk in commercial is assessed not only in accordance with its contractual value.</p> <p>2 There was no awareness of whether current contract for Information Technology services have support from outside the EEA – this needs to be reviewed</p> <p>3 It was acknowledged that there is currently no contract compliance auditing, but it was recognised that this is essential moving forwards</p> <p>4 <a href="#">New Contracts lead, well informed, recognises scale of work to be done. Will seek support for</a></p> | <p>1. Any transfers to 3<sup>rd</sup> countries must be supported by binding corporate rules and standard contract clauses</p> <p>2. Review Information Technology support contracts to establish which country 2<sup>nd</sup> &amp; 3<sup>rd</sup> line support is from</p> <p>3. Ensure that contract compliance checks are routinely carried out and documented</p> <p>4.1. <a href="#">Consider accessing some specific outsourcing training on General Data Protection Regulation requirements</a></p> <p>4.2. <a href="#">Ensure you communicate the requirements of the General Data Protection Regulation to your suppliers</a></p> | <br>Major | <b>Agreed:</b> Mike Clayton  |
|   |   |  | <b>Link to Risk(s):</b> 2,4,5  |
|   |   |  | <p><b>Action to be taken:</b> Contract terms to be reviewed and new standard terms introduced where required.</p> <p><b>Additional Resources Required for implementation:</b> None</p> <p><b>Responsible Officer:</b> Mike Clayton<br/>Finance Director  &amp; Treasurer</p> |



|  |  |  |                                      |
|--|--|--|--------------------------------------|
| General Data Protection Regulation elements which we ran through during the interview. Generally there was recognition that contracts need to be strengthened ahead of any additional requirements for General Data Protection Regulation compliance |  |  | <b>Target Date:</b> 31 December 2017 |
|--|--|--|--------------------------------------|

## 3.2. Privacy by Design

### a) Statutory Requests


|   |   |  |  |
|---|---|--|--|
| <p><i>Freedom of Information (Freedom of Information) and Environmental Information Regulations (Environmental Information Regulations) requests:</i></p> <ol style="list-style-type: none"> <li>Freedom of Information requests are logged, but there is no countdown timeline to ensure timely chases to raise compliance</li> <li>No recognition of the Environmental Information Regulations – staff believe no such requests received by the Service. Freedom of Information is not perceived to be important to front line staff, however these are statutory requests</li> <li>Freedom of Information responses do not contain some of the legal requirements for responses, such as refusal notices or exemption explanations.</li> <li>Did not see No evidence provided in relation to the completion of public interests or prejudice tests required by some exemptions in the Act.</li> <li>Limited training, and what was received was too detailed a level and confusing. Freedom of Information eLearning was too simplistic, so hard to fail</li> <li>Poor records management makes locating and preparing information for disclosure difficult</li> </ol> | <p><i>Freedom of Information/Environmental Information Regulations</i></p> <ol style="list-style-type: none"> <li>Update Excel logging sheet with a 'countdown clock', including colour changes – green for days 1 – 9, amber for days 10 – 16, red for days 17 – 20</li> <li>Ensure staff are trained to recognise the relevant legislation for responding to statutory requests</li> <li>Ensure staff are adequately trained to understand the relevant law and how to write legally compliant responses, including the application of exemptions within the Act</li> <li>Staff would benefit from a template approach to responses, this will standardise and improve responses, saving time and embedding learning for the staff collating responses. Templates are available as part of our training package.</li> <li>Awareness campaign and training required for all staff to ensure they understand the organisations duty to</li> </ol> | <br>Major | <b>Agreed:</b> Tracy King  |
|   |   |  | <p><b>Link to Risk(s):</b><br/>2,4</p> <p><b>Action to be taken:</b> Tracking of FOI/EIR/SAR requests to be improved and additional data held. Further staff development to be undertaken.</p> |
|   |   |  | <p><b>Additional Resources Required for implementation:</b> Support for external development.</p>  |
|   |   |  | <p><b>Responsible Officer:</b> Tracy Kind AD Performance</p> <p><b>Target Date:</b> 31 December 2017</p>   |

