BROMLEY CIVIC CENTRE, STOCKWELL CLOSE, BROMLEY BRI 3UH

THE LONDON BOROUGH
www.bromley.gov.uk

TELEPHONE: 020 8464 3333
CONTACT: Graham Walton
graham.walton@bromley.gov.uk

DIRECT LINE: 020 8461 7743
FAX: 020 8290 0608

DATE: 28 November 2017

EXECUTIVE

Wednesday 6 December 2017

9 REVIEW OF CORPORATE CUSTOMER SERVICES IT SYSTEMS

Please note that this report has been WITHDRAWN (including the part 2 appendix at agenda item 23.)

10 THE GENERAL DATA PROTECTION REGULATIONS 2016 (Pages 3 - 32)

The report marked as “to follow” on the agenda is now attached.

Copies of the documents referred to above can be obtained from http://cds.bromley.gov.uk/

This page is left intentionally blank

London Borough of Bromley

Report No. CSD17173	PART I – PUBLIC	Agenda Item No.:

Decision Maker:	**Executive**
Date:	**6th December 2017**
Decision Type:	Non-Urgent Executive Key
TITLE:	**THE GENERAL DATA PROTECTION REGULATIONS 2016**
Contact Officer:	Mark Bowen and Vinit Shukle Tel: 020 313 4461 email: Mark.Bowen@bromley.gov.uk; Vinit.Shukle@bromley.gov.uk
Chief Officer:	Mark Bowen, Director of Corporate Services
Ward:	All Wards

1. REASON FOR REPORT

This report details the significant changes that will be required to ensure that LB Bromley is compliant with the General Data Protection Regulations 2016 (GDPR). The GDPR will apply in the UK from 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

2. RECOMMENDATIONS

Executive are requested to:

2.1 Note the changes proposed by the GDPR and the work to be undertaken to address them.

2.2 Agree a one-off cost of £495k from the under spend in the 2017/18 Central Contingency, in order to progress the works required to enable the Council to become GDPR compliant.

2.3 Agree growth of £287k for the two permanent staff, training & system running costs.

2.4 To note that an additional member of staff may be required to take on the additional responsibility of a Data Protection Officer (DPO) as required under the Article 37 of the GDPR. A report will be brought back to Members to confirm the allocation of this role.

Corporate Policy

1. Policy Status: Existing Policy

2. BBB Priority: Excellent Council

Financial

1. Cost of proposal: Estimated Cost £495k one-off costs and £287k on-going costs

2. On-going costs: Recurring Cost £287k per annum

3. Budget Head/Performance Centre: Information Management

4. Total current budget for this Head: £129k

5. Source of Funding: Existing revenue budget and Central Contingency

---

Staff

1. Number of staff (current and additional): 2 FTEs

2. If from existing staff resources, number of staff hours:

Legal

1) Legal Requirement: Statutory Requirement/Non-Statutory Requirement – Government guidance/No Statutory Requirement or Government Guidance

2) Call In: Call In is applicable/Call In is not applicable

Customer Impact

1. Estimated number of users/beneficiaries (current and projected)

Ward Councillor Views

1) Have Ward Councillors been asked for comments: No

2) Summary of Ward Councillors comments:

3. Commentary

The General Data Protection Regulation (GDPR) will replace the Current Data Protection Act (1998) on 25th May 2018. Although originating in EU law, the provisions will apply regardless of the position reached on Brexit and the government has introduced a Data Protection Bill to Parliament. This report highlights some of the key changes that will have an impact on the Council. The Report also outlines the initial and ongoing investment in resources and technology that will be required to ensure that LB Bromley adheres to this legislative change.

3.2 GDPR radically increases penalties. The maximum penalty for non-compliance and data breaches has increased from £500k to a maximum of £18m or 4% of the annual turnover of an organisation. Under the present system penalties of 10-20% of the maximum are frequently imposed for breaches and it is likely that significant (£1m+) penalties will be imposed from an early stage.

3.3 The GDPR places increased emphasis on the documentation that the Council must maintain in order to demonstrate accountability. Compliance within all areas listed in this report will require the Council to review its policies and approach to information governance and how data protection is managed as a corporate issue.

3.4 GDPR will impose significant changes on the information governance structure of the Council. This will include interaction with customers, the way in which information is recorded, the way in which data processing activities are communicated and a number of other areas all relating to the Council's processing activities of personal information. It will have a significant impact on all directorates and contractual arrangements. The Key Changes required by GDPR are set out in Appendix 1.

3.5 In preparation for this change, an independent review has been undertaken by the Data Protection People (DPP), who were invited to carry out a data protection compliance review and initial gap analysis to compare current practices against the GDPR.

