



INTERNAL AUDIT FINAL REPORT

REVIEW OF INFORMATION GOVERNANCE AND GENERAL DATA PROTECTION REGULATIONS (GDPR) AUDIT FOR 2018-19

Issued to: Mark Bowen, Director of Corporate Services
Vinit Shukle, Head of ISD
Lucinda Bowen, Head of Information Management

Cc Head of Audit

Prepared by: Principal Auditor

Date of Issue: 11 February 2019

Report No: CORP/06/2018/AU

AUDIT REVIEW OF INFORMATION GOVERNANCE AND GENERAL DATA PROTECTION REGULATIONS (GDPR) 2018-19

INTRODUCTION

1. This report sets out the results of our audit of Information Governance and General Data Protection Regulations for 2018-19. The audit was carried out in quarter three as part of the programmed work specified in the 2018/19 Internal Audit Plan agreed by the Section 151 Officer and Audit Sub-Committee.
2. The controls we expect to see in place are designed to minimise the department's exposure to a range of risks. Weaknesses in controls that have been highlighted will increase the associated risks and should therefore be corrected to assist overall effective operations.

AUDIT SCOPE

3. The scope of the audit was outlined in the Terms of Reference issued on 30 August 2018. An external review of GDPR and Information Governance was carried out in 2017 by Contractor 'A'. Following the review, which made 51 recommendations, actions plans were put in place by management and monitored by using a percentage rating for the completion of each recommendation.
4. We have therefore examined the progress made for implementing these and verified the supporting evidence. Our testing shows that 16 out of the 51 recommendations made have been fully implemented with the remaining recommendations at varying stages of completion. This approach has helped us to form an overall audit opinion on the controls put in place at a corporate level over GDPR and Information Governance.
5. We have also placed reliance on other relevant work carried out by management, notably the compliance with the IG toolkit: an on-line system which allows organisations to assess themselves or be assessed against Information Governance policies and standards. Following evidence submitted, the Council has recently been awarded an overall rating of 'Satisfactory'.
6. A separate external review of information governance has been carried out by the Council's insurer as part of their engagement with the Council to provide advice on risk management, insurance and related services. We have liaised with them during our audit to complement and avoid duplication of the work undertaken.

AUDIT REVIEW OF INFORMATION GOVERNANCE AND GENERAL DATA PROTECTION REGULATIONS (GDPR) 2018-19

7. Whilst this audit has focussed on the GDPR and information governance controls put in place corporately, an audit review of the controls locally within Directorates will be included in the 2019/20 annual audit plan.

AUDIT OPINION

8. For this audit we have given a split audit opinion as follows:

Governance and policies and procedures – **Substantial**

Training and awareness and arrangements for the collecting, processing, storing, sharing of data and disposal of IT equipment containing personal data - **Limited**

Definitions of the audit opinions can be found in Appendix C.

MANAGEMENT SUMMARY

9. Controls and areas of good practice are in place over the governance arrangements and policies and procedures. Whilst controls have been put in place over awareness and training and for the collecting, processing, storing and sharing of data, there are issues within those areas which need to be addressed. They are included in the summaries below.

Governance

An Information Governance Board is in place. Terms of reference for the Board have been set out and agreed and the Board meets regularly. The Council has appointed a Data Protection Officer, Senior Information Risk Owner and a Principal Information Assurance Officer (now promoted to Head of Information Management). There is a nominated Caldicott Guardian for Health and Social Care.

AUDIT REVIEW OF INFORMATION GOVERNANCE AND GENERAL DATA PROTECTION REGULATIONS (GDPR) 2018-19

Policies and procedures

Policies and procedures have been documented, reviewed and approved. There are two policies currently in draft form and awaiting approval. The policies are published on the intranet and therefore available to all staff. We have recommended that they are set out in a hierarchical structure on the intranet site to show their relative importance and how they link to each other.

Training and awareness

A newsletter on IT matters is sent to all staff periodically and specific guidance on Information Governance was issued to all staff in May 2018. On-line training for GDPR and Information Governance has been introduced with two modules launched so far. These are mandatory for all staff to complete. Guidance on GDPR and Information Governance is also given to staff at their induction course. IT currently include a link in the introductory email to all new employees when they are set up as a new user on the Council's IT network.

