Statement of Compliance
Data Protection

May 2018
London Borough of Tower Hamlets

Information Governance is everyone's business

VERSION CONTROL

Version	Date	Author	Description
0	March 2018	Enterprise Architect	*Initial draft created*
0.1	April 2018	Enterprise Architect Service Manager IG	*Document amended to include more detail of preparatory work.*
1	May 2018	Enterprise Architect Service Manager IG	*First full version – draft*

Approved by
Corporate Director of Governance

Date

TABLE OF CONTENTS

1 Summary

The London Borough of Tower Hamlets (LBTH) *('we' or 'us' or 'our')* are committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection. We have always had a robust and effective data protection program in place which complies with existing law and abides by the data protection principles. However, we recognise our obligations in updating and expanding this program to meet the demands of the GDPR and the UK's Data Protection Bill.

It should be read in conjunction with the Policies guidance and procedures in the Information Governance Framework.

2 Context

The EU General Data Protection Regulation (GDPR) came into force across the European Union on 25 May 2018 bringing with it the most significant changes to data protection law in two decades. Based on privacy by design and taking a risk-based approach, the GDPR has been designed to meet the requirements of the digital age.

The 21st century brings with it broader use of technology, new definitions of what constitutes personal data, and a vast increase in cross-border processing. The new Regulation aims to standardise data protection laws and processing across the EU; affording individuals stronger, more consistent rights to access and control their personal information.

We are dedicated to safeguarding the personal information under our remit and in developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for the new Regulation. Our preparation and objectives for GDPR compliance have been summarised in this statement and include the development and implementation of new data protection roles, policies, procedures, controls and measures to ensure maximum and ongoing compliance.

3 How we have prepared for the GDPR

We have a consistent level of data protection and security embedded within our organisation. It is our aim to be compliant with the GDPR with specific action plans for the areas requiring further development, which are set out in Appendix 1. The action plan will be updated in the compliance with the Data Protection Bill once the final version is published.

3.1 Policies and procedures

Our preparation includes: -

- ***Information Audit*** - Carrying out a council-wide information audit to identify and assess what personal information we hold, where it comes from, how and why it is processed and if and to whom it is disclosed.

- ***Policies & Procedures –*** Revising existing and, where required, implementing new data protection policies and procedures to meet the requirements and standards of the GDPR and any relevant data protection laws, including: -

    - ***Data Protection*** – Our main policy and procedure document for data protection has been overhauled to meet the standards and requirements of the GDPR. Accountability and governance measures are in place to ensure that we understand and adequately disseminate and evidence our obligations and responsibilities; with a dedicated focus on privacy by design and the rights of individuals.

    - ***Data Retention and Disposal*** – The Retention and Disposal Schedules have been updated to ensure that we meet the *'data minimisation'* and *'storage limitation'* principles and that personal information is stored, archived and destroyed compliantly and ethically. We have dedicated erasure procedures in place to meet the new *'Right to Erasure'* obligation. See https://www.towerhamlets.gov.uk/lgnl/council_and_democracy/data_protection__freedom_of/GDPR/Data_Subject_Rights.aspx

    - ***Data Breaches*** – Our data security incident procedures ensure that we have safeguards and measures in place to identify, assess, investigate and report any personal data breach. Our procedures are robust and disseminated to all employees, making them aware of the reporting lines and steps to follow.

    - ***International Data Transfers and Third-Party Disclosures*** – We have robust procedures and safeguarding measures in place to secure, encrypt and maintain the integrity of the data. None of our data is stored outside of the EU. Our procedures include a continual review of the countries with sufficient adequacy decisions, as well as provisions for binding corporate rules; standard data protection clauses or approved codes of conduct for those countries without. We carry out strict due diligence checks with all recipients of personal data to assess and verify that they have appropriate safeguards in place to protect the information, ensure enforceable data subject rights and have effective legal remedies for data subjects where applicable.