3.6 The review identified good current practice but provided 51 recommendations that LBB need to action to advance towards being compliant with GDPR. A High Level Project Plan has also been provided to assist LBB in its efforts to be compliant by the go-live date of GDPR. The recommendations are attached as Appendix 2.

3.7 Taking the 51 recommendations set out by the Data Protection People, a project plan has been created expanding on the recommendations and creating actionable tasks for working towards GDPR compliance. The actions to ensure compliance to GDPR are attached as Appendix 3.

3.8 There is a need for additional staff support across the organisation to help balance the need for business as usual continuity and addressing the gaps between current practice and the requirements of the GDPR. The risk of diverting attention from one to the other without a measure of the consequences for not meeting either requirement could be detrimental to finances, reputation and compliance to meet various essential accreditations.

3.9 A need for an Information Management Team to be established has been identified to effectively deliver the change. This allocation of resources and associated costs is deemed proportionate to the potential fines and consequences of non-compliance.

3.10 The 25th May 2018 is not a finish line. There is an immediate need to accelerate and increase efforts to meet the go live date, balanced by consideration of the cost of upholding new ways of working. To maintain a demonstrable business process, manage efficiencies and sustain the effectiveness of technological implementations it is necessary to increase staffing to support the organisation.

3.11 Challenging system suppliers and application developers to provide a system that helps to support the business processes in GDPR compliance is a necessity.

3.12 The Council will be putting pressure on bespoke suppliers and in conjunction with other Councils that use common applications, add some weighted peer pressure to encourage them to provide updates to functionality that enables us to work effectively, efficiently and in line with the law.

3.13 It is likely these changes will come at a cost, and consideration needs to be given to having a central budget to support shortfalls in departmental budgets.

3.14 The Council is reviewing its information/data management procedures and policies. Appendix 4 sets out Current policies, where they have been reviewed and updated for GDPR compliance and also identifies new policies which are being or will need to be developed.

3.15 As part of the preparation for GDPR, consideration has to be given to how documents are stored, managed accessed and destroyed. This will also be a key aspect of the work required to move to paper light working, which will be necessary as a part of the accommodation changes.

3.16 The Council has purchased an information asset register system which is presently being rolled out across the Council. This will ensure that key information about the Council's records and systems is recorded in a way which will be compliant with GDPR. Work is also underway to revise polices on document retention and destruction.

3.17 Information Asset Owners and Assistants, who will be responsible for reviewing and implementing document retention policies for their departments have been identified and are being trained.

3.18 Work is also progressing to upgrade and improve SharePoint, which is the council's electronic system for storing and managing unstructured data/information.

3.19 In order to progress the work that has been carried out by the officers and to ensure compliance with the GDPR, additional resources are required including staffing, training and technology.

Staffing

3.20 A permanent Information Management Team is required to oversee and ensure that LBB will be ready for the change in legislation, as well as comply with the GDPR, Information Governance Toolkit, GDPR, Public Service Network (PSN) and Payment Card Industry Data Security Standards (PCI DSS). This will also ensure that LBB is advancing towards becoming a paper light council.

3.21 The team should be made up of a Head of Information or CISO (Chief Information Security Officer), an Information Governance Officer (IGO), an Information Management Officer (IMO) and to include a Support Officer role. The IGO and IMO roles are presently undertaken by existing officers within the Information Services team, who were not in scope for transfer to BT as part of the recent TUPE transfer. A successful bid has been made for support from the Council's Graduate scheme, to support GDPR work in the short to medium term.

3.22 A summary of key aspects of the roles is set out in Appendix 5.

3.23 The team will need to be reviewed annually to ensure adequate resources are assigned to ensure ongoing programs/projects and improvements in Information Management for the organisation. Two additional posts are required above the current establishment – A Head of Service and a Support Officer, which will cost approximately £117k.

3.24 The team will be responsible for the delivery and improvement of the following, to name a few:

- Information Governance Polices
- Development and review of Information Governance & GDPR e-training
- Development of the Corporate Data Sharing Agreement
- Audit of the contracts to ensure that the contract is supported by Data Sharing Agreement
- Development of the Privacy Impact Assessment framework and training for staff
- Data subject consent request on telephone and websites
- Possible communication to the public informing them of what LBB is doing to be compliant with GDPR and possible information relating to their data, that LBB are collecting
- Develop and form GDPR working group
- Develop and deliver an Information Asset Register
- Active Directory cleansing to remove all users that are no longer a LBB employee
- Streamline starter and leavers process
- Carry out system audits to ensure that all systems used by LBB comply with GDPR
- PSN Compliance
- PCI Compliance
- IG Toolkit Certification

3.25 In addition to the permanent team, four temporary workers will also be required, to develop and deliver the project/program. This would include two support officers and a project co-ordinator/Manager for 18 months to support the Information Governance Officer and Information Management Officer/Architect, in policy development that is required by GDPR and the Information Asset Register delivery.