There are areas of training and awareness where improvements could be made. These include providing information on GDPR and Information Governance in the joining pack sent to new members of staff and reminding managers to ensure that new staff complete the on-line information governance course modules within their first week of employment.

There are however no follow up arrangements in place to identify and notify Directors of their staff who have not completed the on-line training modules. The 'Information Governance – guidance for staff' dated 24/05/2018 and issued to all employees showed the timetable for the roll out of the six on-line training modules. The first two modules were issued on time but we note that roll out of the next two modules is behind schedule.

There is no formal instruction on the covering sheet on files reminding social care staff not to remove files off site and to adhere to the relevant security arrangements eg keeping them locked away overnight/when not in use.

AUDIT REVIEW OF INFORMATION GOVERNANCE AND GENERAL DATA PROTECTION REGULATIONS (GDPR) 2018-19

Arrangements for the collecting, processing, storing and sharing of data

Arrangements for the collecting, processing, storing and sharing of data require improvement. These activities have been impacted partly by the outcome of other current review work such as the external review of the information strategy by Contractor 'B' and awaiting the outcome of policy decisions within the Council. Our testing has identified the following areas where progress is being made but not yet complete:

- The compilation of a register of data sources,
- Documenting process maps of key data flows for all business areas,
- Creating and maintaining the information held on the Information Asset Register, Register of Processing Activities and Privacy Impact Assessments,
- Engaging with vendors of any database systems that do not support the data retention policy to find out what steps they are taking to modify their solutions to help support data controllers' compliance, including privacy information of each data subject and
- Out of 380 processor contract agreements required to be signed by contractors, there are only 19 uploaded to the relevant depository. A further 4 contracts have now ended.

For each of the areas highlighted above, together with the roll-out of the modules of on-line training, delays to completing these tasks can be attributed to resourcing challenges within the IT team. This presents a risk to completing the implementation of all recommendations made in the external review of GDPR and Information Governance carried out in 2017. There is also a risk that, in any subsequent investigation, the Information Commissioner's Office may conclude that the Council is unable to demonstrate full compliance with the statutory responsibilities of GDPR and Information Governance. We have recommended that management review the resources available and what remedial action can be put in place to address these risks. In conjunction with this, management should re-introduce a regular and formal review of the implementation of the recommendations outstanding from the external review referred to in paragraph 3 of this report.

AUDIT REVIEW OF INFORMATION GOVERNANCE AND GENERAL DATA PROTECTION REGULATIONS (GDPR) 2018-19

Disposal of IT equipment containing personal data

Whilst there is a documented process and arrangements in place for the disposal of IT equipment, there are some areas which require improvement. In particular, controls should be strengthened over the storage of equipment earmarked for disposal, reconciliation of disposal records and accompanying evidence to confirm that items of IT equipment containing personal data have been collected by the contractor and disposed of correctly.

SIGNIFICANT FINDINGS (PRIORITY 1)

10. There are none.

DETAILED FINDINGS / MANAGEMENT ACTION PLAN

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

ACKNOWLEDGEMENT

12. We would like to thank all staff contacted during this review for their help and co-operation.

APPENDIX A

AUDIT REVIEW OF INFORMATION GOVERNANCE AND GENERAL DATA PROTECTION REGULATIONS (GDPR) 2018-19

DETAILED FINDINGS

No.	Findings	Risk	Recommendation
1	<p><u>Policies to be finalised</u></p> <p>An Individual Rights Policy and an Internal Review Policy have been drafted but need to be finalised and published on the Council's website.</p>	Risk that the public are not aware of the Council's policy and what their entitlements are.	The Individual Rights Policy and the Internal Review Policy should be finalised and published on the Council's website. [Priority 2]
2	<p><u>Hierarchical order of policies</u></p> <p>The Information Management site on onebromley shows the Council's GDPR and information governance policies which should be adhered to. There are 18 policies named and listed, but in no particular order.</p>	Staff may not be aware of the relative importance of the policies or the significant aspects of each policy, resulting in the risk of a data breach.	GDPR and information governance policies should be set out in a hierarchical order showing their relative importance and how they relate to each other. [Priority 3]