|  |  |  |  |
|--|--|--|--|
| <p>7 No regular reporting path for senior leader awareness of performance – done on demand when needed</p> <p>8 Internal reviews are completed by the Clerk, meaning no “lessons learned” are captured by the team members as they do not see those responses. It appears they come back into the Authority to the ECFRS Solicitor, but are not fed through to the team responsible for the completion of requests</p> <p>9 Failure to respond to requests within the statutory timescale is a breach of the legislation and creates risk for the Authority</p> <p>10 Staff requested to provide information to satisfy a request do not always receive full and explanatory information, which can lead to delays in responses</p> <p><i>Subject Access Requests (Subject Access Requests):</i></p> <p>1 All staff records from 2011 have been digitised, so only ex-employees files are held in paper copy offsite storage. The retrieval process works well and there is a contract in place. There does not appear to be a full documented process for handling Subject Access Requests. No central logging of Subject Access Requests. in the fullest</p> | <p>respond to requests; and to ensure that information is located and provided within the legal timescales</p> <p>6 Improve records management to enable timely access to requested data</p> <p>7 Regular reporting to Service Leadership Team to ensure visibility of risk of poor performance</p> <p>8 All internal reviews must be copied to the responsible officer to ensure lessons learned are captured and understood. This also allows appropriate and full record keeping in relation to statutory requests, something the ICO will ask for following complaints or as part of an audit</p> <p>9 Treat overdue Freedom of Information responses as security incidents to ensure the risk is fully captured</p> <p>10 Use email template when requesting data from teams to fulfil a requests, stating the statutory nature of the request, timescales for response, and outcomes for non-provision of data</p> <p><i>Subject Access Requests:</i></p> <p>1. Full Subject Access Requests process to be documented, including log and a suite of template letters for communicating with requestors, e.g. acknowledgement, ID requests, provision letters including redaction explanations etc.</p> <p>2. Training required for key staff (HR and anyone else processing Subject Access Requests). We are able to</p> |  |  |
|--|--|--|--|


|  |   |  |  |
|--|---|--|--|
| <p>sense<br/>For staff Subject Access Requests systems are searched, however emails must also be disclosed where requested, and this does not appear to be current practice. A process needs to be documented to manage this. Searches for staff files did not appear to extend to previous managers and systems outside the PRF record, unless the request received made specific reference to it.</p> <p>2 Essex Legal Services (ELS) complete some Subject Access Requests – Essex Fire Authority supply data to ELS for redaction. Essex Fire Authority do not know if a request has been fulfilled by ELS or when. So no record of compliance with timescales. There is uncertainty amongst the workforce as to who is responsible for responding to Subject Access Requests. There is no confidence internally on what should be redacted before disclosures identifying a training need.</p> <p>3 There is uncertainty over who is doing the required identification verification process required before any work can commence in relation to the Subject Access Requests. There is an assumption by ECFRS staff that ELS carry out this part of the process. If a clear verification process is not defined and understood by staff it exposes the organisation to significant risk</p> <p>4 Where cases are prepared internally for disclosure there does not appear to be any facility for electronic redaction, relying on a manual process which is costly in both monetary and resource terms.</p> <p>5 <a href="#">Be aware of changes under the General Data Protection Regulation affecting the processing of</a></p> | <p>provide targeted training for both Subject Access Requests and Freedom of Information/Environmental Information Regulations if required.</p> <p>3. Logging mechanism must be introduced to verify compliance level, verify ID checks, and manage requests appropriately</p> <p>4. Recommend redaction software, e.g. Adobe Pro, Rapid Redact is procured to ease manual processes open to human error and lacking security; in areas such as HR (Subject Access Requests), Finance (transparency Code publishing), Occupational Health (Reports).</p> <p>5. <a href="#">Ensure whatever logging processes you use can be further aligned when the timescales for disclosure change to 20 working days. Note also:</a></p> <p>a. <a href="#">You will no longer be able to charge for Subject Access Requests</a></p> <p>b. <a href="#">You will be able to refuse requests which meet the threshold for ‘manifestly unfounded’ or ‘excessive’.</a></p> |  |  |
|--|---|--|--|