3.26 A legal support will also be required for a period of 12 months to check and put in place Information Sharing Agreements, drafting of privacy notices, dealing with contract variations, drafting appropriate commercial contracts clauses and providing general legal support to the Information Management Team and the Council as a whole in connection with the GDPR coming into force

3.27 This will ensure coordination of departmental and corporate policies as well as develop, edit and review all processes and policies that are required. The resources will also be assigned to coordinate the GDPR Program with the Information Management Program that will run pre and post introduction of GDPR.

3.28 The estimated cost of the four temporary posts over the 18 months is £240k.

Information Strategy and Framework

3.29 With the Accommodation Project commencing, (subject to final Member decision) there will be a greater need for the Information Management and Information Retention policy to be written and communicated. The responsibility of this work will lie with the Information Management Team, who will commission the work.

3.30 A high level gap analysis of the current initiatives and future requirements has identified the need for a coordinated Information Management Strategy and Framework, which, together with the above mentioned initiatives, will provide the foundations for the Council's new working practices.

3.31 The approximate cost of £55k is envisaged for the key deliverables that are:

- A comprehensive framework for information governance and management
- A vision for how information should be managed through an Information Management Strategy
- Develop an enterprise approach to Information Architecture
- Provide a Target Operating Model for an information management function
- Identify how current initiatives including the Civic Centre Programme and the SharePoint Implementation can be improved and how these initiatives can be fitted into a wider programme of information management improvements
- A report outlining a series of pragmatic recommendations, detailing where appropriate, the associated estimated costs, effort, impact, risk and benefits of each

3.32 The Council is embarking on the FAST (Crayon) Software Asset Management programme. A gap analysis is being scheduled in the next 10 weeks to allow us to work towards Bronze accreditation. The ultimate goal is to reach Platinum level which takes a minimum of three years to achieve. In conjunction with BT the Council will be reviewing the software licenses held for Microsoft, IBM, Oracle and other

peripheral developers. This programme will be moderately labour intensive for the period of 3 years.

3.33 ISO27001is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes.

3.34 Recent development in Technology and infrastructure has resulted in the threat landscape evolving at an ever increasing pace, the threat agents becoming more intelligent and resourceful and the attack vectors and vulnerabilities being identified and circulated more efficiently on the dark web.

3.35 The ability of the Council to comply with PSN Certification, PCI DSS standards as well as remediate exploits and vulnerability, brings the Council close to achieving ISO27001 certification and align with ISO27002 (a best practice collection of information security guidelines that are intended to help an organisation implement, maintain, and improve its information security management).

3.36 As a Commissioner and Data Controller, we are increasingly demanding our Third Party Processors and Data Processors to be ISO27001 accredited and prove ongoing compliance. To be viewed as a trusted Commissioner, we should be in the same state of compliance.

Technology

3.37 Approximately £200k will be required to implement various technologies to ensure that LBB comply with GDPR, such as:

- HR System EDRM
- The Security Information and Management (SIEM)
- Data discovery tool that can assist with subject access requests, ring fencing for pause requests and subsequent erasure requests.
- Scanning and Document Management to promote paper light office
- Document Classification
- Email classification
- Pseudonymisation

3.38 From a technology perspective the Security Information and Management (SIEM) tool that provides a holistic and centrally managed view of an organisation's information technology (IT) security, will need to be introduced, as this will enable Information and Security Audits to take place. The cost of the system is £90k and it is envisaged that the on-going running costs will be approximately £50k per annum.

3.39 A key vulnerability will be around how HR information is held and consideration should be given to procuring a new consolidated HR system to manage documentation in a way which ensures compliance with GDPR.

3.40 Currently, HR holds all personnel files as hard copy, paper records. As well as the significant storage and office space this takes up, there is also a need to look at more secure ways of storing this information.

3.41 Having carried out some initial soft market testing with companies that could provide an EDRMS, it is envisaged that the initial set up costs would be approximately £110k and £90k per annum for on-going hosting and license costs.

3.42 As well as compliance of GDPR, a new HR system (EDRMS) will deliver a number of other benefits such as:

- Automatic retention schedules and deletion of data in line with these
- Freeing up of office space which will aid any development of the Civic Centre site
- Facilitating more flexible working
- More efficient way of working, less room for error
- Supporting any future changes to service
- Reduction in the time/cost of copying documents
- Easier transfer of information
- Ability to respond more quickly to information requests

Training

3.43 A clear communication plan and a training plan will be required for all staff at LBB to cover all aspects of GDPR. It is recommended that additional training resources and a budget of £30k be allocated to ensure that training is delivered and continually refreshed periodically throughout the organisation to keep staff updated.

