BARLEY MONT GROUP POLICY ON PERSONAL DATA PROTECTION

Contents

Policy Statement ........................................................................................................ 2
Policy Scope .............................................................................................................. 3
Policy Objectives .................................................................................................... 4
Policy Principles ...................................................................................................... 5
  Fair Collection and Processing ............................................................................ 5
  Security .............................................................................................................. 6
  Data Sharing ...................................................................................................... 6
  Privacy Impact Assessments ............................................................................. 6
  Access .............................................................................................................. 7
  Links with the Freedom of Information 2000 .................................................... 7
Policy Responsibilities ............................................................................................ 8
Policy Communication ............................................................................................ 9
Policy Benefits ....................................................................................................... 10

Appendices:
  1: Relevant Authoritative Bodies and Related Documents............................... 11
  2: Document and Version Control .................................................................... 12
  3: Data Protection Definitions and Terms ......................................................... 13
  4: Schedule 2 (Data Protection Act) Conditions for Processing Personal Data... 14
  5: Schedule 3 (Data Protection Act) Conditions for Processing Sensitive Data ... 15
  6: Rights of Data Subjects ................................................................................ 16
  7: Qualified European Economic Areas ............................................................ 17
Policy Statement

1.0 Pedagogy Auras T/A Barley Lane Montessori Day Nursery, Pre-School and After-School Centre(s), aka Barley Mont Group (BMG) fully understands its obligations to ensure that personal information is treated fairly, lawfully and correctly, and is committed to achieving compliance with the laws of the Data Protection Act (DPA) 1998.

2.0 The DPA sets out the rules for how organisations must process personal data and sensitive personal data about living individuals. It gives individuals the right to find out what personal data is held about them by organisations (both electronically and within a manual filing system) and to see and correct any personal data held.

3.0 BMG needs to collect and process personal data about people, including staff, children and individuals with whom it deals with, in order to operate its daily business and for the organisation to operate effectively.

4.0 BMG is committed to ensuring that staff are appropriately trained and supported to achieve compliance with the DPA. This is regarded by BMG as being very important in maintaining the confidence between them and with those whose personal data they hold.

5.0 BMG fully endorses and adheres to the Data Protection Principles given below.

**The Eight Principles of the Data Protection Act**

P1: Personal data must be fairly and lawfully processed, and in particular, shall not be processed unless specific conditions\(^1\) under Schedule 2 and Schedule 3 of the Act are met.

P2: Personal data shall be obtained and used for one or more specified and lawful purposes, and shall not be processed in any manner incompatible with that purpose or purposes.

P3: Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

P4: Personal data shall be accurate and kept up to date.

P5: Personal data shall not be kept for longer than is necessary for the purpose or purposes it was collected for.

P6: Personal data shall be processed in line with the individuals’ rights (see Appendix 6).

P7: Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

\(^1\) Specific conditions under Schedules 2 of the DPA must be met to process personal data (see Appendix 4).
Specific conditions under Schedule 3 of the Act must be met to process sensitive personal data. (see Appendix 5)

P8: Personal data shall not be transferred to a country or territory outside the European Economic Area (see Appendix 7) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of their personal data.

Policy Scope

6.0 This policy has been written within the guidelines of relevant authoritative bodies and related documentation listed at Appendix 1.

7.0 Definitions and terms used throughout this policy are defined at Appendix 2.

8.0 This policy applies to all personal data and sensitive personal data collected and processed by BMG in the conduct of its business, in electronic format in any medium and within structured paper filing systems.

9.0 This policy applies to all BMG employees, whether permanent, temporary, contractors, consultants or seconders (hereafter referred to as ‘staff’).

10.0 Disciplinary action may be taken against staff failing to comply with this policy.

11.0 BMG is the Data Controller of, and registered with the Information Commissioner’s Office (ICO) for collecting and using personal data about:

- individuals who have applied for, or been awarded, funding by the government for the children in their care to enable such children to attend BMG’s facilities
- members of BMG management
- past, current and prospective employees
- suppliers, consultants, external business partners and other third parties with whom BMG communicates
- other persons as required by law

12.0 BMG places a duty of responsibility on members of the BMG community, such as members of Parents committee and reviewers, to respect the requirement for confidentiality on receipt of confidential papers or correspondence containing BMG personal data. Members are provided with information in compliance with this policy, relative to their official capacity with BMG membership.