|  |  |  |  |
|--|--|--|--|
| <p>Subject Access Requests</p> <ul style="list-style-type: none"> <li>➤ 40 calendar days reduced to 20 working days</li> <li>➤ Removes the ability to charge for Subject Access Requests</li> <li>➤ Allows an additional 40 days for complex Subject Access Requests, but requestors must be advised in the acknowledgement of the request if claiming this additional time</li> <li>➤ Provides the opportunity to refuse manifestly unreasonable/repeated requests</li> </ul> |  |  |  |
|--|--|--|--|


## b) Security Incidents

|  |   |   |   |
|--|---|---|---|
| <ol style="list-style-type: none"> <li>1 No formal Security Incident process defined. On day 2 of the audit the Senior Information Risk Owner provided us with a security incident policy (dated January 2016), however no staff interviewed were aware of its existence. The policy is quite well detailed, but does not include a decision tree/criteria or process for identifying the need to notify the regulator</li> <li>2 Security incidents should be linked through to the risk register where appropriate to ensure alignment</li> <li>3 Security incidents reports should be regularly reported to Service Leadership Team to ensure visibility and risk management</li> <li>4 Security incidents must be regularly analysed to inform training needs and to mitigate risks arising.</li> <li>5 To comply with the General Data Protection Regulation a process must include the threshold and process for referral of serious incidents to the ICO</li> </ol> | <ol style="list-style-type: none"> <li>1 Introduce an information security incident policy, process and guidance               <ol style="list-style-type: none"> <li>1.1 Raise awareness and deliver training to ensure culture change is made</li> </ol> </li> <li>2 Assess and align security incidents to information risks held on software from JC Applications Development</li> <li>3 Service Leadership Team must have visibility of all SIs on a monthly basis, including trends analysis to ensure they are available to feed into strategy, policy, risk management and staff training</li> <li>4 Central logging tool to manage and analyse security incidents</li> <li>5 Vital for General Data Protection Regulation compliance where there is a requirement for serious Security Incidents to be notified to the ICO and data subjects within 72 hours.</li> </ol> | <br>Critical | <b>Agreed:</b> Mike Clayton   |
|  |   | <b>Link to Risk(s):</b><br>1,2  | <b>Action to be taken:</b> Existing Security Incident Policy to be reviewed and promulgated. Reporting to Service Leadership Team to be introduced. |
|  |   |   | <b>Additional Resources Required for implementation:</b> ICT Security Officer   |
|  |   |   | <b>Responsible Officer</b> Mike Clayton Finance Director & Treasurer<br><br><b>Target Date:</b> 31 December 2017                                    |

### c) Impact Assessments


|   |  |  |  |
|---|--|--|--|
| <ol style="list-style-type: none"> <li>Only 1 instance of evidence of PIA completion or review process, relating to a new system for L&amp;D – no evidence of corporate policy or process for completing PIAs</li> <li>Observed that the Safeguarding team, processing sensitive data are sited in an open office with no facility for confidential conversations/communications</li> <li><a href="#">PIA's are a legal requirement under General Data Protection Regulation. High risk projects are likely to need approval from the ICO before work can begin.</a></li> </ol> | <ol style="list-style-type: none"> <li> <ol style="list-style-type: none"> <li>Create policy and process for PIA and ensure awareness/training is delivered in this area. We are able to provide training in this area and templates to assist the development of procedures</li> <li>The people/policy element of the PIA need to be completed by a qualified/experienced DP Practitioner to ensure risks are identified and appropriately mitigated</li> </ol> </li> <li>Review of allocation of work spaces to ensure teams processing sensitive data have an appropriately confidential environment to operate in – consider the use of screens where open offices are the norm</li> <li> <ol style="list-style-type: none"> <li>All systems processing personal data will require a retrospective PIA to be completed for General Data Protection Regulation compliance as part of the Records of Processing Activity</li> <li>Consider publishing elements of PIAs to drive transparency for the public</li> </ol> </li> </ol> | <br>Major | <b>Agreed:</b> Mike Clayton  |
|   |  | <b>Link to Risk(s):</b><br>2   | <b>Action to be taken:</b><br>Development of staff to support them undertaking Privacy Impact Assessments. Policy element to be picked up by HR. Departmental managers to be supported by discussion with property services if they believe office environment inappropriate and alternative options identified. |
|   |  |  | <b>Additional Resources Required for implementation:</b> third party support for development   |
|   |  |  | <b>Responsible Officer:</b> Mike Clayton, Finance Director & Treasurer<br><br><b>Target Date:</b> 31 December 2017   |