Data Protection Officer

3.44 Article 37 states that all Local Authorities must appoint a Data Protection Officer (DPO). The main tasks of the DPO are provided within Article 39 and a cost of £70k per annum is anticipated should the responsibility not be allocated to an existing member of staff. A report will be brought back to Members with the outcome.

3.45 Article 37 of the GDPR also states that the person who is appointed into the role of the DPO must be designated on the basis of their professional qualities; in particular they will require expert knowledge of data protection law and practices and the tasks of the DPO cannot be delegated to a junior member of staff.

3.46 Article 38 also states that the Council must support the DPO in performing their tasks by providing resources necessary to carry out their tasks and to maintain their expert knowledge. Failure to provide an adequate budget could be classed as a breach of the Regulations.

3.47 Article 38 also explains that the role of the DPO contains protected Characteristics, it outlines that the DPO must be allowed to act independently of the Council and should not receive instructions from their employer on how they are to discharge their statutory functions. The DPO cannot be dismissed or penalized by the Council for performing these tasks.

4. POLICY IMPLICATIONS

4.1 This report supports BBB and Corporate Governance policies which invest in technology to enable greater flexible working.

5. FINANCIAL IMPLICATIONS

5.1 This report is highlighting the additional work that needs to be carried out in order to ensure that the Council is compliant with the GDPR.

5.2 Additional resources of £495k are required to carry out the one-off work to install new technology and temporary staff to develop and deliver the project in as well as £287k to cover the on-going costs for permanent staff, training and hosting services.

5.3 The table below summarises the costs between one-off and on-going, as well as the expected spend profile over the next four years: -

	One-Off £'000	On-Going £'000	2017/18 £'000	2018/19 £'000	2019/20 £'000	2020/21 £'000
Permamnent staffing (2 FTEs)	0	117	30	117	117	117
Temporary staffing (3FTEs)	171	0	28	114	29	0
Legal staffing (1FTE)	69	0	17	52	0	0
Training	0	30	8	30	30	30
Information strategy & framew ork	55	0	55	0	0	0
Security Information & Managemt system	90	50	90	50	50	50
HR System	110	90	110	90	90	90
Total	**495**	**287**	**338**	**453**	**316**	**287**

5.4 Approval is sought to drawdown funding from the underspend in the 2017/18 Central Contingency for the one-off costs of £495k and growth of £287k s required to meet the on-going costs, as profiled in the above table.

5.5 A future report will be brought back to Members with details of the allocation of the DPO role.

6. LEGAL IMPLICATIONS

6.1 The GDPR is due to come into force on 25 May 2018. The Government will repeal the Data Protection Act 1998 and replace it with a new Act which will set new standards for protection of general data in accordance with the GDPR.

6.2 Compliance with the GDPR and the new Act will be a statutory obligation on the Council. Non-compliance will lead to significant fines and reputational damage. It is necessary to put in place appropriate measures to ensure compliance with the Councils statutory obligations.

7. PERSONNEL IMPLICATIONS

7.1 As part of the introduction of the new GDPR regulations a review of existing contracts of employment and HR policies and procedures will need to be undertaken to ascertain whether or not existing contractual arrangements provides sufficient and necessary employee consents to allow the Council to process their personal data. Documentation relating to the processing of employee personal data may need to be amended if it is identified that this is not the case.

7.2. The newly created posts would be subject to job evaluation through the Council's agreed job evaluation processes. New posts would be advertised through the Council's normal recruitment processes, initially giving priority to any redeployees at risk elsewhere in the Council. In the case of the 4 temporary positions, they will either be filled on the basis of fixed-term contracts, or via Adecco, the Council's provider of agency workers. Existing staff within the Information Management team will be assimilated in to the redesignated roles of Information Governance Officer (IGO) and Information Management Officer (IMO).

Non-Applicable Sections:	
Background Documents: (Access via Contact Officer)	

Appendix 1 – Key Changes

1. Key Principles

1.1 The GDPR updates and enhances controls on the processing of personal data. This includes any information relating to an identified or identifiable natural person. The definition is wide and covers someone who can be identified directly or indirectly in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, psychological, genetic, mental, economic cultural or social identity of that natural person. This means that under GDPR an IP address can be personal data.

1.2 Personal data can only be lawfully processed in accordance with the provisions of the GDPR. Processing means: "any operation or set of operations which is performed on personal data -whether or not by automated means , such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use , disclosure by transmission, dissemination or otherwise making available, alignment or combination." restriction, erasure or destruction".

