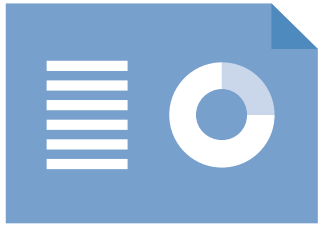
London Borough of Waltham Forest Council

Data protection audit report

July 2021

Information Commissioner's Office

Executive summary



Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA18) and other data protection legislation. Section 146 of the DPA18 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA18 allows the ICO to carry out consensual audits. The ICO sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach.

London Borough of Waltham Forest Council (LBWF) agreed to a consensual audit by the ICO of its processing of personal data. An introductory telephone meeting was held on 17 March 2021 with representatives of LBWF to discuss the scope of the audit.

The purpose of the audit is to provide the Information Commissioner and LBWF with an independent assurance of the extent to which LBWF, within the scope of this agreed audit, is complying with data protection legislation.

The scope areas covered by this audit are determined following a risk based analysis of LBWF's processing of personal data. The scope may take into account any data protection issues or risks which are specific to LBWF, identified from ICO intelligence or LBWF's own concerns, and/or any data protection issues or risks which affect their specific sector or organisations more widely. The ICO has further tailored the controls covered in each scope area to take into account the organisational structure of LBWF, the nature and extent of LBWF's processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to LBWF.

It was agreed that the audit would focus on the following areas:

Scope area	Description
Governance & Accountability	The extent to which information governance accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor data protection compliance to both the UK GDPR and national data protection legislation are in place and in operation throughout the organisation.
Freedom of Information (FOI)	The extent to which FOI accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor compliance are in place and in operation throughout the organisation.

Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are normally a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

However, due to the Covid -19 pandemic this methodology was no longer appropriate. Therefore, LBWF agreed to continue with the audit on a remote basis. A desk based review of selected policies and procedures and remote telephone interviews were conducted from 10 – 20 May 2021. The ICO would like to thank LBWF for its flexibility and commitment to the audit during difficult and challenging circumstances.

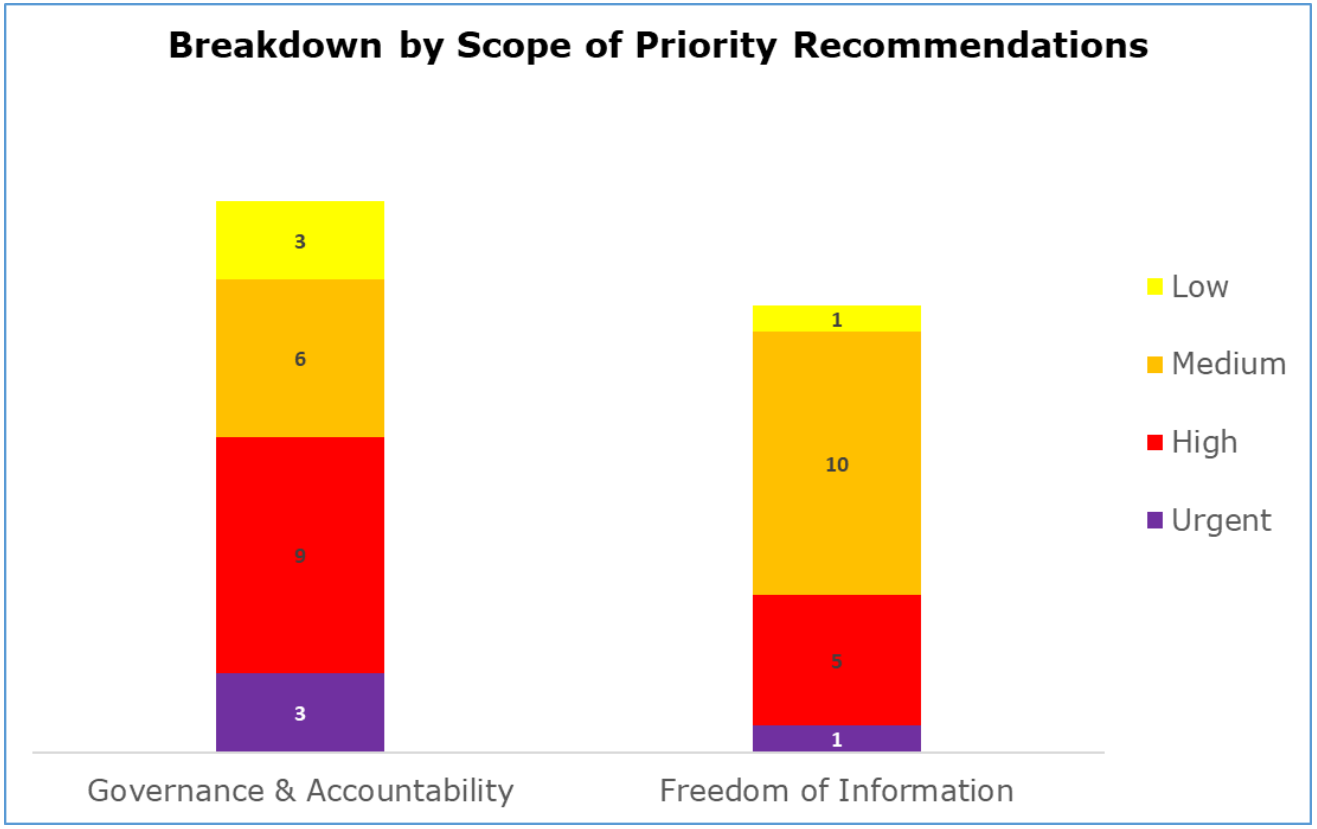
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist LBWF in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. LBWF's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Audit Summary

