DATA PROTECTION POLICY

May 2012

Version Control

Version / revision	Date	Description of changes	Reviewed/edited by
v1.1	15.05.2012	Adding new logo & reformatting	Rachael Clauson
v1.2	13.06.2012	Revisions to reflect the changes from OPLC ('the Company') to LLDC ('the Corporation')	Danny Budzak

Approvals

Approval by	Name/Department	Signed (Y/N)	Date
Author	Dionne Knight	Y	04.05.11
Executive Director	Jonathan Dutton	Y	04.05.11

DATA PROTECTION POLICY

1. INTRODUCTION

1.1 PURPOSE

The London Legacy Development Corporation (the 'Corporation') holds a significant amount of personal data, mainly belonging to staff and contractors, as well as members of the public. The Corporation aims to achieve best practice standards in managing its information, and to be compliant with information law. This policy sets out the standards the Corporation will adopt when managing personal data. This is to ensure:

- compliance with legal obligations
- adherence to best practice guidelines
- protection of our staff and the public

1.2 SCOPE

The scope of this policy applies to:

- the London Legacy Development Corporation
- all staff, contractors and volunteers working on behalf of the Corporation
- personal data in any medium that is not already in the public domain.

1.3 LEGISLATIVE FRAMEWORK, STANDARDS AND GOVERNMENT REQUIREMENTS

The effective implementation of this policy is critical to ensuring the Corporation is compliant with the legislative requirements governing personal data and privacy, namely the:

- Data Protection Act (1998)
- Human Rights Act (1998)

Compliance with the Data Protection Act is monitored by the Information Commissioner's Office (ICO), an independent authority that has the power to fine organisations and publicly issue Undertakings for non-compliance.

The following legislation, international standards and Government requirements are also applicable:

- Freedom of Information Act (2000)
- Environmental Information Regulations(1992) & Environmental Information (Amendment) Regulations(1998)
- ISO 15489 -1 and ISO 15489 -2 Information and Documentation - Records Management

- ISO 27001- Information technology - Security techniques - Information security management systems
- Data Handling Review, Cabinet Office, 2008
- Security Policy Framework, v5.0, Cabinet Office, 2011

1.4 DEFINITIONS

In this Policy, the terms listed below have the meaning ascribed to them as defined by the Data Protection Act.

Data is information which is being processed by an automated system (such as payroll) or recorded with the intention that it should be processed by such a system; or recorded as part of a relevant filing system, or is another form of recorded information held by the Corporation as a public authority.

Personal data means data which relates to a living identifiable individual. This may also include visual material, such as videos, photographs and CCTV images.

Sensitive personal data means personal data consisting of information which may include any of the following: racial or ethnic origin, political opinions, religious beliefs, membership of a trade union, physical or mental health, sexual orientation, actual or alleged criminal offence(s).

Processing data means obtaining, recording or holding the information or carrying out any operation on the information such as organisation, retrieval, disclosure or destruction.

Data subject means an individual who is the subject of personal data.

Data controller means a person who (either alone or on behalf of an organisation) determines the purposes and the manner in which personal data are processed.

1.5 DATA PROTECTION PRINCIPLES

There are eight key principles detailed in the Data Protection Act which determine how personal data must be processed.

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

    (a) at least one of the conditions in Schedule 2 is met, and
    (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up-to-date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

2. DATA PROTECTION POLICY STATEMENT

2.1 The London Legacy Development Corporation will ensure that the retention and management of personal data complies with the Data Protection Act. The Corporation recognises that there is a need to receive, process and retain personal data but acknowledges that:

- personal data will be held for legitimate business purposes only
- it will be accessible to staff members on a need to know basis only
- it will be accessible to individuals if they wish to inspect data about themselves, providing it does not breach the confidentiality of a third party
- it will not be used in a manner incompatible with the reasons for which it has been collected and is held
- at the point of collecting data, individuals will be informed of the purpose and use of that data, and consent will be acquired.

2.2 In addition, the Corporation will create and maintain an Information Asset Register detailing the personal datasets that it holds, to document the security and access controls in place and ensure that it is not retained longer than necessary. No data will be disclosed to a third party without either the employee's written consent, or where the third party has a statutory or legal authorisation to be supplied with the information. Fair processing notices and an Information Charter will ensure that the Corporation is open and transparent about the use of the personal data it holds, particularly that of the public.

