London 2012 data protection policy

Introduction
The Data Protection Act (DPA) 1998 regulates the processing of information relating to individuals, this includes the obtaining, holding, using or disclosing of such information, and covers computerised records as well as manual filing systems and card indexes.

The Olympic Delivery Authority (ODA) and the London Organising Committee of the Olympic Games and Paralympic Games (LOCOG) (jointly 'London 2012') will hold the minimum personal information necessary to enable it to perform its functions. All such information is confidential and needs to be treated with care, to comply with the law.

This applies to all London 2012 and its operations, personnel, third party consultants, contractors and vendors.

1. Summary of principles

Data users must comply with the data protection principles of good practice which underpin the Act. These state that personal data shall be:

- obtained and processed fairly and lawfully (the subject of the data has consented to its collection and use);
- held only for specified purposes;
- adequate, relevant but not excessive;
- accurate and kept up to date;
- held for no longer than necessary;
- accessible to data subjects;
- subject to the appropriate security measures; and
- not be transferred outside the European Economic Area (Austria, Belgium, Denmark, Eire, Finland, France, Germany, Greece, Italy, Luxembourg, Netherlands, Portugal, Sweden & the UK as well as Iceland, Liechtenstein, Norway and Switzerland).

London 2012 and all staff who process, or use personal data must ensure that they abide by these principles at all times. This policy has been developed to ensure this happens.

2. Requirements of the Act - notification and registration

Staff must notify the Data Protection Officer, their departmental data protection representative and Information Security of any filing system or computer database that contains (or will contain) personal data (e.g. full name, street address and post code,

national insurance number, personal telephone number, personal email address, driver's license number, fingerprints, medical records, bank details) and complete the relevant notification forms to register systems. This notification will then be added to the London 2012's registration that is held by the Information Commissioner for approval.

London 2012 will keep some forms of information longer than others in line with Financial, Legal, Regulatory or Archival requirements.

A Retention and Disposal Policy shall be prepared which will require a list of retention periods, for personal data records, to be made available to the Data Protection Officer.

3. Responsibilities of staff

It is the responsibility of the Data Protection Officer to:

- assess the understanding of the obligations of London 2012 under the DPA;
- be aware of current compliance status;
- identify and monitor problem areas and risks and recommend solutions; and
- promote clear and effective procedures and offer guidance to staff on data protection issues. This will include familiarisation with the Act starting in the new starters' induction process, security awareness training programmes/seminars, annual appraisals and intranet/internet resources.

It is not the responsibility of the Data Protection Officer to apply the provisions of the DPA. This is the responsibility of the individual collectors, keepers and users of personal data. Therefore, all staff are required to be aware of the provisions of the DPA 1998, such as keeping records up to date and accurate, and its impact on the work they undertake on behalf of the organisation.

It is the responsibility of the Heads of business functions that all computer and manual systems within their respective service areas that contain personal data must be identified and the Data Protection Officer informed for notification purposes.

Any breach of the Data Protection Policy, whether deliberate, or through negligence may lead to disciplinary action being taken or even a criminal prosecution.

4. Data security

All staff are responsible for ensuring that:

- any personal data they hold, whether in electronic or paper format, is kept secure; and
- personal information is not disclosed deliberately or accidentally either orally or in writing to any unauthorised party.

5. Subject access requests

Stakeholders, partners, staff and members of the public have the right to access personal data that is being kept about them insofar as it falls within the scope of the 1998 DPA.

Any person wishing to exercise this right should make their request in writing, to the London 2012 Data Protection Officer. The ODA reserves the right to charge the recommended administrative fee on each occasion that access is requested.

The London 2012 aims to comply with request for access to personal information as quickly as possible, but must comply with a subject access request within forty days of receipt or the request, or if later, within forty days of the receipt of the identity information required, the completed subject access request form and any relevant fee.

London 2012 does not need to comply with a request where it has received an identical or similar request from the same individual unless a reasonable interval has elapsed between compliance with the original request and the current request.

6. Subject consents

The need to process data for normal purposes will be communicated to all staff. In some cases, if the data is sensitive, for example information on health, race or gender, express consent to process the data must be obtained. This processing may be necessary to operate policies such as health and safety and equal opportunities.

7. Data Protection Officer

London 2012 is the data controller under the Act and is therefore ultimately responsible for implementation. However day to day matters, the registration of systems and subject access requests will be dealt with by the Data Protection Officer.