Peninsula Learning Trust

Data Protection Policy

Date	Author	Update
18th March 2015	Ben Bull	Initial Document
19th March 2015	Ben Bull	Incorporate changes from E Willcocks
9th June 2015	Ben Bull	Incorporate changes from Legal Counsel

All data users, who process personal data on behalf of the Peninsula Learning Trust (the "Trust", "we", "our") must comply with this policy.

This policy will be reviewed at least every 2 years by a committee of senior staff to include the Director of IT and Data Protection Officer.

The Data Protection Officer is Ben Bull who can be contacted on bbull@peninsulatrust.org.

Introduction

The Trust is whole heartedly committed to protecting the rights and freedoms of individuals including with regard to the way in which their personal data is handled. This policy sets out the key measures which the Trust has adopted to ensure good practice and compliance with the requirements of the Data Protection Act 1998 ("the Act").

The Act is the United Kingdom's statutory implementation of a European Data Protection Directive and applies to personal data held in any medium, including but not limited to;

- Paper
- Computer
- Microfiche
- Tape
- Enterprise storage
- Tablet computers, laptops and smart phones
- Portal media such as memory sticks, optical media, etc.

The Trust acknowledges that it must comply with the principles of the Act. These provide that personal data must be:

A. Processed fairly and lawfully.
B. Processed for limited purposes and in an appropriate way.
C. Adequate, relevant and not excessive for the purpose.
D. Accurate.
E. Not kept longer than necessary for the purpose.
F. Processed in line with data subjects' rights.
G. Secure.
H. Not transferred to people or organisations situated in countries without adequate protection.

This document defines personal data as information about identifiable, living individuals. During the course of our activities we will collect, store and process personal data of current, past and present employees, students, temporary staff, contractors, suppliers and other users and we recognise that the correct and lawful treatment of this data will maintain confidence in the Trust and will provide for successful operations. In accordance with our notification under the Act, personal data will be used for the following purposes:

- Education
- Student and Staff Support Services
- Staff, Agent and Contractor Administration
- Accounts and Records
- Advertising, Marketing, Public Relations, General Advice Services
- Commercial Services
- Fundraising
- Publication of prospectuses, magazines, and the promotional material
- Crime Prevention and Prosecution of Offenders
- Archive Services
- Realising the Objectives of an Educational Charitable Organisation or Voluntary Body.

We will only process data for these purposes or for any other purposes specifically permitted by the Act. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources and sets out the rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data. This policy applies to all staff working for, or on behalf of, the Trust and includes direct employees, the board of directors and governors, employees of other organisations working for in association with the Trust, associates and contractors, students, volunteers or other 3rd parties with access to the Trust's personal data or systems ("**data users**"). All data users are obliged to comply with this policy when processing personal data on our behalf.

Any breach of the data protection policy or the Data Protection Act 1998 will be automatically considered as a breach of discipline and existing Peninsula Learning Trust disciplinary proceedings will apply.

This policy does not form part of any employee's contract of employment and may be amended at any time.

Definition of Data Protection Terms

Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

Data subjects for the purpose of this policy include all living individuals about whom we

hold personal data save for our employees. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our business for our own commercial purposes.

Data processors include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on the Trust's behalf.

Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

Responsibilities

The Trust is the 'data controller' under the Act and the Board of Governors is the highest authority within the Trust which is responsible for compliance with the Act. The Trust will take the appropriate measures to ensure compliance and to protect data subjects' rights under the Act.

The Trust has appointed a Data Protection Officer (senior management member) who is responsible for the administration and oversight of the Trust's data protection matters including dealing with day-to-day data protection matters, organising training for data users and for developing and encouraging good information handling practice amongst all data users within the Trust. The Data Protection Officer will ensure that the Trust annually notifies the Information Commissioner of its processing.

All employees in managerial or supervisory roles have the responsibility of overseeing compliance and developing good data protection practice within their designated areas. Managers should ensure that staff are appropriately informed, aware of this policy and where applicable, trained.

All data users are responsible for complying with the Data Protection Act and this policy. Failure to comply could lead to disciplinary action.

All employees, volunteers and students must also ensure that any personal data they supply to the Trust is accurate and up-to-date.