2. Key Changes in the GDPR

Accountability and Governance:

2.1 GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. While the principles of accountability and transparency have previously been implicit requirements of data protection law, GDPR makes them explicit and the new accountability principle in Article 5(2) requires the Council to demonstrate that we comply with the principles and put in place a comprehensive range of enhanced governance measures.

2.1 As a consequence the Council must implement appropriate technical and organisational measures that ensure and demonstrate that we comply with Article 5. This will include the creation of several internal data protection policies, increased staff training, internal audits of processing activities, and reviews of internal policies e.g. HR policies. Relevant documentation must be maintained which we will be required to make available to the relevant supervisory authorities for investigatory purposes.

Data protection by design and data protection by default:

2.2 Under GDPR the Council has an obligation to implement technical and organisational measures to prove that the Council has considered and integrated data protection into our processing activities. We will be required to ensure and demonstrate that privacy and data protection is a key consideration in the early stages of any project which includes the following:

- building new IT systems for storing or accessing personal data;
- developing, policy or strategies that have privacy implications;
- embarking on a data sharing initiative; or

- using data for new purposes.

Data Protection Impact Assessments:

2.3 Article 35 requires a Data Protection Impact Assessment to be undertaken in order to identify the most effective way to comply with the data protection obligations and meet individuals' expectations of privacy. A Data Protection Impact Assessment will outline the description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the Council. It will evaluate the necessity and proportionality of the processing in relation to the purpose. It will assess and establish potential risks to individuals and allow the Council to put measures in place in order to limit any risks by increasing the security of the data thus demonstrating that the Council is complying with the Regulations. The DPO, will be responsible for overseeing this process.

Privacy Notices:

2.4 GDPR places an obligation on the Council to provide individuals with fair processing information in the form of a privacy notice. The current data protection provisions require the Council to inform individuals of our processing activities."

2.5 GDPR takes this further and emphasises the need for transparency over how we use personal data. GDPR sets out the information that the Council must supply and when individuals should be informed.

2.6 Specific information we must provide under GDPR includes:

- The identity and contact details of the controller and where applicable, the controller's representative) and the data protection officer
- Purpose of the processing and the legal basis for the processing
- The legitimate interests of the controller or third party, where applicable
- Categories of personal data
- Any recipient or categories of recipients of the personal data
- Details of transfers to third country and safeguards
- Retention period or criteria used to determine the retention period
- The existence of each of data subject's rights
- The right to withdraw consent at any time, where relevant
- The right to lodge a complaint with a supervisory authority
- The source the personal data originates from and whether it came from publicly accessible sources
- Whether the provision of personal data collected or held is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data.
- The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.

2.7 GDPR also requires further information to be placed within our privacy notices about the processing of personal data which must be:

- Concise, transparent, intelligible and easily accessible;
- Written in clear and plain language, particularly if addressed to a child; and
- Free of charge.

2.8 All current privacy notices will need to be reviewed and where necessary, to satisfy the conditions set out under Articles 12 and 13 of GDPR.

2.9 Work will be needed to identify any services that are currently processing personal information without appropriate privacy notices in place. This process must be documented in order to demonstrate compliance with Articles 12 and 13. The DPO will take the lead role in this area.

Records of processing activities:

2.10 In order to ensure that the Council can demonstrate that we are complying with the GDPR we must document our processing activities. This will primarily be set out within our obligation to provide comprehensive, clear and transparent privacy policies. However we must also maintain additional internal records of our processing activities. It is therefore essential that data protection audits are carried out across the Council on at least an annual basis in order to ensure we are complying with and continue to comply with GDPR.

2.11 The DPO will take the lead role in conducting these audits, liaising with the Council's Internal Audit Department when required.

A change in how we obtain consent:

2.12 The GDPR has references to both 'consent' and 'explicit consent'. The difference between the two is not clear given that both forms of consent have to be freely given, specific, informed and an unambiguous indication of the individual's wishes.

2.13 Consent under GDPR requires some form of clear affirmative action. Silence, pre-ticked boxes or inactivity will not constitute consent. A record must be kept of how and when consent was given. Individuals have a right to withdraw consent at any time and work is underway to review consent mechanisms to ensure they meet the standards required under the legislation.

New rights for individuals:

2.14 The GDPR creates some new rights for individuals and strengthens some of the rights that currently exist under the DPA. The time limits for a response have changed. The Council will have less time to comply with a data request under the GDPR. Under Article 14 of the GDPR information must be provided without delay and at the latest within one month of receipt. Currently the Council has 40 calendar days to respond to a request from receipt of the fee. GDPR removes the £10 statutory fee for providing information.