13.0 BMG is registered with the ICO to process personal data for the following specified purposes:

- Staff Administration
- Advertising, Marketing and Public Relations
- Accounts and Records
- Benefits, Grants and Loans Administration
- Consultancy and Advisory Services
• Crime Prevention and Prosecution of Offenders
• Journalism and Media
• Property Management
• Research

14.0 A further description of each purpose can be found on the ICO Website (http://www.ico.gov.uk/ESDWebPages/search.asp), by quoting the Registration Number ZA009018

15.0 A list of relevant legislation, regulations and supporting frameworks that provide background to this, as well as related BMG policies and strategies are listed in Appendix 1.

Policy Objectives

16.0 The objectives of this policy are to ensure that:

• proper procedures are in place for the processing and management of personal data

• there is someone within the organisation who has specific responsibility and knowledge about data protection compliance.

• a better and supportive environment and culture of best practice processing of personal data is provided for staff

• all staff understand their responsibilities when processing personal data, and that methods of handling that information are clearly understood

• individuals wishing to submit a Subject Access Request are fully aware of how to do this and who to contact

• Subject Access Requests are dealt with promptly and courteously

• individuals are assured that their personal data is processed in accordance with the data protection principles, that their data is secure at all times and safe from unauthorised access, alteration, use or loss

• other organisations with whom BMG data needs to be shared or transferred, meet compliance requirements

• any new systems being implemented are assessed on whether they will hold personal data, whether the system presents any risks, damage or impact to individuals’ data and that it meets this policy

Policy Principles
17.0 In order to meet the requirements of the 8 principles of the DPA, BMG adheres to the following values when processing personal data:

18.0 Fair Collection and Processing

- The specific conditions contained in Schedules 2 and 3 of the DPA (see Appendices 4 and 5) regarding the fair collection and use of personal data will be fully complied with.

- Individuals will be made aware that their information has been collected, and the intended use of the data specified either on collection or at the earliest opportunity following collection. This may be verbally, written or through electronic direction to the BMG Privacy Notice.

- Personal data will be collected and processed only to the extent that it is needed to fulfil business needs or legal requirements.

- Personal data held will be kept up to date and accurate.

- Retention of personal data will be appraised and risk assessed to determine and meet business needs and legal requirements, with the appropriate retention schedules applied to that data.

- Personal data will be processed in accordance with the rights of the individuals about whom the personal data are held.

- Individuals whose personal information is held on a BMG Contacts Database will be provided with the option to ‘opt out’ of receiving event invitations and future communications.

- A ‘cease processing request’ from an individual will be acknowledged within 3 working days, with the final response within 21 days. The final response will state whether BMG intend to comply with the request and to what extent, or will state the reasons why it is felt the requestor’s notice is unjustified.

- Staff will advise the Data Protection Officer in the event of any intended new purposes for processing personal data. No new purpose for processing data will take place until the ICO has been notified of the relevant new purpose and the data subjects have been informed, or in the case of sensitive data, their consent has been obtained.

19.0 Security

- Appropriate technical, organisational and administrative security measures to safeguard personal data will be in place.

- Staff will report any actual, near miss, or suspected data breaches to the BMG Data Protection Officer for investigation. Lessons learnt during the investigation of
breaches will be relayed to those processing information to enable necessary improvements to be made.

- Any unauthorised use of corporate email by staff, including sending of sensitive or personal data to unauthorised persons, or use that brings BMG into disrepute will be regarded as a breach of this policy.

- Staff will use appropriate protective markings to protect and secure any document containing personal information. In this way informing recipients of the document of the measures that need to be employed for its appropriate handling.

- An Information Asset Register will be maintained identifying personal data held at the main office, where it is held, how it is processed and who has access to it.

- Updated Data Protection Information will be provided to staff to keep them better informed of relevant legislation and guidance regarding the processing of personal information.

- There is a member of staff within BMG Office who has specific responsibility for data protection, covering all aspects within the scope of this policy.

20.0 Data Sharing

- Personal data will not be transferred outside the European Economic Area unless that country or territory can ensure a suitable level of protection for the rights and freedoms of the data subjects in relation to the processing of their personal data.