Personal Information in the Public Domain

It is considered to be necessary for the Trust's legitimate interests for certain personal information about its staff to be in the public domain. Personal data classified as being in the 'public domain' refers to information which will be publicly available world-wide and may be disclosed to third parties without recourse to the data subject.

The Trust's policy is to make the following items of personal data freely available unless individuals have objected;

- Names of members of the Trust Board and the Boards of Governors
- Names and academic qualifications of academic and of support staff where appropriate
- Staff workplace e-mail addresses and telephone numbers where appropriate
- Any additional information relating to data subjects which they have agreed to be placed in the public domain and which may be in automated and/or manual form

Any individual who has good reason for not wanting his/her work telephone number or email address to be made public may, with agreement from their line manager, specify a department telephone number or email address instead.

The Trust will take reasonable steps as necessary to ensure that personal data not in the 'public domain' are secure from unauthorised or unlawful processing and accidental loss, damage or destruction, will process the data in accordance with the current legislation and the Trust's Data Protection Register entry and will not disclose the information to any unauthorised third party.

Processing Personal Data

In accordance with the Act, Personal data must be processed fairly and lawfully, without adversely affecting the rights of the data subject and individuals should be made aware of how the Trust intends to use their personal data. All students and staff are provided with a Data Protection notice when they join the Trust outlining in general terms how the Trust uses their personal data.

For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the Act. These include:

- The data subject has given consent to the processing;
- The processing is necessary for the performance of a contract to which the data

subject is a party;
- It is necessary for the compliance with any legal obligation to which the Trust is subject;
- It is necessary in order to protect the vital interests of the data subject;
- It is necessary for the administration of justice;
- It is necessary for the purposes of legitimate interests of the Trust or a third party.

Where sensitive personal data is being processed, additional conditions must be met. As a general rule, the Trust will only process sensitive data on the basis of explicit consent of data subjects, in order to protect the vital interests of the data subject or another person or where a legal obligation exists.

Notifying Data Subjects

If we collect personal data directly from data subjects, we will inform them about:

- The purpose or purposes for which we intend to process that personal data.
- The types of third parties, if any, with which we will share or to which we will disclose that personal data.
- The means, if any, with which data subjects can limit our use and disclosure of their personal data.

If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

We will also inform data subjects whose personal data we processes that we are the data controller with regard to that data, and who the Data Protection Officer is.

Transfer to Data Processors and Contractors

We may share personal data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.

We may also disclose personal data it holds to third parties:

A. In the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets.
B. If we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.

If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

Any third party or contractor who has access to personal data and/or is acting as a data processor should be fully aware of their obligations to comply with the Data Protection Act and be contracted to act accordingly.

Personal data will not be transferred to any country outside the European Economic Area (EEA) unless there is adequate protection in place through local data protection laws, organisational policies or contractual arrangements.

Retention and Destruction of Personal Data

We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from its systems, all data which is no longer required. Data users of the Trust should ensure that personal data is destroyed confidentially. Where multiple copies exist all copies should be destroyed in line with the schedule.

Paper records should be shredded or destroyed using the Trust's approved confidential waste process and all electronic equipment used for storing personal data should be fully wiped before disposal, which will be controlled by the IT Department and overseen by the Data Protection Officer.

Security of Personal Data

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

Data users are responsible for ensuring that any personal data which they hold or process is kept secure and not disclosed either orally, or in writing, accidentally or otherwise to any unauthorised third party.

Anyone who becomes aware of any breach of this policy or of the Act should inform the Trust's Data Protection Officer and/or the Director of IT directly.

Further information regarding security measures can be obtained from the Director of IT.

Rights to Access Information

Data subjects have the right to access their personal data which are held by the Trust. Data subjects must make a formal request for information we hold about them in writing.

Employees who receive a written request should forward it to the Data Protection Officer.

Unless a valid exemption exists, this right of access covers all personal information held in electronic format and most paper records with the exception of limited unstructured paper personnel records.

Any data subject who wishes to exercise this right (Subject Access Request) should apply in writing to the Data Protection Officer and the Trust will normally make a charge of unto £10 per request.

Further Information

We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or e-mail.

This policy should be read in line with associated standards, policies and arrangements including:

- **ANY ASSOCIATED INTERNAL POLICIES**
- Information Commissioner's Office - **https://ico.org.uk**
- Data Protection Act 1998 - **http://www.legislation.gov.uk/ukpga/1998/29/contents**