2.3 The following internal policies are applicable to maintain the confidentiality, integrity and availability of the personal data that is held by the Corporation

- Information Security Policy and Incident Management Procedures
- Information and Records Management Policy
- Freedom of Information Policy and Procedures

3. KEY PERSONAL DATA RISKS

3.1 The effective management of personal data is not simply about ensuring compliance with the Data Protection Act, but about following best practice guidelines for information security, information risk management and

openness, accountability and transparency. Personal data is a particularly sensitive type of information held by the Corporation, and should be factored in our information risk management processes. The key potential risks which this policy is designed to address are:

- breach of confidentiality (information being disclosed inappropriately)
- breach of security by allowing unauthorised access
- failure to present fair processing notices and positive consent
- failure to establish efficient systems of managing changes, leading to personal data being not up-to-date.
- insufficient clarity to staff and the public about the way data is used
- ensuring the Corporation's IT service provider (currently East Thames Housing Group) complies with and supports this data protection policy.

4. ROLES AND RESPONSIBILITIES

4.1 All staff have a responsibility to ensure personal data held by the Corporation is appropriately managed. In addition the roles listed below have specific tasks.

4.2 **Executive Management Team:**

- Overall responsibility for ensuring the Corporation complies with legal obligations and this policy.

4.3 **Senior Information Risk Owner**

This role is currently fulfilled by the Director of Finance and Corporate Services. Responsibilities include:

- Designated Data Controller for the Corporation
- Oversight of implementation of appropriate controls to manage and mitigate personal data risks.

4.4 **Data Protection Officer**
This role is currently fulfilled by the Information Manager. Responsibilities include:

- Briefing the SIRO Data Protection responsibilities
- Handling subject access requests
- ICO notification
- Reviewing Data Protection Policy and Procedures
- Advising other staff on Data Protection issues
- Ensuring that Data Protection induction and training takes place
- Approving contracts with Data Processors.

4.5 **Directors/Team Managers**

Each team or department where personal data are handled are responsible for informing the Data Protection Officer of the purpose of their data collection, and of any subsequent changes, and in completing awareness training to ensure that good Data Protection practice is followed.

4.6 **All Legacy Corporation staff**

- Responsible for following policies and procedures for managing personal data
- Responsible for highlighting to the Data Protection Officer or SIRO when they believe the Act and/or this Policy may have been breached
- Responsible for forwarding any subject access requests to the Data Protection Officer to carry out.

4.7 This applies equally to temporary and agency staff, contractors and consultants, volunteers and interns.

4.8 Breaches of this policy may result in disciplinary action.

5. MONITORING

5.1 The Senior Information Risk Owner will oversee the operation of this policy and associated procedures on behalf of the Executive Management Team. Such monitoring will include a review as part of the annual information risk assessment.

DATA PROTECTION PROCEDURES

6. RESPONDING TO SUBJECT ACCESS REQUESTS

6.1 RECEIVING REQUESTS

Subject access requests must be in writing, including email. If a request is received from an individual about information the Corporation may hold about them, it must be passed to the Data Protection Officer without delay. Even if the request appears simple, or is from an existing member of staff, there are certain considerations that must be taken into account, and this must be done consistently and in compliance with Data Protection law.

6.2 Requests for information that relate to someone other than the requestor will be refused, unless such a request is covered by either the Freedom of Information Act or is made through an application to an Employment Tribunal and is covered by one of the relevant acts (e.g. sex discrimination, equal opportunities etc). See the Freedom of Information Policy and Procedures for more information.

6.3 VERIFYING IDENTITY

Where the individual making a subject access request is not known to the Data Protection Officer their identity must be verified before handing over any information. This can be done by:

- requesting sight of photographic ID (passport or driver's licence)
- receiving a witnessed signature
- checking postal address with the electoral register.

6.4 RESPONDING TO REQUESTS

Information must be provided to the requestor within 40 calendar days (not working days). If a fee is being charged then the 40 days start only after the fee has been received and payment processed.

6.5 The requested information will be provided in paper/electronic format unless the applicant makes a specific request to be given supervised access in person. Where face-to-face requests are made, the Data Protection Officer must make the information available to the applicant on Corporation premises, but they must be supervised at all times. Identity verification must take place before the individual is allowed access to the information.