    - ***Subject Access Request (SAR)*** – Our SAR procedures accommodate the revised 30-day timeframe for providing the requested information and for making this provision free of charge. Our procedures detail how to verify the data subject, what steps to take for processing an access request, what exemptions apply and a suite of response templates to ensure that communications with data subjects are compliant, consistent and adequate. See https://www.towerhamlets.gov.uk/lgnl/council_and_democracy/data_protection__freedom_of/data_protection_act.aspx

- ***Legal Basis for Processing*** - we have reviewed all processing activities to identify the legal basis for processing and ensuring that each basis is appropriate for the activity it relates to. Where applicable, we maintain records of our processing activities, ensuring that our obligations under Article 30 of the GDPR and Schedule 1 of the Data Protection Bill are met.

- ***Privacy Notice/Policy*** – we have revised our Privacy Notices to comply with the GDPR, ensuring that all individuals whose personal information we process are informed of why we need it, how it is used, what their rights are, and who the information is disclosed to. See *https://www.towerhamlets.gov.uk/content_pages/legal_notices/legal_notices.aspx*

- ***Obtaining Consent*** – Whilst as a public body we have few data processes depending on Consent as a condition for processing, we have revised our consent mechanisms for obtaining personal data, ensuring that individuals understand what they are providing, why and how we use it and giving clear, defined ways to consent to us processing their information. We have developed processes for recording consent, making sure that we can evidence an affirmative opt-in, along with time and date records; and an easy to see and access way to withdraw consent at any time.

- ***Direct Marketing*** - The wording and processes for direct marketing has been revised, including clear opt-in mechanisms for marketing subscriptions; a clear notice and method for opting out and providing unsubscribe features on all subsequent marketing materials.

- ***Privacy Impact Assessments (PIA)*** – Procedures are in place for processing personal information which is considered high risk, involves large scale processing or includes special category/criminal conviction data in compliance with GDPR, Article 35 requirements. We have implemented processes that record each assessment, allow us to rate the risk posed by the processing activity and implement mitigating measures to reduce the risk posed to the data subject(s).

- ***Processor Agreements, Contact Clauses*** – Any third-party processing personal information on our behalf (*i.e. Payroll, Recruitment, Hosting etc.*), must comply with the Processor Agreements. Procedures are in place for ensuring that they (*as well as we*), meet and understand their/our GDPR obligations. These measures include initial and ongoing reviews of the service provided, the necessity of the processing activity, the technical and organisational measures in place and compliance with the GDPR.

- ***Special Categories Data –*** Is undertaken in compliance with the Article 9 requirements and have high-level encryptions and protections on all such data. Special category data is only processed where necessary and is only processed where we have first identified the appropriate Article 9(2) basis or the Data Protection Bill Schedule 1 condition. Where we rely on consent for processing, this is explicit and is verified by a signature, with the right to

modify or remove consent being clearly signposted. The same measures, documentation and protection will be applied to data concerning crime when the Data Protection Bill is published.

3.2 Data Subject Rights

In addition to our current policies and procedures mentioned, we provide easy to access information via our internal and external website to ensure individuals can enforce their data protection rights. Individuals have the right to access any personal information that we process about them and to request information about:

- What personal data we hold about them
- The purposes of the processing
- The categories of personal data concerned
- The recipients to whom the personal data has/will be disclosed
- How long we intend to store your personal data for
- If we did not collect the data directly from them, information about the source
- The right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this
- The right to request erasure of personal data (*where applicable*) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making that we use
- The right to lodge a complaint or seek judicial remedy and who to contact in such instances

3.3 Information Security and Technical and Organisational Measures

We take the privacy and security of individuals and their personal information very seriously and take every reasonable measure and precaution to protect and secure the personal data that we process. We have robust information security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction and have several layers of security measures, including: -

