Data Protection Policy

Introduction

The Data Protection Act 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 Greater London Authority 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.

Summary

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 (that the subject of the data has consented to its collection and use).
- Be held only for specified purposed.
- Be adequate, relevant but not excessive.
- Be accurate and kept up to date.
- Be held for no longer than necessary.
- Be accessible to data subjects.
- Be subject to the appropriate security measures.
- Not be transferred outside the EEA (European Economic Area which includes the EU member states: Austria, Belgium, Denmark, Eire, Finland, France, Germany, Greece, Italy, Luxembourg, Netherlands, Portugal, Sweden & the UK as well as Iceland, Liechtenstein, Norway and Switzerland)

The Authority 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.

Requirements of the Act (Notification & Registration)

Authority staff must notify the Data Protection Officer, or their departmental Data Protection representative of any filing system or computer database that contains (or will contain) personal data (e.g. name and address) and complete the relevant notification forms to register your system. This notification will then be added to the Authority's registration, which is held by the Information Commissioner for approval.

The Data Protection Officer will manage notification forms.

The Authority will keep some forms of information longer than others in line with Financial, Legal or Archive requirements.

The retention and disposal policy will be prepared which will require a list of retention periods, for personal data records, to be made available to the Data Protection Officer. The Data Protection User Group is current discussing this.

Responsibilities of Staff

It is the responsibility of the Data Protection Officer to:

- Assess the understanding of the obligations of the Greater London Authority under the Data Protection Act.
- Be aware of our current compliance status.
- Identify and monitor problem areas and risks and recommend solutions.
- Promote clear and effective procedures and offer guidance to staff on Data Protection issues. It is anticipated that this will include familiarisation with the Act starting in the new starters induction process, 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 Data Protection Act. This is the responsibility of the individual collectors, keepers and users of personal data. Therefore staff are required to be aware of the provisions of the Data Protection Act 1998, such as keeping records up to date and accurate, and it's impact on the work they undertake on behalf of the Authority.

It is the responsibility of the Head of Service 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.

Data Security

All staff are responsible for ensuring that:

- Any personal data they hold, whether in electronic or paper format, is kept securely.
- Personal information is not disclosed deliberately or accidentally either orally or in writing to any unauthorised third party.

Subject Access Requests

Assembly members, 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 Act. Any person wishing to exercise this right should make their request in writing, using the Authority's subject access request from and then forward it to the Data Protection Officer. The Authority reserves the right to charge the recommended administrative fee on each occasion that access is requested.

The Authority aims to comply with request for access to personal information as quickly as possible, but the Authority 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 the relevant fee.

The Authority 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.

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 Authority policies such as health and safety and equal opportunities.

Data Protection Officer

The Authority is the data controller under the Act and is therefore ultimately responsible for implementation. However, day to day matter, the registration of systems and subject access requests will be dealt with by the Data Protection Officer; Ian Lister, Information Governance team, ext. 4668