### d) Privacy Notices


|   |   |  |                           |
|---|---|--|---------------------------|
| <ol style="list-style-type: none"> <li>No privacy notice policy, process or guidance was evidenced</li> <li><a href="#">Website privacy notice</a> is in place but limited information is provided</li> </ol> | <ol style="list-style-type: none"> <li>Policy and process must be set for managing privacy notices</li> <li>Ensure a full <a href="#">Privacy Notice</a> is held on the public facing website, including a</li> </ol> | <br>Major | <b>Agreed:</b> Roy Carter |
|---|---|--|---------------------------|

|   |   |  |   |
|---|---|--|---|
| <p>3 Consider accessibility for those without access to the internet, and those with additional needs</p> <p>4 No privacy notice in place for staff or contractors.</p> <p>5 Violent hazard warning markers are managed by Community Safety Team but there was no evidence of a documented policy or process</p> <p>6 <a href="#">General Data Protection Regulation sets a higher bar, and requires additional information to be provided to data subjects</a></p> <ul style="list-style-type: none"> <li>➤ <a href="#">Legal basis explained</a></li> <li>➤ <a href="#">Contact Details of the data Protection Officer</a></li> <li>➤ <a href="#">Advise if there is any automated decision making or profiling</a></li> <li>➤ <a href="#">Reference the right and the process for withdrawing consent</a></li> <li>➤ <a href="#">Confirm if processing is contractual or statutory</a></li> <li>➤ <a href="#">Explain the right to data portability where applicable</a></li> <li>➤ <a href="#">Detail the security arrangements for any overseas transfers</a></li> </ul> | <p>breakdown of each service stream explaining what data is collected, who it may be shared with, and for what purpose</p> <p>3. Process to provide hard copy where requested.</p> <p>3.1 Ensure you consider and account for accessibility needs – translations, easy read etc.</p> <p>4. Ensure consent forms have a ‘potted’ privacy notice and a link to the full online notice</p> <p>5. Ensure that staff are provided access to a privacy notice on how their data is processed</p> <p>6. Ensure that privacy notices are given when hazard warning markers are placed on individuals, and explain the appeals process. Such warning markers should be reviewed annually</p> <p>7.1. <a href="#">Consider the additional requirements for privacy notices for compliance with General Data Protection Regulation and build these in from the start of the project.</a></p> <p>7.2. <a href="#">Web-based privacy notice can be checked against data flows to ensure that all flows and processing have an appropriate privacy notice in place</a></p> <p>7.3. <a href="#">Ensure there is a process for providing privacy notices to those who did not provide you with their data</a></p> | <p><b>Link to Risk(s):</b><br/>2,4</p> | <p><b>Action to be taken:</b> A process is being investigated where a marker can be placed against a premises if a “violent marker” is shown against a premises through the safeguarding process. This will be included in our Hoarding policy and notification process.</p> <p>Service Solicitor to review privacy notices on website and intranet.</p> <p><b>Additional Resources Required for implementation:</b> None</p> <p><b>Responsible Officer</b> Roy Carter, Service Solicitor</p> <p><b>Target Date:</b> 31 December 2017</p> |
|---|---|--|---|