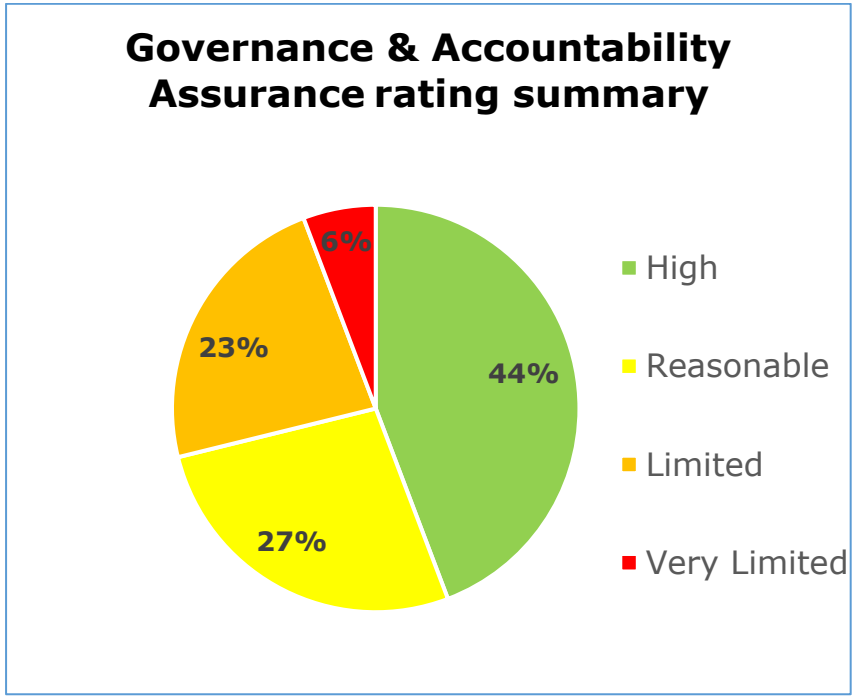
Audit Scope area	Assurance Rating	Overall Opinion
Governance & Accountability	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Freedom of Information	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with freedom of information legislation.

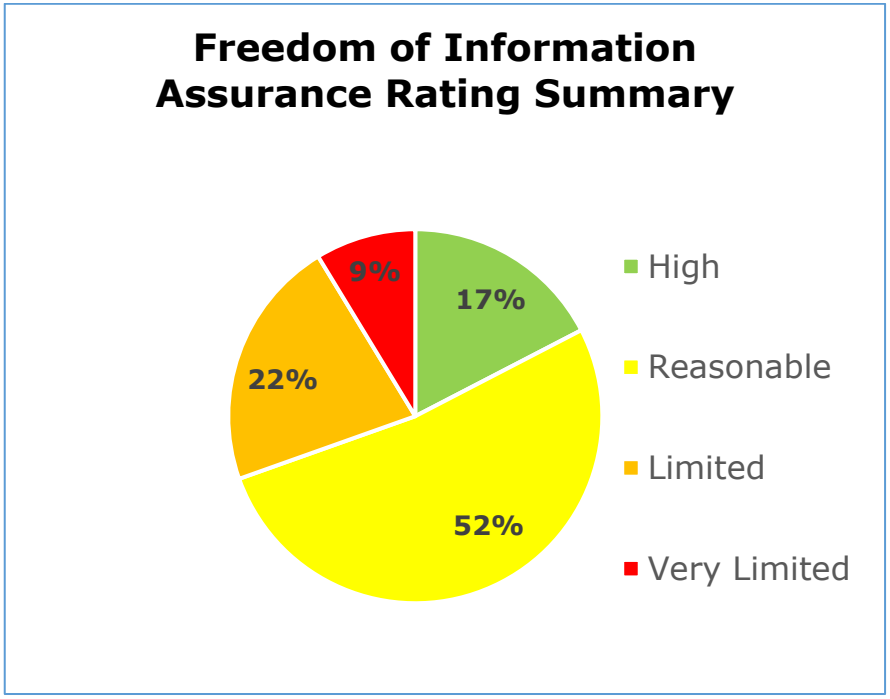
*The assurance ratings above are reflective of the remote audit methodology deployed at this time and the rating may not necessarily represent a comprehensive assessment of compliance.