- **Physical Security**
  - ✓ Locked offices
  - ✓ Swipe cards for access, allocated to named people
  - ✓ Access is tracked on a per fob/user basis
  - ✓ Named key holders and alarm pin holders
  - ✓ CCTV cameras outside key buildings
  - ✓ Locked drawers and cupboards
  - ✓ Visitors are escorted
  - ✓ Servers are kept in lockable cabinets inside a dedicated locked server room within a secure building.
  - ✓ Clear desk policies

- **Electronic Security**
  - ✓ Antivirus and security updates are managed and updated centrally for servers, workstations, laptops and thin client users.
  - ✓ Data/security controls are monitored by the built in Intrusion Detection and Prevention Systems (IDS/IDP) within our security firewall
  - ✓ Two factor authentication is required for login to access network resources.
  - ✓ USB ports are disabled by default, and encrypted USB Sticks are used for mobile use.
  - ✓ Laptops data storage discs are encrypted with Bitlocker encryption.
  - ✓ Clear desk policies

- **Mobile Devices**
  - ✓ Company provided laptops
  - ✓ Encrypted
  - ✓ Two factor authentication required to login.
  - ✓ Maas360 on mobile devices
    - Encrypted communication
    - Additional layer of security with 6 digit pin.

- **Print & Scanning**
  - ✓ Only print to secure devices in offices
  - ✓ All users need to login to print.
  - ✓ Additional building entry card swipe on printer required to enable printing.

- **Back Up Procedures**
  - ✓ Backup of data is completed utilising a local system recovery snapshot technology to NAS storage.
  - ✓ Offsite backup is to a service provider datacentre via a secure and resilient gigabit connection.
  - ✓ Backup is undertaken nightly via the differential methodology, with x5 revisions of a file.
  - ✓ Restore procedures are undertaken on demand and actioned upon request of nominated authorised personnel.
  - ✓ Data destruction requirements are conformed to via the backup data being transferred to a Backup Lifecycle Management system and then purged.

- **Disaster Recovery**
  - ✓ We aim to have tier 1 systems back online within 5 days from system backup copies.
  - ✓ Additional server capacity to accommodate disaster recovery (DR) of tier 1 application is provided by third party contracted DR service provider.

- **Data Destruction**
  - ✓ Policy:
    - Records Management Policy,
    - Retention & Deletion Schedules,
    - Data Disposal Guidance
  - ✓ Periodic destruction activity for each software system, as regular housekeeping. Frequency determined by the type of system.
  - ✓ Planned regular review of locally held shared data and personal storage

- ✓ Email archive / leavers deletion procedure
- ✓ Physical Off-Site Storage contract procedure
- ✓ Confidential waste system completed via secure 3rd party
- ✓ Certificate provided for electronic and hard copy paper files. Approved via Information Asset Owner

- **Policies**
  - ✓ Data Protection Policy
  - ✓ Acceptable Use Policy
  - ✓ Information Security Policy
  - ✓ Information Handling Procedure
  - ✓ HR terms and conditions - Confidentiality and Code of Conduct

- **Continuous Improvement Culture**
  - ✓ Keep abreast of new technology, standards and legislation to monitor and improve processes

3.4 GDPR Roles and Employees

We have designated the Information Governance and Complaints & Information Head of Service as our Data Protection Officer (DPO) until the designated, independent role is recruited to and have a working group appointed to develop and implement our roadmap for complying with the new data protection Regulation. The team are responsible for promoting awareness of the GDPR across the organisation, assessing our GDPR readiness, identifying any gap areas and implementing the new policies, procedures and measures.

This Group is led by the Service Manager – Complaints and Information, and feeds into the existing corporate Information Governance structures and reporting mechanisms, including the multi-disciplinary Information Governance Group and Corporate Information Governance Board.

Continuous employee awareness and understanding is vital to the continued compliance of the GDPR and have involved our employees in our preparation plans. We have an employee training program specific to the GDPR which has provided face to face training, and forms part of our induction and annual training program.