- Personal data in any format will not be shared with a third party organisation without a valid business reason, a Data Sharing Agreement in place, or without the data subjects’ consent.

21.0 Privacy Impact Assessments

- The Information Management and Information Services Teams will work collaboratively to carry out Privacy Impact Assessments on all new systems intended for implementation in BMG to determine the risks and impacts to the personal data of the individuals those systems are intended to hold.

- Personal data will not be used to test any systems, unless it is proven to be satisfactory and safe that such use is the only practical method to test that system.

22.0 Access

- Members of staff will have access to personal data only where it is required as part of their functional remit.

- Staff are made aware that in the event of a Subject Access Request being received in BMG, their emails may be searched and relevant content
disclosed, whether marked as personal or not.

- The BMG Privacy Notice will include a contact address for data subjects to use should they wish to submit a Subject Access Request, make a comment or complaint about how BMG is processing their data, or about BMG’s handling of their request for information.

- A Subject Access Request will be acknowledged to the data subject within 3 working days, with the final response and disclosure of information (subject to exemptions) within 40 calendar days. A fee may be charged for this, at BMG’s discretion, which will be no more than £10.

- A data subject’s personal information will not be disclosed to them until their identity has been verified.

- Third party personal data will not be released by BMG when responding to a Subject Access Request or Freedom of Information Request (unless consent is specifically obtained, obliged to be released by law, or necessary in the substantial public interest).

- All data subjects have a right of access to their own personal data; BMG will provide advice to data subjects on how to request or access their personal data held by BMG.

23.0 Links with the Freedom of Information Act 2000

- The Freedom of Information Act 2000 enables greater public access to information processed by public bodies such as the BMG. However, personal data continues to be protected by the Data Protection Act 1998, and is therefore exempt from disclosure under the Freedom of Information Act (Section 40).
## Policy Responsibilities

### 24.0 Primary Responsibility

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsible for:</th>
</tr>
</thead>
</table>
| Data Protection Officer (DPO) / Information and Records Manager (IRM) | • maintaining the BMG notification with the ICO  
• advising staff on data protection compliance  
• maintaining the BMG Information Asset Register (IAR)  
• assessing management of personal data listed on the IAR for potential risks  
• processing subject access requests  
• reporting any personal data breaches to the SIRO, ISO and ICO as appropriate  
• carrying out Privacy Impact Assessments against planned new systems that will hold personal data  
• issuing data sharing guidance and developing Data Sharing Agreements between BMG and external organisations  
• development, administration, dissemination, review and application of this policy |
| Senior Information Risk Officer (SIRO)                               | • providing an annual statement of internal control relating to the management of personal data to the Chief Executive  
• reporting on Information Risk Management to the BMG Management and parent departments |
| Information Security Officer (ISO)                                   | • assessing information assets held for the impact of loss  
• managing Information Security Incidents and correct reporting to SIRO, ICO and parent department.  
• information risk assessment returns to BMG SIRO and BIS  
• advising staff on information security and assurance matters |
| Information Asset Owners (IAO)                                      | • supporting this policy and implementing within their specific areas of the business  
• personal data processed within their area of business  
• risk management of personal data within their area of business  
• providing annual assurance of the risk controls to the ISO and SIRO  
• maintaining an accurate IAR for their area of the business  
• delegating limited responsibility to an Information Asset Administrator within their area of the business |
| Information Asset Administrators (IAA)                              | • reporting any personal data security incidents or breaches to their IAO, DPO and ISO  
• maintaining an IAR for their area of business for annual sign-off by their IAO  
• encouraging and promoting use of protective marking to their |
team/group

• ensuring appropriate retention and disposal of personal data held within their area of the business in accordance with the BMG retention policy

25.0 Supporting Responsibility

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsible for:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Director</td>
<td>• BMG personal data overall</td>
</tr>
<tr>
<td>Manager/Deputy Managers</td>
<td>• supporting this policy and applying within their respective Groups</td>
</tr>
<tr>
<td>Office Administration Team</td>
<td>• approval, endorsement and support of this policy</td>
</tr>
<tr>
<td>Head of Information Services</td>
<td>• ensuring the security of electronic information</td>
</tr>
<tr>
<td>Head of Information Management</td>
<td>• supporting and applying this policy office wide</td>
</tr>
<tr>
<td>All Staff</td>
<td>• complying with this policy</td>
</tr>
<tr>
<td></td>
<td>• attending annual training for data protection awareness</td>
</tr>
<tr>
<td></td>
<td>• applying the correct protective marking to information they create</td>
</tr>
</tbody>
</table>

Policy Communication

26.0 Internal

• This policy will be made available to all staff by being declared as a record and stored within the appropriate Office Policies folder in Staff rooms or at the Main office.