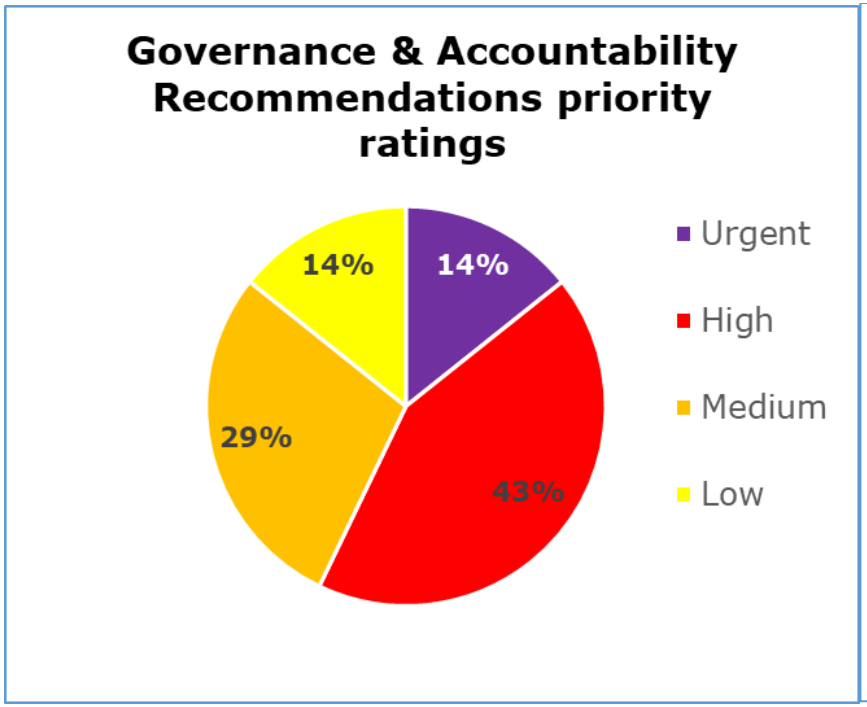
Priority Recommendations

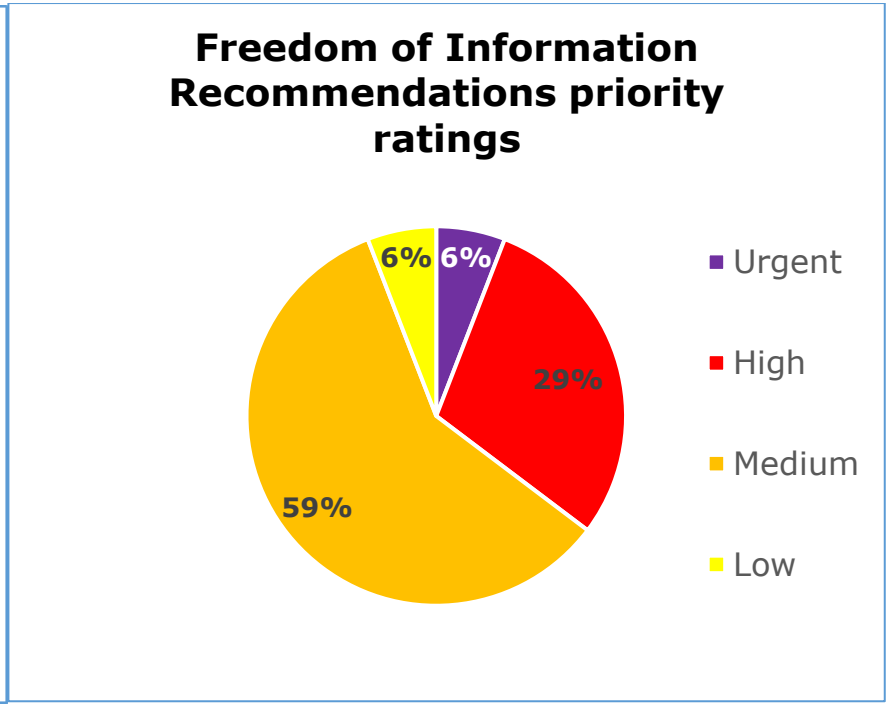


Graphs and Charts






Governance & Accountability Recommendations priority ratings
14%
14%
29%
43%
Urgent
High
Medium
Low


Freedom of Information Recommendations priority ratings
6%
6%
29%
59%
Urgent
High
Medium
Low

Areas for Improvement

- LBWF should consider reassigning its DPO position or putting an alternative reporting structure in place for LBWF's deputy DPO to take the lead on matters which could be perceived as a conflict of interest for its DPO.

- LBWF does not currently report KPIs on its compliance with subject access requests or records management obligations. By not monitoring this data LBWF lacks oversight and assurance that it is in compliance with its statutory obligations. LBWF should begin capturing and monitoring this data on a routine basis.

- LBWF does not currently have sufficient oversight on all the contracts it has in place with data processors. LBWF should create a central log of the contracts it has in place to ensure that all contracts in place are accounted for and monitored as needed.

- LBWF does not have any standard due diligence checks built into its procurement process prior to engaging in the services of a processor. LBWF should implement a set of standard checks as part of its procurement process to ensure that its processors are all meeting UK GDPR requirements and protecting data subjects' rights.

- The Information Governance Board should monitor the completion rates of all staff FOI training and specialist training (at both induction and refresher stages). This will help LBWF provide assurance that all staff have received the correct training.

- A cold case FOI quality assurance process should be established. Periodic reviews of cold case FOI requests should be checked and results recorded and feedback provided to IGB and the individuals involved in the original request.

- LBWF should ensure that all staff receive at least a basic level of training on FOI and EIR requests. Training should cover what a request is, how a request may be received (i.e., can be via social media, EIR requests can be verbal), the fact the request doesn't need to reference the legislation and what to do if they receive a request. This training should be mandatory for all staff and be refreshed on a regular basis.

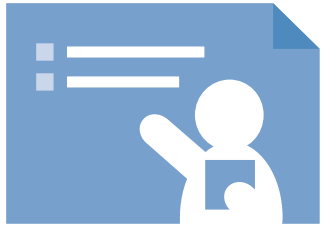
Best Practice

- LBWF have incorporated videos into the privacy notice section of its website to provide privacy information in a different format that may be more accessible to individuals.

- LBWF effectively monitor adherence to statutory timescales for FOI and EIR requests via Executive Assistants and daily and weekly reporting mechanisms.

- All staff interviewed showed a good understanding and knowledge of the LBWF FOI Procedure.

Audit findings



The tables below identifies areas for improvement that were identified in the course of our audit; they include recommendations in relation to how those improvements might be achieved.

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
There is a Data Protection Officer in place with designated responsibility for data protection compliance.	See A.01	See A.01	

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
The DPO role has operational independence and appropriate reporting mechanisms are in place to senior management	A.01. LBWF's DPO is the Council's Director of Governance and Law while its Deputy DPO and SIRO holds the role of Data Protection Manager and oversees the team that handles day to day compliance matters. By holding a Director level role LBWF is unable to provide assurance that its DPO has operational independence and that there is no conflict of interest in the other duties the DPO holds as part of their role. This could result in non compliance of Article 38.6 of the UK GDPR.	A.01. LBWF should consider reassigning its DPO position to its Data Protection Manager to ensure that it can demonstrate its DPO is not in a role which could result in a conflict of interest with their other duties. Alternatively, LBWF could consider creating documentation to account for the possibility that a conflict of interest could arise within the currently assigned DPO's role, and the backup reporting measures in place to mitigate this risk, e.g. allowing the deputy DPO to take the lead on matters which could be perceived as a conflict of interest for the DPO. This will ensure that LBWF can demonstrate compliance with Article 38.6 of the UK GDPR.	High
There is an Information Management Steering Group, Committee, or equivalent, in place, which is responsible for providing the general oversight for information governance and data protection compliance activity within the organisation.	A.02. Evidence provided to ICO auditors of LBWF's Information Governance Board (IGB) agendas and meeting minutes showed that compliance to statutory timescales for individual rights requests including SARs were not routinely monitored or discussed in meetings. This means that LBWF cannot demonstrate that it is monitoring its compliance with its statutory obligations as required by Article 5.2 of the UK GDPR.	A.02. LBWF should add an agenda item to its IGB meetings to ensure that compliance with individual rights requests including SARs are routinely monitored. This will ensure that LBWF can demonstrate compliance with Article 5.2 of the UK GDPR.	High