An internet page with advice has been developed and a programme of staff awareness has been run through our internal communications newsletters and updates.

Further details on our compliance and improvement plan are contained in Appendix A.

4. REVIEW/ SIGN OFF

The compliance statement agreed May 2018 will be reviewed annually or sooner if required, and signed off by the Corporate Information Governance Board, and owned by the SIRO.

Appendix 1 – Information Governance Statement of Compliance
May 2018

Next Review Date – November 2018

Requirement	Position Statement	Action Plan	Time Frame	Lead
• Technical and organisational security measures to protect against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, the personal data in order to comply with the data protection principles;	The Council undertakes a variety of measures to keep data safe and secure including: **Physical Security:** • Locked Office • Swipe cards for Access - Allocated to named people - Access is tracked on a per fob/user basis • Named key holders and alarm pin holders • CCTV cameras outside key buildings • Locked drawers and cupboards • Visitors are escorted • Servers are kept in lockable cabinets inside a dedicated locked server room within a secure building. • Clear desk policies **Electronic Security:** • Antivirus and security updates are managed and updated centrally for servers, workstations, laptops and thin client users.	Monitoring and auditing Plan to procure Security Information and Event Management (SIEM) system.	• At least annually, otherwise at client request or when new legislation is published 2018	

	• Data/security controls are monitored by the built in Intrusion Detection and Prevention Systems (IDS/IDP) within our security firewall • Two factor authentication is required for login to access network resources. • USB ports are disabled by default, and encrypted USB sticks are used for mobile use. • Laptops data storage discs are encrypted with Bitlocker encryption. • Clear desk policies **Mobile Devices** • Company provided laptops - Encrypted - 2 factor authentication required to login. • Maas360 on mobile devices - Encrypted communication - Additional layer of security with 6 digit pin. **Print & Scanning** • Only print to secure devices in offices • All users need to login to print. • Additional building entry card swipe on printer required to enable printing. • Securely wiped before removal			

	Back Up Procedures: • Backup of data is completed utilising a local system recovery snapshot technology to NAS storage. • Offsite backup is to a service provider datacentre via a secure and resilient gigabit connection. • Backup is undertaken nightly via the differential methodology, with x5 revisions of a file. • Restore procedures are undertaken on demand and actioned upon request of nominated authorised personnel. • Data destruction requirements are conformed to via the backup data being transferred to a backup lifecycle Management system and then purged. **Disaster Recovery:** • We aim to have tier 1 systems back online within 5 days from system backup copies. • Additional server capacity to accommodate DR of tier1 application is provided by third party contracted DR service provider. **Data Destruction:** • Policy: - Records Management Policy, - Retention & Deletion Schedules, - Data Disposal Guidance • Periodic destruction activity for each software system, as regular housekeeping. Frequency determined by the type of system.	Policies in place Electronic Data Discovery and Deletion Programme running May 2018 to May 2019	May 2018 to May 2019	DD ICT, Head of IG

	• Planned regular review of locally held shared data and personal storage • Email archive / leavers deletion procedure • Physical off-site storage contract procedure • Confidential waste system completed via secure 3rd party • Certificate provided for electronic and hard copy paper files • Approved via Information Asset Owner **Policies:** - Data Protection Policy - Acceptable Use Policy - Information Security Policy - Information Handling Procedure - HR terms and conditions - Confidentiality and Code of Conduct **Continuous Improvement** • Keep abreast of new technology, standards and legislation to monitor and improve processes	Lead by DPO, Head of Information Governance, Information Governance Group lead officers, Head of ICT Security, etc		
• Staff awareness, training	• Induction / enrolment • Metacompliance enforces mandatory training - Information Governance Framework Policies - Data Protection - Information Security • Regular Comms messages to all staff • Regular briefings to senior managers • Face to face training sessions • Web-based annual training	• Monitoring & Auditing • Detailed Privacy Notice for all New Starters • Provide names of trained staff to DLTs to review knowledge base	• At least Annually or as Required • Ongoing	Head of IG

