Appendix 2 - Recommendations

Section 1: Back office Governance Management (Information Governance)

R01 Establish an information governance working group to work, co-opting data protection champions from the business to a forum that would monitor, review and drive the data protection agenda – in the same way that a health and safety committee might have the similar impact in that discipline. Consider the role of the legal department in that forum.

R02 Establish KPIs with which to measure data protection performance.

R03 Appoint a DPO.

R04 Review and improve the governance framework to include policies required by GDPR such as incident reporting and management, privacy impact assessment etc. and test existing against GDPR requirements. Introduce periodic audit, testing and review of the controls. Update the document register to include new policies, procedures and work instructions.

R05 Introduce an information risk register to accurately record information risks and mitigation and ensure that it is periodically reviewed.

R06 Define and implement a policy and procedures on privacy impact assessments (PIAs). Ensure that PIA processes encompasses the requirement to consult the Regulator in certain circumstances.

R07 Ensure that data protection training is provided at induction and at least on an annual refresher basis. Supplement this with more frequency (monthly) awareness raising of relevant issues or changes in policy.

R08 Introduce compliance checking and audit processes that comply with GDPR's requirements the scope of which will ensure that evidence will be available to demonstrate that LBB complies with the GDPR. Appoint appropriate audit team, internal and external. As a guide this is likely to be at least annual audits of all data protection policies and operating procedures and the gathering and recording of objective evidence of compliance and/or the raising of corrective action requests to modify behaviour in line with policy.

Section 2: Collection and use of data

R09 A register of data processing purposes should be compiled and maintained to assist with other compliance measures such as ensuring the legal basis for processing for each purpose and the formation of privacy information.

R10 Improve evidence of data processing control by reviewing all data that is held and documenting its purpose and lawful grounds for processing particularly in regard of sensitive personal information and behavioural information. Compile a register of data processing purposes as set out in recommendation R08 and ensure that the lawful grounds for processing are marked against each data processing purpose.

R11 To ensure that LBB is able to demonstrate control over its data acquisition processes it is necessary to review all sources of personal data, compile a register of data sources, and ensure there is a process for keeping it up-to-date.

R12 The privacy information provided at all data collection points need to be reviewed and updated in line with the requirements of the GDPR. It might be useful to create and maintain a register of data collection activities and customer "touch points". LBB should introduce a policy on privacy information which ensures data collection activities are reviewed and approved by the information governance steering group (see recommendation **R01**).

R13 Create and maintain an information asset register

R14 Document key data flows to ensure a thorough understanding of how data is captured and moved about the LBB data systems.

R15 Create a system to maintain information describing and defining the data being handled by LBB and the categories of data subject.

R16 Create a data sharing policy setting out a standard process for employees to follow to lawfully share and/or disclose personal data including appropriate pre-contract due diligence.

R17 Establish a register of data sharing agreements/arrangements and undertake a geographic review of all data processors is undertaken once a full list is compiled.

R18 Ensure that an agreement is in place with all instances of outsourced processing and/or sharing. Test each agreement to ensure that: a) the terms are in LBB's favour and compliant with the needs of GDPR; b) indemnities are appropriate; and c) the data processing instructions issued are effective. Consider creating standardised templated agreements.

R19 Undertake a privacy impact assessment on the data processors used in order to properly assess the risks that it might pose and/or to document the measures taken to ensure that adequate protection is in place.

R20 Review existing transfer arrangements and introduce a policy defining approved secure data transfer and operating procedures for employees. If Excel and email are to be used ensure that spreadsheets are password protected or encrypted. Ensure that suitable secure email facilities are provide to employees who need such a method.

R21 Review all data sharing and transfers to test if data is transferred outside of the UK and test the adequacy arrangements where international transfers occur.

R22 Introduce a process for periodically reviewing the adequacy arrangements for all overseas processors to ensure that their adequacy arrangement does not lapse and for ensuring that new arrangements are not put in place without appropriate due process.