• Communication of this policy will be made through notification to the staff verbally, in writing, through staff trainings or by any other means practicable.

27.0 External

• This policy and the BMG Privacy Notice will be communicated externally by publishing it on the BMG website.

• The BMG Data Protection Officer can be contacted via the email address hrbarleylane@hotmail.co.uk
Policy Benefits

28.0 This policy will benefit BMG by:

- enabling excellent standards of management and processing of personal data through the provision of a consistent and stable culture towards data protection applied office wide
- ensuring continued compliance with the DPA principles
- providing an appropriately supportive environment and culture towards best practice processing and protection of personal data
- ensuring employee confidence and compliance in their processing of personal data, being fully informed and aware of their responsibilities and obligations
- improved readiness of the service to process Subject Access Requests, better decision making, development of policy and procedures, and design and implementation of information systems through the consideration and assessment of personal data
- reducing potential risk of legal or reputational damage through poor personal data management
- providing confidence to the BMG community that their personal data is being handled correctly and ensuring data subjects know how to access it
Appendix 1: Relevant Authoritative Bodies and Related Documents

### Authoritative Bodies

<table>
<thead>
<tr>
<th>Information Commissioner Office</th>
<th>The Information Commissioner’s Office is the UK’s independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cabinet Office</td>
<td>The Cabinet Office coordinates policy and strategy across government departments and is the driving force behind the Information Assurance agenda within central government departments and arm’s length bodies.</td>
</tr>
<tr>
<td>Communications – Electronics Security Group (CESG)</td>
<td>The CESG is the Information Assurance arm of UK Government Communications Headquarters (GCHQ) - Author of many of UK Government Security and Information standards and best practices in the UK.</td>
</tr>
<tr>
<td>Joint Information Systems Committee (JISC)</td>
<td>JISC is an advisory committee to the Research Councils providing expertise to support data and information management programmes.</td>
</tr>
<tr>
<td>The National Archives (TNA)</td>
<td>TNA is the UK government’s official archive and central advisory body on the care of, and how the DPA affects, records and archives.</td>
</tr>
</tbody>
</table>

### Related Documents

<table>
<thead>
<tr>
<th>Security Policy Framework</th>
<th>HMG Security Policy Framework authored by the Cabinet Office provides central internal protective security policy and risk management for government departments and associated bodies. It is the source on which all localised security policies should be based.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Good Data Handling Guidance</td>
<td>CESG Good Data Handling Guide 2008 provides advice for departments with a requirement to protect personal and sensitive information as part of their day to day business.</td>
</tr>
<tr>
<td>BMG Information and Records Management Policy</td>
<td>Defines BMG's policy for the management of information and records.</td>
</tr>
<tr>
<td>BMG Retention Policy for Information and Records</td>
<td>Defines BMG’s policy for the retention of information and records.</td>
</tr>
<tr>
<td>BMG Protective Marking Policy</td>
<td>Defines the policy and procedures that enable the correct marking and handling of information by staff.</td>
</tr>
<tr>
<td>BMG Information Governance Policy</td>
<td>This policy provides the framework for the clear ownership of information and the management of information security risks.</td>
</tr>
<tr>
<td>BMG Email Policy</td>
<td>This policy defines the appropriate and acceptable use of email across the Office and supports better information management and data protection principles.</td>
</tr>
</tbody>
</table>
## Appendix 2: Document and Version Control