• Fair Lawful and Transparent	• Records of processing held centrally • Privacy Notice (PN) recorded centrally • Information Asset Register (IAR) held centrally, reviewed locally • Privacy Impact Assessment (PIA) embedded in process initiation • Review of 'crime' data on publication of Data Protection Bill	• Moved IAR to automated system April 2018, which holds PN and DSA • Review and update central record and IAR	• Annual review • June to September 2018	
• Purpose limitation Not use the personal data for any purposes which are inconsistent with the purposes	• Annual review of IAR an data process mapping	• Sign and agree Contract and working instructions with Council	• Prior to contract start	
• Data accuracy and minimisation	• Policy on maintaining and checking accuracy, • Determine minimum necessary for purpose • Pseudonymisation	• Data Quality • PIA • DSAs		
• Data Retention and Disposal -Paper records	• Internal processes and processes integrated in contract award and contract monitoring. • Management review system and then purged. A certificate of destruction is generated by the system for compliance purposes. • Embedded in Privacy Impact Assessment at onset to design process **Data Destruction:** • Via secure 3rd party • Certificate provided for electronic and hard copy paper files	• Review Council Policies • Update Information Asset Register • Assessment and deletion programme • Retain data Destruction Certificate	• Prior to contract start service provision • Destruction certificate provided at end of contract / retention period	

• Secure against, appropriately report on and remedy Security Breaches	• Security Incident Procedures • Record incidents, and report, including: - a recovery plan, including damage limitation; - assessing the risks associated with the breach; - informing the appropriate internal officers, ICO, and where necessary the data subjects that the breach has occurred; and - review the response and where necessary update information security measures, policies & procedures.	• Complete Form • Monitoring of procedures	• Quarterly or if incidents occur	
• Business continuity	**Business Continuity Procedures** **Back Up Procedures:** • Backup of unstructured data is completed utilising a local system recovery snapshot technology to NAS storage. • Offsite backup is to our service provider datacentre via a secure resilient gigabit connection. • Backup is undertaken nightly via the differential methodology, with x5 revisions of a file. • Restore procedures are undertaken on demand and actioned upon request of nominated authorised personnel. • Data destruction requirements are conformed to via the backup data being transferred to a backup lifecyle Management system and then purged. A certificate of destruction is generated by the system for compliance purposes.	• Monitoring and Auditing	• ongoing	

	Disaster Recovery: • Aim to have all tier 1 systems back online within 5 days from backup tapes.. • Additional server capacity to accommodate this is maintained by a third party service provider.			
• Process Data Subject Rights in accordance with legislation and keep appropriate records	• Advise data subjects of rights, through transparency, proactive publicity • Record and processing requests - Privacy Notices • Inform staff of Data subject rights and council procedures - Website and intranet with details • Keep records of requests, processing and decisions	• Sign and agree Contract and working instructions with Council	• Prior to contract start	
• Privacy by Design PIA	• Embed Privacy Impact Assessment in necessary processes - procurement, - ICT Board, - Strategy and policy - Programme Office			
• Contracts and Contract Monitoring	• Effective contract clauses and Invitation To Tender questions • Contract owners undertake monitoring and use 'what compliance/ good looks like' assessments			
• Maintain confidentiality	• Data Sharing Agreements	• Review of current position, establish action plan – in progress	• Review April to November 2018 • At least	

		• Monitoring and Auditing • Sign off sheets	Annually • As required	
• Not transfer any personal data outside of the European Economic Area unless authorised to do so in writing by the Council.	• The Council takes all reasonable steps to ensure that data is processed securely and fairly. Data will only be processed in accordance with Council working instructions. - Project initiation - Privacy Impact Assessment - Contract reviews	• Monitoring and Auditing	• Annually or as required	