### e) Consent

|   |   |   |   |
|---|---|---|---|
| <p>1 Consent form in use in Safeguarding and Community Safety, but no privacy notice is attached or provided to individuals so the requirement for principle one of the DPA is not met (Processing must be <u>fair</u> and lawful).</p> <p>2 Outside of the Safeguarding Team there is a low level of understanding of when consent is required and the extent of the statutory duties of ECFRS</p> <p>3 <a href="#">Current consent process will not meet the requirements of the General Data Protection Regulation</a></p> | <p>1.1. Ensure there is a privacy policy available to staff (may be included in your data protection policy) to ensure methods for gaining consent are understood and appropriately actioned</p> <p>1.2. Review of all consent forms to ensure they capture all of the requirements</p> <p>1.3. Ensure Privacy notices form part of the consent process</p> <p>2. Train relevant staff so they have a full understanding of the legal requirements</p> <p>3.3. <a href="#">Ensure the higher bar set for consent under the General Data Protection Regulation is factored in</a></p> <p>3.4. <a href="#">Establish whether any online services for children are offered where General Data Protection Regulation consent is applicable</a></p> <p>3.5. <a href="#">General Data Protection Regulation Consent is a much higher bar – so there needs to be a full understanding of what statutory duties are undertaken by the Essex Fire Authority so that consent is not sought where it is not necessary, or where there is an imbalance of power</a></p> | <br>Moderate | <b>Agreed:</b> Roy Carter   |
|   |   | <b>Link to Risk(s):</b><br>2,4  | <b>Action to be taken:</b> Data Protection Policy to be amended to include a privacy policy. Consent rules to be defined. |
|   |   |   | <b>Additional Resources Required for implementation:</b> None   |
|   |   |   | <b>Responsible Officer:</b> Roy Carter, Service Solicitor<br><br><b>Target Date:</b> 31 December 2017                     |


### f) Photo & Video

|  |   |   |                           |
|--|---|---|---------------------------|
| <p>1. Although there were some strong processes explained by the Communications Team, and supported by policy, there is disparity in the</p> | <p>1.1. Ensure all staff are trained on how to process images</p> <p>1.2. Ensure your privacy notices cover this type of data in full</p> | <br>Moderate | <b>Agreed:</b> Roy Carter |
|--|---|---|---------------------------|




|  |  |                                |  |
|--|--|--------------------------------|--|
| process for gaining consent from staff versus the public | 1.3. Ensure your retention schedule is explicit regarding how long such data is retained<br>1.4. Ensure you have the capability to delete images from your systems<br>1.5. Ensure there is a consent process in place for processing images where required | <b>Link to Risk(s):</b><br>2,4 | <b>Action to be taken:</b> Specific development of information asset owners of photo and video to be undertaken. Approach to managing images to be determined and implemented consistently across all departments. |
|  |  |                                | <b>Additional Resources Required for implementation:</b> Not yet known.  |
|  |  |                                | <b>Responsible Officer</b> Roy Carter, Service Solicitor   |
|  |  |                                | <b>Target Date:</b> 31 December 2017   |

#### g) Surveillance imagery/ Drones/ Body Worn Cameras

|  |   |  |  |
|--|---|--|--|
| 1 We were advised that 2 registers of CCTV are held, one in property and one in Fleet<br>2 CCTV Policy in draft for use of visual recording aids, but will need supporting processes and awareness raising to become effective<br>3 No consistent retention of CCTV imagery – the Property team have a 30 day recording loop, whereas the retention period varied within the Fleet service<br>4 No evidence was provided of notification to the Surveillance Commissioner<br>5 Fleet signage is not compliant with the | 1. Compile and manage a full CCTV register<br>2.1. Ensure policy, process and procedures are documented on how to handle and secure such data<br>2.2. Ensure relevant staff are trained and aware of their responsibilities<br>3. Ensure consistent and secure retention of images across the Authority<br>4. Register with the <a href="#">Surveillance Commissioner</a> if any CCTV coverage of publicly accessible areas<br>5. Ensure full signage is sited with all | <br>Moderate | <b>Agreed:</b> Roy Carter  |
|  |   | <b>Link to Risk(s):</b><br>2,4   | <b>Action to be taken:</b> Specific development of information asset owners of photo and video to be undertaken. Approach to managing images to be determined and implemented consistently across all departments. |

