

## Information Security Policy

### Purpose

To clearly set out both the Authority's and the individual's responsibilities relating to the handling of information.

### General Principles

- Material marked as 'restricted' must not be sent electronically to personal, insecure email addresses.
- Information which is not suitable for the public domain must not be processed or stored on personal computing equipment.
- The delivery of hard copy material must be undertaken in the most appropriate manner, with regards to the level of the security of the information being conveyed.
- Storage and retention of 'restricted' documents must be on a needs basis and each case reviewed individually.

### How are the general principles achieved?

- No security descriptor should be included on the outside of the envelope when posting sensitive information to outside persons.
- When sending sensitive material by post, strong and secure means of postage should be used in all instances
- Where appropriate, sensitive papers should be returned at the end of meetings – the papers could be clearly marked "Not to be retained after meeting on <date>" to ensure they are returned.
- Regular review of internal circulation of papers will be undertaken to determine whether distribution lists are up to date and appropriate.
- Clear desk policy – restricted papers to be out of sight and stored securely when not in use.
- Once restricted papers are returned, they must be destroyed appropriately and immediately, by shredding. Multiple copies should not be retained, or where this is necessary, they should be secured appropriately

- Regular review of storage of information (both in hard copy and in electronic form), ensuring adherence to the retention and disposal policy.
- General correspondence files should be regularly weeded and non-necessary correspondence destroyed in line with the retention and disposal policy.
- Duplication of both hard and electronic storage of information must be avoided. This can be assisted by having only one place where such records are stored and a clear labelling policy for all files stored electronically

Mark Sellwood  
Chief Executive  
31 December 2008