Project Code: CORP/06/2018/AU

Page 7 of 20

Priority 1

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

Priority 2

Required to address issues which do not represent good practice

Priority 3

Identification of suggested areas for improvement

APPENDIX A

AUDIT REVIEW OF INFORMATION GOVERNANCE AND GENERAL DATA PROTECTION REGULATIONS (GDPR) 2018-19

DETAILED FINDINGS

No.	Findings	Risk	Recommendation
3	<p><u>Training and awareness for new staff</u></p> <p>No information about GDPR or Information Governance is included in the joining pack which is sent to new employees by HR.</p>	<p>New employees are not made aware of the importance that the Council places on compliance with GDPR and information governance.</p>	<p>HR should include a copy of the 'Information Governance - Guidance for staff in the joining pack which is sent to new employees.</p> <p>[Priority 2]</p>
4	<p><u>Training and awareness for new staff</u></p> <p>When they are set up as a new user on the IT network new users are sent an email by IT about the importance of completing the information governance on-line training. This email is not copied to the individual's manager as IT are not aware who the manager will be.</p>	<p>New employees do not undertake the information governance on-line training, resulting in a lack of knowledge and awareness and, as a consequence, risk of data breaches.</p>	<p>Managers should remind new employees of the importance of completing the information governance on-line training within the first week of starting their employment.</p> <p>[Priority 2]</p>

Project Code: CORP/06/2018/AU

Page 8 of 20

Priority 1

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

Priority 2

Required to address issues which do not represent good practice

Priority 3

Identification of suggested areas for improvement

APPENDIX A

AUDIT REVIEW OF INFORMATION GOVERNANCE AND GENERAL DATA PROTECTION REGULATIONS (GDPR) 2018-19

DETAILED FINDINGS

No.	Findings	Risk	Recommendation
5	<p><u>Follow up arrangements for on-line training</u></p> <p>Two on-line training courses and accompanying tests have been set up for GDPR and Information Governance. All staff are required to complete them. There has been a 100% completion rate of the first module. The second module, which should have been completed by 30 September 2018, has a 60% completion rate. No follow up arrangements are in place however to identify and notify relevant Directors of those staff who have not completed it.</p>	<p>Staff are not aware of what action to take in certain situations, resulting in a lack of knowledge and awareness and risk of consequent GDPR breaches.</p>	<p>A follow up process is put in place to identify and notify relevant Directors of employees who have not yet completed the second on-line GDPR training module.</p> <p>[Priority 2]</p>
6	<p><u>Training and awareness for children's social care staff</u></p> <p>From discussion with the Senior Support Services Assistant and Safeguarding Support Assistant, there is no formal instruction on the covering file sheet reminding children's social care staff not to remove files off site and to adhere to the relevant security arrangements eg keeping them locked away overnight/when not in use.</p>	<p>Risk of loss of original source of personal and sensitive data if a file is mislaid, leading to a data breach with a significant fine imposed by the ICO and damage to the Council's reputation.</p>	<p>ECHS support services team should revise the wording on the covering file sheet of a client to state clearly that the file must not be taken off site and must be kept secure when not in use.</p> <p>[Priority 2]</p>

