



Data Protection Policy

1. Policy scope

- 1.1 This policy outlines our approach to ensuring that information is handled securely, confidentially and in accordance with the law.
- 1.2 This policy applies to all employees, board members and others who are involved in the collection of, and processing of, personal data on behalf of Peabody.
- 1.3 This policy applies to all data, whether it is held in paper form or by electronic means. This includes data, images and recordings on all Peabody equipment and any Peabody information held on personal devices being used under Peabody's "Bring Your Own Device" policy.
- 1.4 This policy also applies to all data held by our contractors in paper form or by electronic means.

2. Policy statement

- 2.1 We will ensure that there is a nominated individual responsible for data protection compliance: the Data Compliance Manager will provide a central point of contact for all data protection issues.
- 2.2 We will ensure that Peabody complies with the Data Protection Act 1998, including the 8 data protection principles.
- 2.3 We will ensure that all data collected is used fairly and lawfully. This means we will:
 - Only use data in ways that are justifiable;
 - Be transparent about how we use personal data; and
 - Ensure that it is handled only in ways that the individuals would expect.
- 2.4 We will ensure that data is only processed for the purposes of meeting our operational needs or to fulfil our legal requirements.
- 2.5 We will have appropriate retention periods for personal data and not keep data for any longer than is necessary to meet our operational needs or to fulfil our legal requirements.
- 2.6 We will ensure that the data we hold is accurate and up to date.
- 2.7 We will ensure that all employees responsible for personal data are appropriately trained.
- 2.8 We will have appropriate technical and organisational measures in place to guard against unauthorised access to, and accidental loss of, personal data.

- 2.9 We will have a policy and process in place for capturing and reporting information security breaches (Information Security Breach Policy).
- 2.10 We will ensure that all staff are aware of the need to report information security breaches.
- 2.11 We will ensure that any disclosures made without the explicit consent of the individual whom the information is about are made in line with the Data Protection Act 1998.
- 2.12 We will disclose information to the relevant agencies for the purposes of safeguarding, in line with the Data Protection Act 1998.
- 2.13 We will share information with the police for the prevention and detection of crime, in line with the Data Protection Act 1998.
- 2.14 Peabody acknowledges individuals' rights under the law to have access to information which is about them. We will have processes in place to deal with these requests effectively and within the statutory timeline.
- 2.15 Peabody will not make personal data commercially available to any third party except with the express consent of the data subject.

3. Monitoring and continuous improvement

This policy will be reviewed every three years, unless legislation, business or sector developments require otherwise. This is to ensure that it continues to meet its objectives and takes account of good practice developments.

Version number	8
Approved by	IMG
Effective from	05/2015
Policy owner	Data Compliance Manager
Policy author	Data Compliance Manager
Date of next review	04/2018
Equality Impact Assessment (EIA)	N/A