R23 Draft a data quality policy focussing on how different types of information will be maintained accurately. Give emphasis in particular to data such as communication preferences, volatile data which may change frequently, data based on opinions and hear-say, and data which would cause harm/distress to the subject if it is incorrect such as that collected through housing, public health, environmental services, and social services.

R24 Undertake a deep dive review of data being collected and handled by LBB and consider what steps would be appropriate to implement a data minimisation strategy.

R25 Review the data processing purposes and data used for each processing activity and determine how long it needs to be held in a format allowing identification of data subjects for the purpose(s). Review which mechanisms would be appropriate in each of the cases to enable LBB to comply with the 5th data protection principle. This information is most likely best to come from each department who are either applying their own retention periods or need assistance in their determination.

R26 Carry out a deep dive exercise on data retention across all information assets then review and to disseminate the records management policy and retention schedules for compliance and work-ability.

R27 Engage with the 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.

Section 3: IT Controls

R28 Review ICT policy framework to ensure that they are adequate for GDPR purposes and review the strength of the IT team.

R29 The physical and logical measures to control access to the network and data are in place at LBB but some of the controls have been poorly applied (such as assigning permissions and rescinding the rights of movers and leavers). LBB should undertake a comprehensive review of user permissions and enforce the JML process.

R30 The process of signing in/out of files in areas such as social services should be revised to provide enhanced control as well as improvements to the procedures for handling paper files.

R31 Review encrypted email solutions and enforce their use in circumstances where personal data are being transferred via email presenting a risk to privacy.

R32 Introduce regular periodic vulnerability testing of networks to assist in the identification of threats and information security assurance.

R33 Consider using dedicated log servers to improve logging of events on the systems and also increasing the frequency of IT security audits.

R34 LBB needs to determine a policy and apply it in relation to BYOD.

R35 Implement the policy discussed of recalling approximately 800 mobile devices, improve the JML process to ensure leavers who have been issued with mobile devices are appropriately handled, improve the policy used to acquire confirmation by mobile device users to abide by LBB's acceptable use policy, and review the recycling of SIM cards.

R36 Improve confidential waste handling processes and equipment. Locked cabinets are far superior to sacks for the collection of confidential materials awaiting destruction.

R37 Document how redundant equipment and media are to be disposed of.

R38 Review existing arrangements and test for GDPR compliance.

R39 Review incident reporting provisions to ensure alignment with GDPR. Remind employees through awareness and training.

R40 Review all processor contracts for information security breach notification provisions.

Section 4: The Rights of Data Subjects

R41 It is recommended that all privacy statements and privacy forms are reviewed, catalogued and revised to ensure compliance with the GDPR.

R42 Introduce work methods to ensure that privacy information and its publishing/deployment are strictly controlled.

R43 Devise *a fair processing strategy that provides a workable layered approach to privacy information.*

R44 *Review data systems to ensure that they are able to record what privacy information each data subject has been provided with.*

R45 Create a centralised register of dSARs to ensure visibility and consistent handling. Write a dSAR policy and process and ensure employees are trained in its application if a distributed model for handling them is maintained.

R46 Establish a mechanism for logging any objection raised by a data subject and determining the extent to which their legitimate interests might over-ride those of data subjects.

R47 Review data processing activities and test them against automated decision-making rules.

R48 Establish a mechanism for logging a request for data portability and a process for the effective and secure execution of any transfers of data and further consider where and when such requests might arise.

R49 Define and implement a method of applying restricted processing to data where a relevant objection is received.

R50 LBB should review its processes for executing R2BF requests and also improve its understanding of who data is shared with or disclosed to in order to facilitate onward notification of data erasure or modification.

R51 Identify where R2BF requests may come from. Introduce a R2BF policy and procedures which can identify and erase data as appropriate. Introduce a process which ensures LBB is able to identify and log any such request and execute it in a timely manner.