2.15 GDPR introduces a new best practice recommendation that where possible the Council should be able to provide remote access to requests for personal data through a secure self –service system.

2.16 Key rights include:

- **The right to be informed**
  This encompasses our obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how we use personal data.

.

- **The right of access**
  Under the GDPR, individuals will have the right to obtain:
  - confirmation that their data is being processed;
  - access to their personal data; and
  - Other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.

- **The right to erasure:**
  The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued retention or processing.

- **The right to restrict processing**:
  Under the DPA, individuals have a right to 'block' or suppress processing of personal data. The restriction of processing under the GDPR is similar. When processing is restricted, the Council will be able to store the personal data but will not be able to process (use) it further.

.

- **The right to rectification**:
  Individuals are currently entitled to have errors in their personal data rectified if it is inaccurate or incomplete under the DPA. However the GDPR states that if we have disclosed the personal data in question to third parties, we must inform them of the rectification where possible. We must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

- **The right to data portability**:
  The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows individuals to move copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

- **The right to object:**
  Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

This will mean that the Council will have to implement policies and procedures to ensure that where we are processing data for the purposes listed above, individuals are given the opportunity to object and there are means for us to withdraw their data if they decide to object.

- **Rights in relation to automated decision making and profiling:**
  The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. These rights work in a similar way to existing rights under the DPA. The Council will need to carry out a review of all our ICT systems in order to identify whether any of our processing operations constitute automated decision making. Once we have established what systems are making automated decisions we will be required to update our procedures to deal with the requirements of the GDPR.

- **New rights for children:**
  The GDPR contains new provisions intended to enhance the protection of children's personal information. Where services are offered directly to a child, the Council must ensure that our privacy notice, and any other documentation we produce relating to these types of processing activities are written in a clear, plain way that a child will understand. If the Council offers an online service to children, we will need to obtain explicit consent from a parent or guardian to process the child's data. This particular element of the GDPR may impact children's social services or education services. A review of our online presence will need to be carried out to ensure we are compliant.

  The GDPR states that parental/guardian consent for access to online services is required for children aged 16 and under (presently it is 13 and under in the UK). Online Services includes most internet services provided at the user's request. The GDPR emphasises a high level of protection where children's personal information is used for the purposes of marketing and creating online profiles.

  Parental/guardian consent is not required where the processing is related to preventative or counselling services offered directly to a child.

Existing and new contractual arrangements:

3.17 All existing contractual arrangements which involve third parties processing the Council's data, must be reviewed. Recent work on the contracts register will support this.

3.18 Under GDPR specific legal obligations are placed upon Data processors, where the contractor holds and processes data on behalf of the Council (The Data Controller).

3.19 Under Article 28 GDPR Contracts must stipulate that the data processor will:

- Process only on documented instructions
- Ensure those processing personal data are under a confidentiality obligation
- Take all measures required by Article 32 GDPR to ensure a level of security appropriate to risk.
- Only use sub-processors with controller's consent
- Assist the controller in responding to requests
- Assist the controller in complying with obligations relating to security, breach notification, impact assessments and consulting with supervisory authorities
- Delete or return all personal data at the end of the agreement
- Make available to the controller all information necessary to demonstrate compliance; allow and contribute to audits, and inform the controller if its instructions breach the law.

3.20 In addition to updating the data protection clauses in contracts, other agreements, such as database access agreements, data processing agreements, data disclosure agreements and also the information sharing protocols will need to be re-negotiated in order for them to comply with Article 28.

Breach notification:

3.21 There is at present no general duty to report information breaches to the Information Commissioner. GDPR changes this and introduces a legal duty to report the majority of breaches in 72 hours. Where the breach puts the data subject at a high risk, the Council is obliged to tell the subject(s) directly about the breach and advise them as to what actions have, and, are to be taken as a result.

3.22 The most significant consequence is that of the fines. A Data Breach and failure to notify the ICO and subject within the stated time scales can result in a Tier 1 maximum fine of around £8.9m.

3.23 The Council must therefore review and strengthen its current breach notification policies and disseminate this information to all staff and members.

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.

Appendix 3 - Action to Ensure Compliance.

1. GDPR Working groups and Project plan

1.1 Taking the 51 recommendations set out by the Data Protection People, a project plan has been created expanding on the recommendations and creating actionable tasks. These recommendations and tasks are organisation wide and in an attempt to get departments to adopt ownership of their own data working groups have been created in the following areas:

Adults Social Care	Children's Social Care
Public Health	Housing
Education	Finance
Planning	Environment
Regeneration	HR
Corporate Services	Commissioning & Procurement

1.2 Each group meets with the Principal Information Assurance Officer on a 4-6 week basis to review the pending legislation that will be replacing the DPA, to have and understanding and opinion of the roadmap and communications plan and to identify and understand whether, and how, corporate policy might change.