|  |   |  |  |
|--|---|--|--|
| <p>requirements of the DPA, however Property signage fully in place</p> <p>6 We were advised that 2 drones are owned by Essex Fire Authority, but they are not sure where 1 is currently. Body Worn Cameras were used during an industrial dispute, but have not used since. Staff were unaware if any footage has been retained.</p> <p>7 No evidence of the capability to redact data (pixilating)</p> <p>8 No evidence of awareness of any covert surveillance, however historically/anecdotaly there was a 'dusty bin'; but there is no knowledge of where this equipment is now, if it still exists</p> | <p>recording equipment</p> <p>6.1. Ensure awareness that the CCTV policy covers the use of Drones and Body Worn Cameras, including retention and access to recordings</p> <p>6.2. Asset tag, and manage via a log, the drones and body worn cameras to maintain awareness of their location an security</p> <p>7. Buy in, or contract 3<sup>rd</sup> party, to carry out any necessary redaction of images</p> <p>8. Identify key roles in an authorisation process for covert surveillance</p> |  | <p><b>Additional Resources Required for implementation:</b> not Known</p> <p><b>Responsible Officer:</b> Roy Carter, Service Solicitor</p> <p><b>Target Date:</b> 31 December 2017</p> |
|--|---|--|--|

h) **Technical Security – PLEASE NOTE** – this was reviewed purely from an information management perspective rather than technical expertise

|   |   |   |                             |
|---|---|---|-----------------------------|
| <ol style="list-style-type: none"> <li>1. The organisation does not currently monitor or receive updates on known security threats from respected sources</li> <li>2. Proposed cloud strategy is being finalised. Strategy owner aware of the Cloud Security Principles but will need to ensure they are embedded in the process as compliance standards.</li> <li>3. The majority of 3<sup>rd</sup> party access provided is to external Information Technology suppliers to facilitate maintenance support activities for procured systems. There is inconsistent knowledge of an approval process for granting this access. The move to cloud will create much greater flexibility for allowing 3<sup>rd</sup> party access without the need to providing managed Information Technology accounts.</li> <li>4. There was uncertainty over whether the Authority is compliant with the PSN requirements. This is confirmed as necessary for the Authority to meet.</li> <li>5. There was no evidence of a security classification marking scheme in operation, and no firm</li> </ol> | <ol style="list-style-type: none"> <li>1. Register with Care, CertUK and/or CiSP to receive regular notifications of day 1 cyber threats</li> <li>2. Ensure awareness of the cloud security principles and the Cloud Security Alliance; and that these are captured in infrastructure design and procurements</li> <li>3.1. A third party access procedure needs to be embedded in policy so that every instance is documented, approved by an appropriate risk owner in the organisation, time limited and monitored. This will form part of the records of processing activity</li> <li>3.2. Support contracts need to be reviewed to ensure that suppliers who have access to data in order to support systems have effective controls in place to ensure the confidentiality of the data</li> <li>4. Progress with certification as this will strengthen the legitimacy of requiring</li> </ol> | <br>Moderate<br><br><b>Link to Risk(s):</b><br>2,5 | <b>Agreed:</b> Jan Swanwick |
|---|---|---|-----------------------------|