Project Code: CORP/06/2018/AU

Page 9 of 20

Priority 1

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

Priority 2

Required to address issues which do not represent good practice

Priority 3

Identification of suggested areas for improvement

APPENDIX A

AUDIT REVIEW OF INFORMATION GOVERNANCE AND GENERAL DATA PROTECTION REGULATIONS (GDPR) 2018-19

DETAILED FINDINGS

No.	Findings	Risk	Recommendation
7	<p><u>Arrangements for the collecting, processing, storing and sharing of data</u></p> <p>For each of the areas highlighted below, together with the roll-out of the remaining modules of on-line training, delays to completing these tasks can be attributed to resourcing challenges within the IT team:</p> <ul style="list-style-type: none">• The compilation of a register of data sources,• Documenting process maps of key data flows for all business areas,• Creating and maintaining the information held on the Information Asset Register, Register of Processing Activities and Privacy impact Assessments,• Engaging with vendors of any database systems that do not support the data retention policy to find out what steps they are taking to modify their solutions to	<p>Risk of not completing timely the implementation of all recommendations made in the external review of GDPR and Information Governance carried out in 2017.</p> <p>Risk that, in any subsequent investigation, the Information Commissioner's Office may conclude that the Council is unable to demonstrate full compliance with the statutory responsibilities of GDPR and Information Governance.</p>	<p>Management should review what resources are available and how they can be used to progress the completion of the outstanding tasks arising from the 2017 external review.</p> <p>[Priority 2]</p>

Project Code: CORP/06/2018/AU

Page 10 of 20

Priority 1

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

Priority 2

Required to address issues which do not represent good practice

Priority 3

Identification of suggested areas for improvement

APPENDIX A

AUDIT REVIEW OF INFORMATION GOVERNANCE AND GENERAL DATA PROTECTION REGULATIONS (GDPR) 2018-19

DETAILED FINDINGS

No.	Findings	Risk	Recommendation
	<p>help support data controllers' compliance, including privacy information of each data subject and</p> <ul style="list-style-type: none">Out of 380 processor contract agreements required to be signed by contractors, there are only 19 uploaded to the relevant depository. A further 4 contracts have now ended.		
8	<p><u>Implementation of recommendations arising from external review</u></p> <p>Action is being taken by IT to implement the recommendations arising from the external review carried out in 2017. A percentage completion rating has been introduced for each recommendation. Progress has not however been formally reviewed recently.</p>	<p>Risk that progress on implementing the recommendations arising from the external review is not maintained and the Council is unable to demonstrate full compliance with the statutory responsibilities of GDPR and Information Governance.</p>	<p>Management should re-introduce a regular and formal review of the implementation of the recommendations outstanding from last year's external review.</p> <p>[Priority 2]</p>

Project Code: CORP/06/2018/AU

Page 11 of 20

Priority 1

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

Priority 2

Required to address issues which do not represent good practice

Priority 3

Identification of suggested areas for improvement

APPENDIX A

AUDIT REVIEW OF INFORMATION GOVERNANCE AND GENERAL DATA PROTECTION REGULATIONS (GDPR) 2018-19

DETAILED FINDINGS

No.	Findings	Risk	Recommendation
9	<p><u>Disposal of IT equipment containing personal data</u></p> <p>Our testing identified that there is no independent reconciliation of the items recorded and stored for disposal by the Council's IT contractor and collected by their disposal contractor, or the report listing the items disposed of and the certificates to confirm that the hard drives of pcs, laptops and tablets had been erased or destroyed. We carried out our own reconciliation of the most recent disposal of items and confirmed that appropriate certificates had been received for those items.</p> <p>At present, items awaiting collection are stored in rooms in the North Lodge. Whilst the majority of the IT equipment for disposal is encrypted, there are 'old' laptops and pcs stored which have not been encrypted. These items represent a greater risk of loss of personal data if the item is not properly secured. Our enquiries revealed that access to that building is not restricted to the Council's contractor. We are aware that the building security staff employed by the Council's facilities</p>	<p>Risk that IT equipment containing personal data is not disposed of correctly, leading to a data breach with a significant fine imposed by the ICO and damage to the Council's reputation.</p>	<p>Management review the current arrangements in place for the disposal of IT equipment containing personal data, to ensure that :</p> <p>(i) items earmarked for disposal are kept secure with access restricted appropriately,</p> <p>(ii) when collecting the items for disposal the contractor signs to confirm which items are being taken away and</p> <p>(iii) a reconciliation is carried out of the data disposal certificates subsequently</p>