### Document Control

<table>
<thead>
<tr>
<th>Version</th>
<th>1.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective From Date</td>
<td></td>
</tr>
<tr>
<td>Approved By</td>
<td>Office Administration Group</td>
</tr>
<tr>
<td>Date of Approval</td>
<td></td>
</tr>
<tr>
<td>Date of Review</td>
<td></td>
</tr>
<tr>
<td>Retention Period</td>
<td>Indefinitely; 2 years after superseded</td>
</tr>
<tr>
<td>Owner</td>
<td>Human Resources Department</td>
</tr>
<tr>
<td>Author</td>
<td>Sarah Okwese-Ayodele</td>
</tr>
</tbody>
</table>

### VERSION CONTROL

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Status</th>
<th>Revision Date</th>
<th>Author(s)</th>
<th>Summary of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Draft</td>
<td>26/06/2013</td>
<td>Sarah Okwese-Ayodele</td>
<td>Creation of Policy Document</td>
</tr>
</tbody>
</table>

### DISTRIBUTION FOR REVIEW

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Approved Date</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Meesha Jalah</td>
<td>Director/Manager</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### TAGS/KEYWORDS

<table>
<thead>
<tr>
<th>Policy</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record</td>
<td>Information</td>
</tr>
<tr>
<td>Data Protection</td>
<td>Document</td>
</tr>
<tr>
<td>Security</td>
<td>Data</td>
</tr>
<tr>
<td>Protect</td>
<td>Legislation</td>
</tr>
<tr>
<td>Information Management</td>
<td>Information Security</td>
</tr>
<tr>
<td>Personal</td>
<td>Personal Information</td>
</tr>
<tr>
<td>Personal Data</td>
<td>Sensitive</td>
</tr>
</tbody>
</table>
## Appendix 3: Data Protection Definitions and Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>Information which is recorded in any format, whether stored electronically or in a structured paper based filing system.</td>
</tr>
<tr>
<td>Personal Data</td>
<td>Any information that identifies a living individual. This includes any expression of opinion about the individual and any intentions towards the individual.</td>
</tr>
<tr>
<td>Sensitive Personal Data</td>
<td>Personal information relating to racial or ethnic origin, political opinion, religious beliefs, trade union membership, sexual life, physical or mental health, commission or alleged commission of any offence.</td>
</tr>
<tr>
<td>Processing</td>
<td>Any activity where the data is used, such as obtaining, recording, storing, viewing, copying, accessing, disclosing, erasing, destroying.</td>
</tr>
<tr>
<td>Data Subject</td>
<td>An individual who is the subject of personal information.</td>
</tr>
<tr>
<td>Data Controller</td>
<td>The organisation that determines how the personal data will be used and the manner in which it will be processed.</td>
</tr>
<tr>
<td>Data Processor</td>
<td>An organisation that processes personal data on behalf of a Data Controller.</td>
</tr>
<tr>
<td>Exemptions</td>
<td>Some personal data are exempt from disclosure under the DPA, including confidential references given (not received), consideration of suitability for honours, management forecasts and career planning.</td>
</tr>
<tr>
<td>Relevant Filing System</td>
<td>Any set of manual information which is structured by reference to individuals or other criteria making the content readily accessible.</td>
</tr>
<tr>
<td>Subject Access Request</td>
<td>A request by a data subject, to the data controller, asking to see their personal information.</td>
</tr>
<tr>
<td>Third Party</td>
<td>This can either mean that the data is about someone else, or someone else is the source; i.e. any other person or organisation other than</td>
</tr>
<tr>
<td></td>
<td>• the data subject</td>
</tr>
<tr>
<td></td>
<td>• the data controller</td>
</tr>
<tr>
<td></td>
<td>• a data processor</td>
</tr>
<tr>
<td>Recipient</td>
<td>Any person to whom the data are disclosed including employees or agents of the data controller; this does not include any person to whom disclosure is made as a result of an inquiry or request for information.</td>
</tr>
</tbody>
</table>
## Appendix 4: Conditions for Processing Personal Data