|  |   |  |   |
|--|---|--|---|
| <p>confirmation able to be provided that the data handled within the Authority is limited to the OFFICIAL category.</p> <p>6. There was no confidence that a device asset register was complete (estimated at 90% compliant) although efforts were in place to improve this. Asset tagging is not currently common practice; devices are currently being registered by supplier identifiers. The regulator would see a lack of control over device management as a significant vulnerability.</p> <p>7. System owners were not able to consistently confirm the location of hosting and support locations of externally hosted systems and Information Technology have not completed a contract review to establish this for certain.</p> <p>8. The movers and leavers process is not comprehensively documented and does not effectively cover those systems where access credentials are not checked against the Authority's active directory register. There is a risk that leavers may still have access to certain system</p> | <p>the same standard of suppliers. However if not progressed the Authority must align to Cyber Essentials as a minimum standard and this should be confirmed and regularly reviewed</p> <p>5. Check Public Service Network compliance and take appropriate action to comply if not already met</p> <p>6. Check understanding of classifications in use, i.e. Official, Secret etc. Associated handling practices should be implemented in policy and awareness raised through training</p> <p>7. Asset register for devices needs to be complete and maintained on CMDDB system– recommend a consistent asset tagging process is introduced with an authority specific convention</p> <p>8. Check all hosted systems holding personal data sited are within the European Economic Area (EEA),</p> |  | <p><b>Action to be taken:</b> Existing ICT security procedures to be reviewed for compliance with GDPR.</p> <p><b>Additional Resources Required for implementation:</b> not Known</p> |
|--|---|--|---|

|  |   |  |  |
|--|---|--|--|
| <p>data.</p> <p>9. The process of notifying Information Technology of leavers through the HR system does not cover contractors which presents a risk of third parties having access to Authority data after the entitlement having lapsed</p> <p>10. Information Technology staff are Information Technology Infrastructure Library (ITIL) qualified, however Information Technology Service Manager has identified a need to implement ITIL processes to improve consistency of and accountability for the activities of the Information Technology service.</p> <p>11. Managed devices are permitted general access to application stores therefore there is little control over the security of the platforms on which Authority data is stored.</p> <p>12. There is an unclear approach to use of unmanaged/ personal devices for working with Authority data. This presents challenges to maintaining confidentiality of Authority data and prevents the Authority from having control over</p> | <p>including 2<sup>nd</sup> &amp; 3<sup>rd</sup> line support services</p> <p>9. Ensure the leavers process is explicit about return of devices and closure of AD account, including any web based systems accessed by the leaver</p> <p>10. Investigate managing contractor accounts in line with accounts for directly employed staff. If an additional process is required, it should ensure that all Information Technology account holders have a current and valid entitlement to access Authority data.</p> <p>11. ITIL processes should be implemented and maintained, ensuring Information Technology staff have the relevant training to support this activity.</p> <p>12. Managed devices (e.g. laptops, smart phones, assistive technologies, tablets, removable media) should be blocked from open access to application stores. There should be a whitelist of applications approved by Information</p> |  | <p><b>Responsible Officer – Jan Swanwick</b> Head of ICT</p> |
|--|---|--|--|

|  |   |  |   |
|--|---|--|---|
| <p>and access to all of its data.</p> <p>13. Where lost or stolen devices are reported to Information Technology such instances are not investigated and recorded as security incidents as part of a corporate process</p> <p>14. Secure methods of transferring sensitive data such as Egress and SFTP are available, however there is questionable understanding of when they should be used, and how to use them.</p> | <p>Technology and Information Governance which staff can access. There should be a process to request an evaluation of applications which staff support with a valid business case. Controls should show who has access to what apps on which devices. The whitelist is regularly reviewed for security and a valid business need.</p> <p>13. Policy should establish a clear instruction to staff on whether working with Authority data on personal devices is permitted, and if it is then develop effective instructions on how this may be done whilst safeguarding the data</p> <p>14. Include lost and stolen devices within the security incident process</p> <p>14.1. Utilise Egress to increase security and reduce costs in business areas such as HR, Occupational Health &amp; Compliance when sending sensitive information or large files</p> <p>14.2. Ensure policy is clear on when there is a need to use Egress and SFTP and how to access the services.</p> |  | <p><b>Target Date:</b> 31 December 2017</p> |
|--|---|--|---|