Project Code: CORP/06/2018/AU

Page 12 of 20

Priority 1

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

Priority 2

Required to address issues which do not represent good practice

Priority 3

Identification of suggested areas for improvement

APPENDIX A

AUDIT REVIEW OF INFORMATION GOVERNANCE AND GENERAL DATA PROTECTION REGULATIONS (GDPR) 2018-19

DETAILED FINDINGS

No.	Findings	Risk	Recommendation
	<p>management contractor also have access. We have been unable to verify if any other staff can access the property.</p> <p>The asset register is maintained by the Council's IT contractor. There were 13 pcs, laptops and tablets which had been disposed of but for which there was no record on the asset register. The Head of ISD informed us that the IT transformation project due to take place will identify all IT equipment which has not previously been recorded on the Council's asset register.</p>		<p>received from the contractor to the items taken away. Any discrepancies identified are investigated by the IT team.</p> <p>[Priority 2]</p>

Project Code: CORP/06/2018/AU

Page 13 of 20

Priority 1

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

Priority 2

Required to address issues which do not represent good practice

Priority 3

Identification of suggested areas for improvement

APPENDIX B

AUDIT REVIEW OF INFORMATION GOVERNANCE AND GENERAL DATA PROTECTION REGULATIONS (GDPR) 2018-19

MANAGEMENT ACTION PLAN

Finding No.	Recommendation	Priority *Raised in Previous Audit	Management Comment	Responsibility	Agreed Timescale
1	The Individual Rights Policy and the Internal Review Policy should be finalised and published on the Council's website.	2	The policies will be finalised at the next meeting of the Information Governance Sub-Group. .	Head of Information Management	31 March 2019
2	GDPR and information governance policies should be set out in a hierarchical order showing their relative importance and how they relate to each other.	3	These will be re-structured on the intranet page and arrangements are being made to do this.	Head of Information Management	31 March 2019
3	HR should include a copy of the 'Information Governance - Guidance for staff' in the joining pack which is sent to new employees.	2	This has been actioned and a copy of the Newsletter detailing Information Governance guidance is being sent to all new Staff with their contract of employment.	Head of HR Strategy and Education	Implemented

Project Code: CORP/06/2018/AU

Page 14 of 20

Priority 1

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

Priority 2

Required to address issues which do not represent good practice

Priority 3

Identification of suggested areas for improvement

APPENDIX B

AUDIT REVIEW OF INFORMATION GOVERNANCE AND GENERAL DATA PROTECTION REGULATIONS (GDPR) 2018-19

MANAGEMENT ACTION PLAN

Finding No.	Recommendation	Priority *Raised in Previous Audit	Management Comment	Responsibility	Agreed Timescale
4	Managers should remind new employees of the importance of completing the information governance on-line training within the first week of starting their employment.	2	This is included on the Employee Induction Checklist, located on the intranet, which managers are required to complete for new starters.	Head of HR Strategy and Education	Implemented
5	A follow up process is put in place to identify and notify relevant Directors of employees who have not yet completed the second on-line GDPR training module.	2	A follow up process is being put in place. In the meantime, a reminder will be issued at the next meeting of the Information Governance Sub-Group. Results will be issued to Directors.	Head of Information Management	28 February 2019
6	ECHS support services team should revise the wording on the covering file sheet of a client to state clearly that the file must not	2	We have now revised the front sheet adding the following instruction:	Business Support Manager, Quality and Improvement, ECHS	Implemented

Project Code: CORP/06/2018/AU

Page 15 of 20

Priority 1

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

Priority 2

Required to address issues which do not represent good practice

Priority 3

Identification of suggested areas for improvement

APPENDIX B

AUDIT REVIEW OF INFORMATION GOVERNANCE AND GENERAL DATA PROTECTION REGULATIONS (GDPR) 2018-19

MANAGEMENT ACTION PLAN

Finding No.	Recommendation	Priority *Raised in Previous Audit	Management Comment	Responsibility	Agreed Timescale
	be taken off site and must be kept secure when not in use.		This File is Strictly Confidential and must not be removed from the Civic Centre When the file is not being viewed it must be locked away securely.		
7	Management should review what resources are available and how they can be used to progress the completion of the outstanding tasks arising from the 2017 external review.	2	We are in the process of recruiting an additional member of staff. This will help us to complete the outstanding tasks.	Head of Information Management	31 July 2019
8	Management should re-introduce a regular and formal review of the implementation of the recommendations outstanding	2	The Information Governance Sub-Group is now meeting regularly. Weekly meetings are taking place within IT to discuss and review the	Head of Information Management	Implemented