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
There are local level operational meetings where data protection, records management and information security matters are discussed.	A.03. A number of examples were reported to ICO auditors of local level operational meetings taking place where data protection matters are discussed. However, LBWF did not provide any evidence of data protection being included on any local level meeting agendas or minutes. This means LBWF is unable to evidence that communication and direction from senior management is embedded at a local level.	A.03. Data protection matters should be included on agendas of local level meetings on a routine basis. This will ensure that LBWF can demonstrate that communication and direction from senior management is embedded on a local level.	Low
Policies and procedures are readily available to staff and are communicated through various channels to maintain staff awareness	A.04. LBWF currently advises staff that its policies and procedures relating to data protection should be read after the completion of its mandatory data protection e-learning module. However, there is no requirement for staff to confirm that they have read and understood these policies and procedures. This means LBWF is unable to demonstrate that staff are aware of and understand its data protection policies and procedures.	A.04. LBWF should require staff to confirm that they have read and understood its data protection policies and procedures once they have completed its data protection e-learning module. This will ensure that LBWF can demonstrate that staff are aware of and understand its data protection policies and procedures and reduce the risk of breaches caused by staff being unaware of their responsibilities.	Medium
There is an overarching IG training programme in place for all staff.	A.05. It was reported that LBWF had not conducted a documented training needs analysis exercise for all staff including staff in IG positions. This means that LBWF cannot demonstrate that it has sufficiently considered and documented what data protection training staff should receive in addition to the mandatory e-learning modules for their role.	A.05. Conduct a training needs analysis exercise for all staff including those in IG roles and document the outcome. This will ensure that LBWF can demonstrate that it has considered what data protection training should be provided to staff based on their roles to ensure they can properly carry out their responsibilities in compliance with data protection law.	Medium

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
There is provision of more specific DP training for specialised roles (such as the DPO, SIRO, IAOs) or particular functions e.g. records management teams, SAR teams, information security teams etc.	See A.05.	See A.05.	
There is a programme of risk- based internal audit in place covering information governance / data protection.	A.06. Data protection matters are included within the scope of all audits included within LBWF's internal audit plan. However, LBWF does not routinely conduct internal audits based solely around data protection compliance matters. This means LBWF may be lacking oversight and assurance that it is maintaining compliance with all its data protection obligations.	A.06. LBWF should conduct internal audits covering a range of data protection compliance areas on a routine basis. This will ensure that LBWF has continuous oversight and assurance that it is maintaining compliance with all of its data protection obligations.	Medium
The organisation actively monitors or audits its own compliance with the requirements set out in its data protection policies and procedures.	A.07. LBWF's data protection policies and procedures do not specify what the monitoring process is to ensure that staff are in compliance with the policies. Without ongoing compliance monitoring LBWF lacks assurance that the controls it has in place are being implemented to prevent non-compliance.	A.07. Establish within data protection policies and procedures how compliance will be monitored. By continually monitoring staff compliance to policies and procedures LBWF will have ongoing assurance that the controls it has in place are being correctly implemented and preventing non-compliance of data protection legislation.	Low

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
There are data protection Key Performance Indicators (KPI) in place	A.08.A. LBWF does not have KPIs in place to cover SAR performance. Without having KPIs on SAR performance LBWF lacks oversight on its compliance with statutory timescales and cannot demonstrate accountability as required under Article 5.2 of the UK GDPR. B. LBWF does not have KPIs in place to cover records management. Without having KPIs on records management LBWF lacks oversight on its compliance with statutory obligations and cannot demonstrate accountability as required under Article 5.2 of the UK GDPR.	A.08.A. LBWF should start reporting its KPIs on SAR performance and individual rights requests under the UK GDPR on a routine basis. This will ensure that LBWF has oversight on its compliance with statutory timescales and can demonstrate accountability as required under Article 5.2 of the UK GDPR. B. LBWF should start reporting its KPIs on records management including use of metrics such as file retrieval statistics, adherence to disposal schedules, and the performance of the system in place to index and track paper files containing personal data. This will ensure that LBWF has oversight on its compliance with statutory obligations and can demonstrate accountability as required under Article 5.2 of the UK GDPR.	Urgent
Performance to IG KPIs is reported and reviewed regularly.	See A.08.A and B above	See A.08.A and B above	

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
There are written contracts in place with every processor acting on behalf of the organisation which set out the details of the processing	A.09.A. LBWF does not have a central log of all processor contracts it currently has in place. This means it does not have oversight of all the processing of personal data being done by third party processors. B. LBWF provided insufficient evidence that the contracts it has in place with data processors are reviewed on a periodic basis. By not reviewing the agreements it has in place with processors on a periodic basis LBWF risks personal data being processed by third parties where it is no longer fit for purpose or in line with the correct requirements.	A.09.A LBWF should record all of its contracts in place with processors that are processing personal data on a central log. This will ensure that LBWF has oversight of all the processing of personal data being done by third party processors. B. LBWF should review the contracts it has in place with data processors on a periodic basis. This will ensure that all processing being undertaken by processors remains fit for purpose and in line with legislative requirements.	Urgent
The organisation has sought sufficient guarantees that a potential processor will implement appropriate technical and organisational measures to ensure their processing will meet UK GDPR requirements and protect data subjects' rights.	A.10. LBWF does not currently have standard due diligence checks built into its procurement process prior to engaging the services of a processor. Without seeking sufficient guarantees that a potential processor will implement appropriate technical and organisational measures to ensure their processing will meet UK GDPR requirements and protect data subjects' rights, LBWF risks breaches of the controller/processor requirements and non conformance with Articles 28.1 and 5.2 of the UK GDPR.	A.10.A. LBWF should implement a set of standard due diligence checks within its procurement process prior to engaging in services with a processor. This will ensure that LBWF has sufficient guarantees that its processors are implementing appropriate technical and organisational measures to ensure their processing will meet UK GDPR requirements and protect data subjects' rights, as required by Articles 28.1 and 5.2 of the UK GDPR. B. In addition to A.10.A, LBWF should have a documented process to add additional due diligence checks such as site visits and system testing, where it is appropriate to the level of risk of the processing taking place.	Urgent