The objectives of the working groups are:

- Agree action plan and milestones on GDPR Toolkit
- To make further recommendations to the organisation for necessary policy changes and identify gaps
- Discuss the GDPR action plan and designate group members to foster ownership and help achieve specific tasks
- Increase awareness and communications across the department
- Discuss and plan communications service users
- Discuss any outstanding action points from previous meetings;
- Discuss any near misses or breaches which may have occurred in the past month and their impact if occurred post May 2018;
- Ensure the changes are imbedded and implemented post go live

Work Streams in Practice

1.3 Of the recommendations there is a clear distinction between actions that need to be taken by the Information management team; writing policies, providing a robust training framework, ensuring that the technology provided can support the business and keeping up a momentum of communications, awareness and good practice.

1.4 Actions required to be driven and supported closely by Information Management are:

- Privacy impact Assessments
- Information Sharing Agreements

- Touchpoint Disclaimers
- Process mapping
- Identification of legal basis for processing and sharing
- Aligning processes with the individual's rights
- Completing training
- Understanding of the Breaches and notification

Supplier and Third party processor engagement

1.5 Key to the success of being compliant with the GDPR and ensuring that our applications and systems support our processing practices for Information Governance and Security is the level of engagement with our suppliers and processors (those hosting our data on their infrastructure).

1.6 As part of the GDPR working group, we will be contacting current as well as potential suppliers and inviting them to provide a statement of intent on their bid to also be ready and provide a product that is compliant with the GDPR. This will challenge their development and gain valuable insights that will help us partner with responsible and competent partners.

1.7 Similar to supplier engagement, any business area that outsources/commissions another organisation to carry out data collection and/or processing on our behalf must be able to demonstrate a level of commitment to the change in law.

1.8 As Data owners, and in most instances, controllers we have a requirement to be diligent and specific as to how our third party processors handle data on our behalf. The significant issues of the law will be addressed by the contract managers and Principal Information Assurance officer and form part of the contract monitoring framework.

1.9 Challenging our supplier and third party development will help us gain valuable insights that will enable us to partner with responsible and competent associates, feeding into the requirement or privacy by design and privacy by default mandated by the law.

Commissioning, Procurement & Contract Monitoring

1.10 Work has been identified and started to provide an end-to-end process for commissioning and procurement that creates a symbiotic relationship between the business areas and information security and governance.

- Use of Privacy impact assessments at the business requirement stage
- Gateway evaluation questions
- Variations to existing contract
- Future proofed clauses for new contracts
- KPI's and monitoring framework

Legal Support

1.11 The legal division plays a crucial role in supporting the organisation towards compliance. Assisting in creating sharing agreements, disclaimers, identification of legal entities and legal basis for processing. This will ensure our business areas stand up to the necessary litmus tests to ensure the processes are aligned.

Training

1.12 Training and Awareness is an essential component of keeping the Council operating in a safe and legal manor. We currently have an Information Governance Training module on the InfoAware platform that we encourage officers to conduct every 2 years.

1.13 To comfortably meet the requirements of the new law we are seeking to add 6 modules to the portal for all officers to complete in a rolling 2 years cycle interspersed with policy acceptance. This will allow us to demonstrate by means of reports that our network users have received a comprehensive training package that has been backed-up by our policies and procedures. Beyond these Council-wide modules we have a need to provide role specific training for areas such as social work, contract managers and commissioners and Subject Access Request (SARs) coordinators.

SARS

1.14 The Council has a devolved approach to handling Subject Access and Freedom of Information requests with Individual departments. The role of coordinating and replying to them has been assigned to an existing post.

1.15 The bulk of the annual requests across the Council are concentrated in Adult's and Children's social care, handling on average 45 and 39 requests respectively. With confidence we can assert that all requests pertaining to adults are being met within the current timescales mandated by the data protection act.

1.16 An area of concern is that Children's requests are not being wholly met under the current parameters. This is due to the retrieval of boxes from TNT having an associated cost and time constraint, printing time is a constraint due to volume and there is no dedicated resource for redaction.

1.17 Under the GDPR the timescale for reply shorted from 40 calendar days to 30. We can no longer charge for requests unless deemed unnecessary or repetitive and we have to provide information on how long we keep the files for, with evidence of our retention policy. There is speculation that Subject Access Requests along with the additional rights of the individual and ability to claim compensation from the organisation could mean a significant uplift in requests with the top tier of fines being reserved for this type of failure.

Schools Awareness Program

1.18 The Council is embarking on a Schools awareness program which aims to give the relevant accountable personnel encouragement priorities and plan for an assured route to compliance without alleviating their responsibility.