Project Code: CORP/06/2018/AU

Page 16 of 20

Priority 1

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

Priority 2

Required to address issues which do not represent good practice

Priority 3

Identification of suggested areas for improvement

AUDIT REVIEW OF INFORMATION GOVERNANCE AND GENERAL DATA PROTECTION REGULATIONS (GDPR) 2018-19**MANAGEMENT ACTION PLAN**

Finding No.	Recommendation	Priority *Raised in Previous Audit	Management Comment	Responsibility	Agreed Timescale
	from last year's external review.		information management workstreams. We are recruiting an additional member of staff and, when that person has been recruited, it will provide more resource to help us address this.		
9	Management review the current arrangements in place for the disposal of IT equipment containing personal data, to ensure that : (i) items earmarked for disposal are kept secure with access restricted appropriately,	2	The Information Management page on onebromley has now been updated instructing staff how to dispose of items. (i) Items earmarked for disposal will be stored at a new secure location on site. This is currently being arranged and will be restricted to relevant IT and the	Head of ISD and Head of Information Management	28 February 2019

Project Code: CORP/06/2018/AU

Page 17 of 20

Priority 1

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

Priority 2

Required to address issues which do not represent good practice

Priority 3

Identification of suggested areas for improvement

AUDIT REVIEW OF INFORMATION GOVERNANCE AND GENERAL DATA PROTECTION REGULATIONS (GDPR) 2018-19**MANAGEMENT ACTION PLAN**

Finding No.	Recommendation	Priority *Raised in Previous Audit	Management Comment	Responsibility	Agreed Timescale
	(ii) when collecting the items for disposal the contractor signs to confirm which items are being taken away and		<p>staff of the Council's IT contractor. The majority of the items stored are encrypted. We will put arrangements in place to ensure that data does not remain on any unencrypted items stored for disposal.</p> <p>(ii) The contractor now signs for the receipt of items when collecting them.</p> <p>(iii) Arrangements have now been put in place for a reconciliation to be carried out once the information including disposal certificates has</p>	Head of ISD and Head of Information Management Head of ISD and Head of Information Management	Implemented Implemented

Project Code: CORP/06/2018/AU

Page 18 of 20

Priority 1

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

Priority 2

Required to address issues which do not represent good practice

Priority 3

Identification of suggested areas for improvement

APPENDIX B**AUDIT REVIEW OF INFORMATION GOVERNANCE AND GENERAL DATA PROTECTION REGULATIONS (GDPR) 2018-19****MANAGEMENT ACTION PLAN**

Finding No.	Recommendation	Priority *Raised in Previous Audit	Management Comment	Responsibility	Agreed Timescale
	(iii) a reconciliation is carried out of the data disposal certificates subsequently received from the contractor to the items taken away. Any discrepancies identified are investigated by the IT team.		been received from the contractor.		

Project Code: CORP/06/2018/AU

Page 19 of 20

Priority 1

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

Priority 2

Required to address issues which do not represent good practice

Priority 3

Identification of suggested areas for improvement

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

Assurance Level	Definition
Full Assurance	There is a sound system of control designed to achieve all the objectives tested.
Substantial Assurance	While there is a basically sound systems and procedures in place, there are weaknesses, which put some of these objectives at risk. It is possible to give substantial assurance even in circumstances where there may be a priority one recommendation that is not considered to be a fundamental control system weakness. Fundamental control systems are considered to be crucial to the overall integrity of the system under review. Examples would include no regular bank reconciliation, non-compliance with legislation, substantial lack of documentation to support expenditure, inaccurate and untimely reporting to management, material income losses and material inaccurate data collection or recording.
Limited Assurance	Weaknesses in the system of controls and procedures are such as to put the objectives at risk. This opinion is given in circumstances where there are priority one recommendations considered to be fundamental control system weaknesses and/or several priority two recommendations relating to control and procedural weaknesses.
No Assurance	Control is generally weak leaving the systems and procedures open to significant error or abuse. There will be a number of fundamental control weaknesses highlighted.