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
The organisation takes accountability for ensuring all processors comply with the terms of the written contract(s)	A.11. It was evidenced that LBWF includes clauses within its contracts to allow the organisation to conduct audits or checks to confirm the processor is complying with all contract terms and conditions. However, LBWF was unable to evidence that it conducts compliance checks on its processors on a routine basis. This means LBWF has no assurance that their processors are abiding by the terms of their contract as required by UK GDPR Articles 28 and 5.2.	A.11. LBWF should conduct routine compliance checks on its processors that are appropriate for the risk of the processing that is undertaken. This will ensure that LBWF has assurance that its processors are abiding by the terms of their contract as required by UK GDPR Articles 28 and 5.2.	Medium
The organisation has a process to ensure all processing activities are documented accurately and effectively	A.12. It was reported that LBWF had not conducted any information audits or data mapping exercises for its Record of Processing Activities (ROPA). This means that LBWF lacks assurances that it has captured all of its processing activities within its ROPA.	A.12. Conduct information audit or data mapping exercises across its service areas, consulting relevant staff members a required, to gain assurances that all processing activities are reflected within the ROPA.	High

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
There is an internal record of all processing activities undertaken by the organisation	A.13. It was reported that there is a process in place to ensure that the ROPA is reviewed and updated on a regular basis by both service areas and the data protection team. However the ROPA document provided to auditors had a number of unfilled sections across different service areas including the lawful basis for processing. This means that the processes LBWF currently have in place to ensure the ROPA is routinely updated and reviewed are not sufficient.	A.13. LBWF should review its processes for reviewing and updating the ROPA to ensure that all service areas have fully documented their current processing activities and update these on a routine basis.	High
The information documented within the internal record of all processing activities is in line with the requirements set out in Article 30 of the UK GDPR.	See A.13. See A.09.A	See A.13. See A.09.A	
The lawful basis and condition(s) for processing personal data, special category data and data relating to criminal convictions and offences has been identified appropriately, defined and documented internally.	See A.13.	See A.13.	

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
The lawful basis or bases for processing personal data and special category data is made publicly available	A.14. The lawful basis for processing personal data is not specified on all of LBWF's departmental privacy notices, such as the Adult social care privacy notice. This means LBWF risks non compliance with Article 13.1.c of the UK GDPR.	A.14. LBWF should review its departmental level privacy notices to ensure that the purposes of the processing and the lawful basis for processing are clearly documented. This will ensure compliance with Article 13.1.c of the UK GDPR.	High
Where the organisation is required by Schedule 1 of the DPA 2018 to have an Appropriate Policy Document (APD) in place, the document in place is sufficient to fulfil the requirement	A.15. LBWF does not have an Appropriate Policy Document (APD) in place for its processing of special category data under Schedule 1 of the Data Protection Act 2018. This means LBWF has failed to meet its obligations under Schedule 1 of the DPA 18 and Articles 5.1.a and 5.2 of the UK GDPR.	A.15. LBWF should create an APD for the processing of special category data and criminal offence data that it processes under Schedule 1 of the DPA 18. This document should demonstrate that the processing of special category and criminal offence data based on these specific Schedule 1 conditions is compliant with the requirements of the UK GDPR Article 5 principles. This will ensure compliance with Schedule 1 of the DPA 18 and Articles 5.1.a and 5.2 of the UK GDPR.	High
Consent mechanisms used meet the UK GDPR requirements on being specific, granular, clear, prominent, opt-in, documented and easily withdrawn.	A.16. Evidence provided to ICO auditors of a Fostering applicant form did not provide information to individuals when seeking consent on their right to withdraw consent and how to do this. Failure to provide this information may mean that the consent obtained by LBWF becomes invalid and non compliant with Articles 6 and 9 of the UK GDPR.	A.16. LBWF should review its consent forms to ensure that they all provide information on the individual's right to withdraw consent and how to do this. This will ensure that consent obtained by LBWF remains valid and in compliance with Articles 6 and 9 of the UK GDPR.	High

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
Where the lawful basis is Legal Obligation, the organisation has clearly documented the obligation under law for that type of processing activity for transparency purposes.	See A.14.	See A.14.	
The organisations privacy information or notice includes all the information as required under Articles 13 & 14 of the UK GDPR.	See A.14	See A.14.	
Existing privacy information is regularly reviewed and, where necessary, updated appropriately.	A.17. LBWF does not currently conduct user testing on its privacy information. This means LBWF has no assurance on the effectiveness of the communication of its privacy information.	A.17. LBFW should conduct user testing on its privacy information. This will ensure LBWF has assurance that its privacy information is effective and understandable for individuals.	Low

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
Fair processing policies and privacy information are understood by all staff and there is periodic training provided to front line staff whose role includes the collection of personal data on a regular basis.	A.18.A. LBWF's mandatory data protection training does not include information on fair processing and privacy information. This means staff may not be aware of the importance of providing data subjects with privacy information and provide incorrect guidance to individuals. B. Evidence provided to auditors of additional data protection training provided to frontline staff did not include how to recognise individual rights requests including subject access requests. This means that frontline staff may not recognise and correctly handle individual rights requests or provide appropriate privacy information to individuals.	A.18.A. LBWF should include guidance on fair processing and privacy information within its mandatory data protection training for all staff. This will ensure that staff are aware of the importance of providing data subjects with privacy information and provide correct guidance to individuals. B. Specialist training provided to front line staff should include guidance on fair processing information and individual rights requests including subject access requests. This will ensure that front line staff can give correct guidance to individuals and correctly identify and handle individual rights requests.	High
DPIA are undertaken before carrying out types of processing likely to result in high risk to individuals' rights and freedoms	A.19. LBWF's DPIA template does not include a section for staff to clearly set out the relationships and data flows between controllers, processors, data subjects and systems. This means LBWF risks not fully documenting and considering the flow of data and the parties involved as part of its DPIA and not identifying potential risks related to this.	A.19. LBWF should include an additional section within its DPIA template for staff to clearly set out the relationships and data flows between controllers, processors, data subjects and systems. This will ensure that the flow of data and the parties involved are properly documented as part of its DPIA and any potential risks related to this can be considered.	Medium