1.19 The Principal Information Assurance Office is attending the School's Forum for Primary, Secondary and Special schools to present in the next half term. Present will be Head Teachers and an invitation will be extended to Data Protection Officers if required by larger schools, federations and multi academy trusts..

1.20 To support this contact, communications will be included in the schools bulletin and the Council will be compelling the schools to engage with their supplier and third party processors as an act of due diligence.

Appendix 4 - Policies

Current Policies Reviewed

Policy Name	Target Draft Completion Date	Target Review Date
iPad and Tablet policy	July 2017	August 2017
Incident Reporting Policy	July 2017	August 2017
Information Sharing Policy	September 2017	October 2017
Remote Working Policy	October 2017	November 2017

Current Policies Work in Progress

Policy Name	Target Draft Completion Date	Target Review Date
Infrastructure Policy	October 2017	November 2017
Data Protection and Confidentiality	October 2017	November 2017
Information Security Policy	October 2017	November 2017
Network Access Policy	October 2017	November 2017
Remote Working Policy	October 2017	November 2017
Subject Access request Policy	October 2017	November 2017

Policies to be Reviewed

Policy Name	Target Draft Completion Date	Target Review Date
Privacy Policy/Notice	October 2017	December 2017
Acceptable Use Policy for Internet & Email	November 2017	December 2017
Communications Policy	November 2017	December 2017
Data Quality Policy	November 2017	December 2017
Information Classification Scheme and Handling	November 2017 November 2017	December 2017
Information Governance Management Framework	November 2017	December 2017

Clear Desk & Screen Policy	November 2017	December 2017
Information Governance Policy	November 2017	December 2017
Network Account Password Policy	November 2017	December 2017

Required Policies

Policy Name	Target Draft Completion Date	Target Review Date
Anonymisation Policy	January 2018	February 2018
Data transfer policy	January 2018	February 2018
Secure Email policy	January 2018	February 2018
Privacy Impact Assessment Policy	January 2018	February 2018
Redaction Policy	January 2018	February 2018
Anonymisation/Pseudonymisation Policy	January 2018	February 2018
Scanning and Digitisation Policy	January 2018	February 2018
Laptop Policy	January 2018	February 2018
Mobile Phone Policy	January 2018	February 2018
Records Management policy	January 2018	February 2018
Social Media Policy	January 2018	February 2018
Paper Records – Secure handling and transit policy	January 2018	February 2018
FOI Policy	January 2018	February 2018

Appendix 5 - High Level Role for Information Team

1. **Head of Information/CISO (Chief Information Security Officer)**

- GDPR Compliance Program management
- PSN, PCI DSS, N3 Compliance Lead
- Commission/Write Strategy Information Strategy
- Commercial Management
- Information Programme Management
- Management and delivery of Information Security, Governance and Management Programme
- Attend Board level meetings and consult services on Information Security, Governance and Management
- Key Stake Holder Communications
- Information Security, Governance and Management Road Map

2. **Information Assurance (Governance & Security)**

- Ensure effective framework of IA policies and procedures for Bromley and 3rd Parties
- Ensure compliance with standards: LPSN, GCSx, N3, ISO27001
- Arrange and manage technical audit measures – pen testing, vulnerability scanning
- Create and review IA Policies
- Manage and resolve security incidents
- Audit outsourced providers to ensure compliance
- Give presentations to councillors and senior officers on Information Assurance
- Develop and manage IA and IG training
- Information governance management
- Advice the council on DPA and GDPR best practices and procedures

3. **Information Architect & Analyst**

- SharePoint architecture
- Develop a robust audit framework for reviewing Council data management and quality,
- Support system / process managers in the creation of privacy and information risk/impact assessments.
- To work with heads of service to ensure that information audits are carried out on a regular basis and meet the LBB polices criteria.
- Build and maintain the Information Asset Register.
- Information Management integration within lifecycle of all line of business systems and processes.
- Develop data retention policies

4. **Support Officer**

- To support the Principal Information Assurance Officer in the management, resolution, and effective reporting of Information Security Incidents
- Managing/updating ISD project pages, UATing out of hours
- Information Asset Register Project Support
- Information Asset Training coordination and support
- GDPR Project coordination and Support for IA Officer
- Provide project support and work with ISD System Managers and Inform Consult to develop the new SharePoint Online architecture.
- Provide updates to Information Subgroup and IT Training Steering Group on work streams
- Supporting staff with ISD project changes e.g. Citrix help desk queries, SharePoint architecture changes, Monitoring project mailboxes etc
- Engage with Consultants and 3rd party's and gather quotes/raise work when needed

This page is left intentionally blank