**Schedule 2 of the Data Protection Act 1998**

The 1st Principle of the DPA requires personal data to be processed fairly and lawfully, and, not to be processed unless one of the conditions (below) in Schedule 2 is met.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The data subject has given his/her <strong>consent</strong> to the processing.</td>
</tr>
<tr>
<td>2</td>
<td>Processing is necessary for:</td>
</tr>
<tr>
<td></td>
<td>a) the performance of a <strong>contract</strong> to which the data subject is a party</td>
</tr>
<tr>
<td></td>
<td>b) taking steps at the request of the data subject with a view to entering into a contract</td>
</tr>
<tr>
<td>3</td>
<td>Processing is necessary for compliance with any <strong>legal</strong> obligations to which the data controller is subject.</td>
</tr>
<tr>
<td>4</td>
<td>Processing is necessary in order to protect the <strong>vital interests</strong> of the data subject.</td>
</tr>
<tr>
<td>5</td>
<td>Processing is necessary for the:</td>
</tr>
<tr>
<td></td>
<td>a) administration of justice</td>
</tr>
<tr>
<td></td>
<td>b) exercise of any functions conferred on a person under any enactment</td>
</tr>
<tr>
<td></td>
<td>c) exercise of any functions of the Crown or a government department</td>
</tr>
<tr>
<td></td>
<td>d) exercise of any other functions of a public nature carried out in the public interest by any person</td>
</tr>
<tr>
<td>6</td>
<td>Processing is necessary for the purposes of <strong>legitimate interests</strong> of the data controller or by the third party to whom data may be disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedom or legitimate interests of the data subject.</td>
</tr>
</tbody>
</table>

**In practice this means that organisations must:**

a) have legitimate grounds for collecting and using the personal data  

b) not use the data in ways that have unjustified adverse effects on the individual  

c) be transparent about how it is intended to use the data by provide appropriate privacy notices when collecting personal data  

d) handle personal data only in ways they would reasonably expect  

e) make sure no unlawful activities are carried out with the data
Appendix 5: Conditions for Processing Sensitive Personal Data

Schedule 3 of the Data Protection Act 1998

Under the 1st Data Protection Principle, sensitive personal data must not be processed unless one of the following 19 legitimate conditions (below) from Schedule 3 of the DPA is met.

- Explicit consent of the data subject
- Compliance with employment law obligations
- Vital interests of the data subject
- Processing by not-for-profit organisations.
- Information made public by the data subject
- Legal advice and establishing or defending legal rights
- Public functions
- Medical purposes
- Records on racial equality
- Detection of unlawful activity
- Protection of the public
- Public interest disclosure
- Confidential counselling
- Certain data relating to pensions
- Religion and health data for equality of treatment monitoring
- Legitimate political activities
- Research activities that are in the substantial public interest
- Police processing
- Processing by elected representatives
Appendix 6: Rights of Data Subjects

Principle 6 of the Data Protection Act 1998 gives rights to individuals in respect of the personal data that organisations hold about them. These are a right to:

- have access to a copy of the information comprised in their personal data
- object to processing that is likely to cause or is causing damage or distress
- prevent processing for direct marketing
- object to decisions being taken by automated means
- have inaccurate personal data rectified, blocked, erased or destroyed
- claim compensation for damages caused by a breach of the Act

The right of subject access is wide-ranging and unless a relevant exemption applies an individual is entitled to see their personal data contained in all locations, including:

- Appraisal records
- Minutes of meetings
- Emails stored on any system in the workplace
- References received from third parties
- Disciplinary records
- Sickness records
- Performance review notes
- Interview notes

Individuals are only entitled to see their own personal data and are not entitled to receive any information which relates to anyone else.
Appendix 7: European Economic Areas

There are no restrictions on the transfer of personal data to EEA countries. These are currently:

Austria  | Greece  | Netherlands  
Belgium  | Hungary  | Norway  
Bulgaria | Iceland  | Poland  
Cyprus   | Ireland  | Portugal  
Czech Republic | Italy  | Romania  
Denmark  | Latvia  | Slovakia  
Estonia  | Liechtenstein  | Slovenia  
Finland  | Lithuania  | Spain  
France   | Luxembourg  | Sweden  
Germany  | Malta  

The European Commission has decided that certain countries have an adequate level of protection for personal data. Currently the following countries are considered as having adequate protection:

Argentina  | Isle of Man  | Faroe Islands  
Canada  | Jersey  
Guernsey  | Switzerland  

Personal data sent to the United States of America under the ‘Safe Harbor’ scheme is considered by the European Commission to be adequately protected. When a US company signs up to the Safe Harbor arrangement, they agree to:

- follow 7 principles of information handling and
- be held responsible for keeping to those principles by the Federal Trade Commission