HILLINGDON
LONDON

Information Security Statement

The objective of this statement is to provide executive direction for the protection of information owned by the London Borough of Hillingdon and our citizens, partners or suppliers in whatever form it may be held or communicated, whether verbal, on paper or electronic. Information is one of our most valuable assets. Of equal value is the trust of our partners and clients that we will protect the information that they have shared with us.
LBH proprietary and client, partner or supplier information, when created, stored, transmitted or communicated, must be protected from unauthorised access, use, modification or destruction.

Consequently, all access to, and use of this information and data, requires adherence to the following policy principles:

- **Confidentiality -** Appropriate measures must be taken to ensure that LBH proprietary, private, or client information is accessible only to those authorised to have access.
- **Integrity -** The accuracy and completeness of LBH information must be maintained and all changes or modifications affecting that information must be authorised, controlled, and validated.
- **Availability –** Information must be available to authorised individuals when required. In the event of a disaster or malicious attack, the Council's information and the systems critical to the ongoing activities of the Council must be recoverable.
- **Authentication -** All persons and systems seeking access to information, or to our networked computer resources must first establish their identity to the satisfaction of the Council.
- **Access Control -** The privilege to view, or modify information, computer programs, or the systems on which the information resides, must be restricted to only those whose job functions absolutely require it.
- **Auditing -** User access and activity on each of the Council's computers, firewalls and networks must be recorded and maintained in compliance with all security, retention, legislation and regulatory requirements.

Security policies are in place to support these objectives, together with detailed procedures.
The Information Security Officer has responsibility for maintenance of the Security Policies, which will be reviewed annually by the Hillingdon Information Assurance Group (HIAG).

It is the responsibility of each member of staff to adhere to LBH Security Policies.

The Information Security Officer has responsibility for maintenance of the Security Policies, which will be reviewed annually by the Hillingdon Information Assurance Group (HIAG).

All managers are responsible for implementing the Security Policies within their areas, and for adherence thereof by their staff.

It is the responsibility of each member of staff to adhere to LBH Security Policies.

Chief Executive **Date**

Fran Beasley 8 October 2015