6.6 CHARGING

The Corporation will charge for subject access requests (the maximum charge is £10). This must be made known to the Data Subject at the point of them making an access request.

7. OPENNESS AND ACCOUNTABILITY

7.1 OBTAINING CONSENT

In order to meet the ICO's Data Protection guidelines, the Corporation must ensure consent to hold personal data is obtained from individuals - employees, stakeholders and members of the public - if their personal details are held or processed by the Corporation in any way.

7.2 Consent must be 'positive', in that it cannot be implied simply because individuals do not object to their personal data being held or processed. The Corporation will ensure that at all entry points where personal data is collected, a 'fair processing notice' will be clearly visible and individuals will need to opt in by positively declaring their consent

7.3 All Staff, temporary contractors, consultants, volunteers, interns or any person working for the Corporation will be informed that their personal data is being processed for staff administration at the point of signing an employment contract, consultancy contract or any other terms and conditions for work activities with the Corporation. This notice will inform them that their data is being processed and:

- for what purpose it is being processed
- what types of disclosure are likely
- how to exercise their rights in relation to the data.

7.4 'Sensitive' data (including health information) will be held only with the knowledge and consent of the individual. In certain circumstances, such as a request from the police in a criminal investigation or in a health emergency, the Corporation may be obliged to pass on personal and sensitive details of their staff without prior consent being obtained.

7.5 Members of the public, and other individuals who provide their personal data to the Corporation, will be informed of the purpose and retention of this data collection before it is submitted. Where possible, this will be done via the corporate website at the point of collection.

7.6 INFORMATION CHARTER

In addition to providing 'fair processing' notices, the Corporation will publish an Information Charter on the corporate website. This will clearly state the purposes for which personal data is collected and processed by the Corporation. The following purposes apply:

- staff administration
- advertising, marketing and public relations
- accounts and financial records.

7.7 DIRECT MARKETING

The Corporation will not carry out direct marketing of individuals whose personal data it holds without prior explicit consent.

7.8 NOTIFICATION

Under the terms of the Data Protection Act, every organisation must notify the Information Commissioner's Office of the data they hold and the purpose for processing it. This notification must be renewed on an annual basis. Failure to do so is a criminal offence. There is a fee for notification and this is now based on a two tier system. LLDC is a Tier 2 organisation, for which the fee is £500. The Corporation's registration number is Z1915440.

8. SECURITY OF PERSONAL DATA

8.1 SECURITY CONTROLS

The security of the Corporation's personal data is paramount and security controls will be enforced to safeguard this information. These security controls include:

- firewalls and anti-virus software to protect the IT network
- folders restricted by permissions
- password protected databases and spreadsheets
- encrypted laptops and removable media
- segregation of duties in terms of user and super-user access to systems
- physical security controls in place for off-site storage of records.

8.2 The Corporation has outsourced its IT service provider, and IT staff with access to the Corporation's IT network and infrastructure have undertaken a Security Clearance vetting check and signed a Non-Disclosure Agreement to mitigate against the risks of unauthorised access to the Corporation's information.

8.3 STAFF AWARENESS AND TRAINING

All staff are required to attend an awareness training session on data protection and information security as part of their induction process, which is mandatory. In addition, guidance on handling personal data is provided to staff via the corporate intranet.

8.4 INFORMATION SHARING AGREEMENTS

The Corporation currently uses third parties to provide services, including the processing of some data. Those that currently have access to personal data are PS Financials and Cintra. Information sharing agreements have been included within the contracts and terms of conditions for those third party providers. Any new contracts or suppliers who either collect, store or process personal data on our behalf, or have physical or virtual access to personal data on the Corporation's IT systems must have an explicit Information Sharing Agreement in the contract. This is to ensure the confidentiality, integrity and availability of this sensitive information, as well as the Corporation's compliance with the Data Protection Act.

8.5 PERSONAL DATA BREACHES

An information security incident can occur if the confidentiality, integrity or availability of any personal data has been compromised. These incidents constitute an illegal breach of the Data Protection Act and must be treated seriously. In the event of a loss or unauthorised access of personal data held by the Corporation the information security incident management policy must be followed. In some situations, the Information Commissioner's Office will need to be informed, and if so, this should be done promptly. The Corporation should also consider seeking advice from the Department for Communities and Local Government and the Ministry of Justice, and possibly legal advisors, before notifying the ICO of a data protection breach.