Governance & Accountability			
Control	**Non-conformity**	**Recommendation**	**Priority**
The organisation acts on the outputs of a DPIA to effectively mitigate or manage any risks identified.	A.20. LBWF does not have a documented process in place to ensure that the ICO is consulted in the event that there are residual high risks that cannot be mitigated that are identified from a DPIA where the processing may still go ahead. This means LBWF may fail to alert the ICO to processing it may carry out that is considered high risk.	A.20. Create a documented process as part of its DPIA template to ensure that any residual high risks that remain where processing will still commence are reported to the ICO. This will ensure that LBWF does not process data involving a high level of risk without prior consultation and assistance from the ICO.	Medium
There are mechanisms in place to notify affected individuals where the breach is likely to result in a high risk to their rights and freedoms	A.21. LBWF does not include a process within its security and personal data breach reporting policy on the requirement to inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms. This means that individuals may not always be contacted when they should or may receive insufficient information on the incident and the actions they can take.	A.21. LBWF should include a process within its security and personal data breach reporting policy on the requirement to inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms. The process should ensure that when individuals are contacted, they are provided with sufficient information on the breach, any mitigating actions taken by the organisation, any advice on how the individual may protect themselves from the breach, and contact details for the DPO and ICO. This will ensure that individuals are always contacted where appropriate in the event that they are affected by a breach and provided with sufficient information and guidance about the incident.	High

Freedom of Information			
Control measure	**Non-conformity**	**Recommendation**	**Priority**
Responsibility has been assigned to ensure compliance with FOI/EIR	B.01. It was reported that the Director of Customer Service and Business Support has overall responsibility for FOI compliance. The Director is not a member of the Management Board, however the Strategic Director of Residents Services will raise issues connected with FOI request compliance with the Board on an ad hoc basis. The Strategic Director's role has not been documented in the relevant organisation chart or FOI procedure.	B.01. Ensure that the Strategic Director of Residents Services role in escalating issues relating to FOI to the Management Board are documented within the FOI organisation chart and/ or the FOI Procedure.	Low
Policies and procedures are in place which explain the organisation's approach to, and responsibilities for, FOI and EIR	B.02. ICO auditors were provided with the FOI Procedure - Guide for Staff (FOI Procedure), FOI Requests for Employee Information and the Staff Guidance FOI Requests Time Limits. The Staff Guidance FOI Requests Time Limits doesn't have any document controls or a review table. The FOI Requests for Employee Information doesn't include a named owner. If up to date document controls are not in place it may be difficult for staff to understand if they are looking at the latest version of the procedure. It may also be difficult to determine if the guidance has been reviewed and is up to date with the latest ICO and legislative guidance. If a document doesn't have a named owner it may not be clear who is responsible for updating the document and ensuring it remains compliant with the legislation and latest guidance.	B.02. Ensure that all FOI policies and procedures have the requisite document control information, review table and owner.	Medium

Freedom of Information			
Policies and procedures are easily accessible by staff	B.03. It wasn't clear whether staff who may not have regular access to computers are able to read policies and procedures in a non-electronic format. It was reported that line managers could print a copy of the FOI procedures and guidance from the Foresthub (intranet). If staff do not have access to policies and procedures then staff may react to situations differently, resulting in non-compliant actions being taken by LBWF.	B.03. LBWF should review whether staff who work in roles without regular access to computers are able to read a hard copy of the procedure or at the minimum have a guide on what an FOI and ER request is and what to do if they receive one. For example, EIR requests can be made verbally.	Medium
The organisation ensures that staff are informed of any changes to policies and procedures regarding FOI/EIR	B.04. Staff are not required to say whether they have read and understood key policies such as the FOI Procedure. Staff interviewed reported that they had read the procedure and the FOI intranet pages as part of induction, but this is dependent on role and department. It is important that all staff have a basic awareness of FOI and EIR Requests so that they are able to recognise and deal with a request should they receive one. If staff are not aware of how to recognise a request and where to send it there is a risk that it may not picked up and processed within the statutory timescales leading to a breach of the legislation.	B.04. Ensure it is mandatory for all staff to have at least read the key information on Foresthub around FOIs and EIR requests so they know what a request is and what to do should they receive one. They should sign or indicate that they have read and understood this information as part of the induction process. Those staff who are involved in the FOI / EIR request process should be required to read the procedure and also sign off for evidential purposes that they have read and understood the procedure.	Medium

Freedom of Information			
There are reporting mechanisms in place to provide oversight of requests and ensure that statutory deadlines are met	B.05. All FOI and EIR requests are logged on the Achieve system. The system logs the expected information apart from: - details of the type of exemptions used; - whether a clarification has been requested; - Whether the Public Interest Test (PIT) has been applied. This information is recorded within the response letter to the requester on Achieve. However, as these are not actively recorded as fields on the system it means that LBWF are not able to actively report on and complete trend analysis on the use of clarifications, types of exemptions applied and whether a PIT has been applied. If appropriate reporting mechanisms are not in place, LBWF may not be aware of any failure to meet statutory deadlines, and so may not be able to remedy its performance	B.05. LBWF should explore whether it is able to capture the information detailed opposite on the Achieve system and report on it as part of the Management Dashboard to Information Governance Board (IGB).	Medium
There are mechanisms to monitor the quality of responses to requests and ensure that any reasons for refusal/application of exceptions are valid.	B.06. Responses to requests are reviewed and signed off by a manager, usually the head of service, prior to being sent to the requester. However, there are no cold case quality and assurance checks carried out on responses sent out by services by suitable staff such as the GDPR team. This means there is a lack of central oversight and assurance that service areas are adhering to the FOI Procedures and legislative guidance. If there is no monitoring of FOI responses then LBWF may be not be aware if it is misusing any refusals, exceptions, or exemptions, which may result in statutory non compliance.	B.06. A cold case quality assurance process should be established. Periodic reviews of cold case FOI requests should be checked and results recorded and feedback to IGB and the individuals involved in the original request.	High

Freedom of Information			
Contracts with third parties do not restrict the release of information that should be available to the public and provide for access to information, by the public authority, when needed.	B.07. ICO auditors were provided with the Open ITT Template for contracts and a Provision of Cleaning Services Contract. The latter contract contained all the relevant clauses expected regarding FOI requests and responsibilities around disclosing information. However, the Open ITT Template did not include any details around contractors requiring provision of information relating to FOI or EIR requests within a suitable timeframe when requested by LBWF. If there are no clearly documented instructions on timescales when information is required by in order to answer an FOI request then LBWF may not receive the information on time in order to answer the requests within statutory timescales.	B.07. The Open ITT Template should be reviewed and updated to ensure that it contains details around a timeframe for contractors to provide information to LBWF in the event of a request.	High
Documented governance arrangements exist where the authority works in partnership with other organisations in relation to the handling of requests and/or the management of records.	B.08. LBWF has not identified from a central governance viewpoint whether they are interdependent with other organisations in relation to the handling of requests or the management or records. Individual service areas may have local arrangements in place, for example with contractors but there is no central oversight to ensure that appropriate documented arrangements are in place. If there is no clear governance, either or both organisation's may fail to comply with statutory requirements, potentially in the false belief that the other organisation is taking care of the compliance on their behalf.	B.08. Review arrangements across LBWF to understand whether there are any interdependencies with other organisations in relation to the handling of requests or the management of records. Where these organisations are identified LBWF should check whether there are appropriate documented procedures in place for dealing with FOI/EIR requests between the organisations.	Medium

Freedom of Information			
Internal review procedures comply with the relevant Codes of Practice and ensure that timely responses are provided to complaints.	B.09. There is an FOI Review process in place to deal with any complaints about the handling of FOI requests. However, management information around the reviews is not regularly reported to IGB. Statistics around FOI reviews are only reported as part of the annual Information Governance Report to the Management Board. This means there is a risk that LBWF don't have oversight of the complaints received about FOI requests and are not able to monitor whether reviews are completed within timescales or conduct any trend analysis on the type of complaints received.	B.09. FOI reviews should be reported to the IGB on a periodic basis. Data should include a summary of the complaint, the outcome and whether the complaints have been completed within timescales.	Medium

Freedom of Information			
Exemptions/Exceptions should be applied on a case-by-case basis, by appropriately trained staff, with no evidence of the use of blanket exemptions.	B.10.A. Not all staff who are involved in the processing of FOI requests have completed the FOI eLearning modules. This means that staff may not have sufficient knowledge about the key exemptions and how these should be applied. If untrained staff are responsible for applying exemptions/exceptions, then the organisation risks that they will be applied incorrectly, or not applied at all. B. The FOI Procedure and template letters don't say that exemptions should be applied on a case by case basis. Interviewees did indicate that they would consider the individual facts of each request before deciding whether information should be withheld. The statutory requirement is for case by case decision making, and failing to do so would place LBWF in a position of non compliance.	B.10.A. Ensure that all key staff have received sufficient training on FOI requests, including on the key exemptions. B. The FOI Procedure and template letters should be updated to remind staff that exemptions should be applied on a case by case basis.	High

Freedom of Information			
There is evidence of an oversight or approval process for the use of exemptions.	B.11. It was reported that a senior manager such as the Head of Service, authorises the response and release / withholding of any data to the requester. For high priority FOI requests these are reviewed and signed off by a strategic director. This authorisation is recorded via email and a copy of the authorisation is held on Achieve. It doesn't appear that requirements around this authorisation process have been documented within the FOI Procedure. If there are no documented requirements around the approval process then service areas may not be following an approval process and may misapply exemptions.	B.11. Update the FOI Procedure to ensure it reflects the process followed by service areas around the authorisation of requests and the withholding of information under an exemption. A record of authorisations should be held on Achieve as evidence.	Medium

Freedom of Information			
Redactions should be applied on a case-by-case basis, by appropriately trained staff, and records should be maintained of what has been redacted.	B.12.A. Staff demonstrated an awareness of how information should be redacted but have not received any formal training on how to safely redact information. B. Guidance on redactions is contained within the SAR Guidance but there is no reference within the FOI Procedure to this guidance. If staff are not adequately trained or do not know how to access appropriate guidance on how to safely redact information this may lead to redactions being improperly applied and LBWF accidently disclosing information that should be withheld. C. Although a record of the redacted information is held as part of the response it may not be clearly marked to show which exemptions have been applied to allow the withholding of this information. This is important for audit trail purposes particularly for cold case reviews, FOI Reviews or should the ICO wish to review the decision to withhold the information.	B.12.A. LBWF should consider formal / specialist training for staff who need to redact information, the safest methods for doing so and the consequences if this is not followed. B. The FOI procedure should be updated to include reference to the redaction guidance within the SAR Procedure. This will ensure that staff are aware of how to find the guidance. C. Where information has been withheld under an exemption a copy should be kept with a note or label explaining why the information has been withheld. This should be kept on Achieve for audit purposes.	High
There is evidence of an oversight or approval process for the use of redactions.	B.13. Redactions are not subject to dip sample checks. This means that LBWF has no assurance outside of FOI reviews that redactions are being appropriately applied.	B.13. See B.06.	

Freedom of Information			
The organisation is complying with statutory timescales for FOI/EIR	B.14.A. LBWF don't centrally monitor or record the use of the PIT and delays for clarification. It was reported that the use of PIT is very rare. If LBWF don't actively monitor use of PIT and delays for clarifications it cannot demonstrate oversight and gain assurance that the use of these is both reasonable and proportionate. B. Achieve doesn't not allow for an extension to be added to the FOI request timescale and doesn't not have a formal process in place for monitoring the use of extensions. This means LBWF may be at risk of not having oversight of requests that are completed outside of the 20 working day timescale.	B.14.A LBWF should consider updating Achieve to include monitoring of PIT and clarifications of requests and monitor how these are applied to ensure this is proportionate and reasonable. B. LBWF should explore whether Achieve could add a facility to extend the timescale of a request so that an extended FOI can be centrally monitored. Alternatively a process for monitoring any extended FOI requests outside of Achieve should be created and documented.	Medium
There is an induction training programme, with input from Information Governance or equivalent, which includes general training on how FOI/EIR applies to the organisation, what they currently do to comply, and how to recognise an FOI/EIR request.	B.15. There is an FOI eLearning module in place for FOI which is in two parts. It was reported that staff who handle FOI requests complete this as part of the induction process, but the training isn't mandatory unless specified by the service area. It was reported that this training module may be too detailed for some roles. If all staff do not receive training on FOI requests then LBWF cannot demonstrate that it has controlled the risk of them acting in non-compliance with legislative requirements.	B.15. LBWF should ensure that all staff receive at least a basic level of training on FOI and EIR requests. Training should cover what a request is, how a request may be received (i.e. can be via social media, EIR requests can be verbal), the fact the request doesn't need to reference the legislation and what to do if they receive a request. This training should be mandatory for all staff and be refreshed on a regular basis.	High

Freedom of Information			
Staff receive refresher training in the requirements of FOI/EIR, including, where appropriate, updates from the relevant decisions of the ICO and the Information Tribunal.	B.16. There is no mandatory refresher training in place relating to FOI requests.	B.16. see B.15.	
There is specific training for staff with responsibility for handling requests for information, on FOI, EIR and Codes of Practice.	B.17. It was reported that the staff who handle requests have completed the FOI Part 1 and Part 2 eLearning module. However, it wasn't clear whether this training was mandatory across all service areas for staff who handle or are involved in reviewing and signing off requests. It also wasn't clear how often this training is refreshed. If staff have not received adequate training or refresher training there is a risk they may not act in compliance with LBWF procedures or the legislation.	B.17. Specialist training should be mandatory for all staff who process FOI and EIR Requests. This training should be refreshed on a periodic basis.	Medium
Records are maintained, either centrally or by local management, of the FOI/EIR training received by staff. These records are monitored to ensure that all staff receive or attend all relevant training.	B.18. FOI training completion and specialist training completion is not currently monitored by the IGB. If LBWF cannot demonstrate that they have provided training, they have no assurance that comprehensive training has been carried out. They will be unable to carry out checks, reviews, or monitoring of completion rates.	B.18. The IGB should monitor the completion rates of all staff FOI training and specialist training (at both induction and refresher stages). This will help LBWF provide assurance that all staff have received the correct training.	Urgent

Freedom of Information			
Staff receive regular reminders of how to recognise FOI/EIR requests	B.19. There is no formal communication plan in place to help promote awareness of FOI and EIR requests. If staff do not recognise requests, there is a risk that they may not inform the organisation the request has been submitted, which may prevent it being responded to within the statutory timescale.	B.19. LBWF should consider creating a communication for IG issues including FOI/EIR request awareness to ensure that awareness continues to be raised amongst staff.	Medium

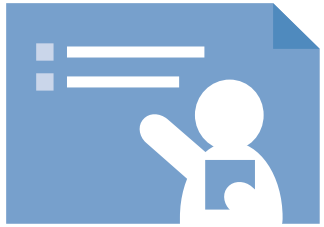
Observations

The tables below list observations made by ICO auditors during the course of the audit along with suggestions to assist LBWF with possible changes.

Governance & Accountability	
Control	**Observation**
The information documented within the internal record of all processing activities is in line with the requirements set out in Article 30 of the UK GDPR.	Where LBWF's lawful basis for processing personal data is consent, LBWF does not currently include or link to the records of this consent within its ROPA. LBWF should consider adding this information to its ROPA to ensure that the document provides a sufficient level of information on all its processing activities.
Where the lawful basis is Legitimate Interests, the organisation has conducted a legitimate interests assessment (LIA) and kept a record of it.	It was reported that LBWF does not currently process any personal data under the lawful basis of legitimate interests and that it does not have a legitimate interests assessment (LIA) template in place in the event that an assessment was needed. LBWF should consider creating a LIA template so there is a clear process to follow in the event that it needs to conduct an assessment.

Freedom of Information	
Control measure	**Observations**
Responsibility has been assigned to ensure compliance with FOI/EIR	LBWF should consider conducting formal documented reviews against workloads and timescales to provide additional evidence that they give adequate consideration to statutory obligations in relation to FOI requests.
Internal review procedures comply with the relevant Codes of Practice and ensure that timely responses are provided to complaints.	The FOI Procedure includes a section on FOI reviews. However, it doesn't include reference to the 20 working days deadline for completion of the reviews. LBWF should consider adding this into the procedure.
There is specific training for staff with responsibility for handling requests for information, on FOI, EIR and Codes of Practice.	LWBF should extend the more service focused specialist FOI training carried out by the Data Protection Manager to enhance and compliment the eLearning module. The training delivered by the Data Protection Manager was very well received.

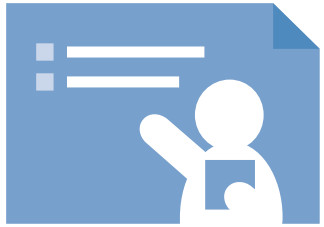
Appendices



Appendix One – Recommendation Priority Ratings Descriptions

Urgent Priority Recommendations - These recommendations are intended to address risks which represent clear and immediate risks to the data controller's ability to comply with the requirements of data protection legislation.
High Priority Recommendations - These recommendations address risks which should be tackled at the earliest opportunity to mitigate the chances of a breach of data protection legislation.
Medium Priority Recommendations - These recommendations address medium level risks which can be tackled over a longer timeframe or where some mitigating controls are already in place, but could be enhanced.
Low Priority Recommendations – These recommendations represent enhancements to existing controls to ensure low level risks are fully mitigated or where we are recommending that the data controller sees existing plans through to completion.

Credits



ICO Audit Team

ICO Team Manager – Lauren Sherratt
ICO Engagement Lead Auditor – Eve Wright
ICO Lead Auditor – Helen Oldham

Thanks

The ICO would like to thank Olivia Shaw (Head of Executive and Hospitality Services) for their help in the audit engagement.

Distribution List

This report is for the attention of Louise Duffield (Director of Customer Services and Business Support), Olivia Shaw (Head of Executive and Hospitality Services) and Mark Hynes (Director of Governance and Law).

Disclaimer

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of London Borough of Waltham Forest Council.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

This report is an exception report and is solely for the use of London Borough of Waltham Forest Council. The scope areas and controls covered by the audit have been tailored to London Borough of Waltham Forest Council and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.