Data Protection Act Policy Statement

Status/Version: 0.1 Review
Information Classification: Unclassified
Effective:

1 Policy Statement Objective

1.1 It is the policy of Penderels Trust to demonstrate compliance in discharging all of its legal obligations in respect of data protection and provide assurance that processing of personal data is in accordance with the Data Protection Act 1998 (DPA).

2 Scope

2.1 This policy statement applies to the following:

i) Penderels Trust employees, including temporary, contractual and agency staff
ii) Trustees, partner agencies, organisations, volunteers, students or any other authorised person contracted or authorised to work or process personal information on behalf of Penderels Trust

2.2 For ease of reference, the term 'data users' will be used throughout this policy to reflect the above.

3 Other Relevant Documents

3.1 The following documents have specific relevance to this policy:

i) Information Security Management Policy
ii) Standards for Information Classification

3.2 Familiarisation with other policies and associated documents supporting Penderels Trust information security management framework, may also need to be taken into account.

3.3 This not an exhaustive list and it is the data user's responsibility to ensure they are aware of Penderels Trust's requirements.

4 Definitions

4.1 Penderels Trust Information Governance Glossary of Terms contains a full list of technical and non-technical terms and their meanings.

5 Risks

5.1 Penderels Trust recognises that there are risks associated with the processing of personal data. This policy statement aims to mitigate risks such as:

i) Loss of customer confidence in Penderels Trust ability to safeguard personal data
ii) Loss of reputation and damage to Penderels Trust corporate image
iii) Ineffective management of information security incidents
iv) Inadequate controls for managing access to, retention and disposal personal data
v) Legal, regulatory or financial penalties

6 Data Controller

6.1 Under the Data Protection Act (DPA), Penderels Trust is the data controller and is responsible for the implementation and monitoring of this policy statement.

7 Data Protection Framework

7.1 A framework of policy, processes, procedures, standards and training material will be established and maintained to support Penderels Trust in meeting its compliance with the Act and its principles outlined below:

i) Personal data will be processed fairly and lawfully and shall not be processed unless specific conditions are met
ii) Personal data will only be obtained for specified and lawful purposes and will not be processed for incompatible purposes
iii) Personal data will be adequate, relevant and not excessive
iv) Personal data will be accurate and kept up to date where necessary
v) Personal data will not be kept longer than is necessary
vi) Personal data will be processed in accordance with the rights of data subjects
vii) Appropriate technical and organisational controls will be applied to protect personal data from unauthorised and unlawful processing and against accidental loss, destruction or damage
viii) Personal data will not be transferred outside the European Economic Area (EEA) if there is inadequate protection

8 Notification

8.1 Penderels Trust will maintain its entry on the Information Commissioner's public register of data controllers.

9 Internal Register

9.1 A register of manual and electronic systems containing personal data will be developed and maintained.

10 Data Subjects' Rights

10.1 Penderels Trust will implement and maintain processes and procedures to support the rights of individuals, namely:

i) How their personal data will be processed
ii) The purpose(s) for which it will be kept and processed
iii) Who the information may be shared with
iv) How to access to information
v) How to request that data processing should cease
vi) How to seek compensation for damage suffered due to Penderels Trust failing to comply with the Act
vii) How to request inaccurate information to be corrected, blocked, erased or destroyed

10.2 The Director of Operations, supported by other suitably qualified staff, will maintain a central register of requests for access to personal data.

11 Exemptions

11.1 Penderels Trust will implement and maintain processes and procedures to support the correct and consistent application of exemptions (reasons not to disclose personal information).

12 Fees

12.1 Penderels Trust will not charge for access to personal data under the subject access regime unless the number of requests from one individual, or the amount of work involved, is considered excessive.

13 Roles and Responsibilities

13.1 The Chief Executive has overall responsibility for DPA within Penderels Trust, however day to day corporate management will be delegated to the Director of Operations

13.2 The Director of Operations will have responsibility for developing, implementing and maintaining corporate policy, processes, procedures, and developing training and awareness material

13.3 The Director of Operations will be supported by 'Departmental Champions,' who will be responsible for helping ensure that requests are processed in line with the Act and Penderels Trust's internal processes and procedures

13.4 The Director of Operations will have access to specialist legal advice from Penderels Trust's external legal advisers and external support as required

13.5 Business areas within Penderels Trust will ensure that their:

i) Regional areas proactively support the Information Commissioner's notification process and Penderels Trust internal register
ii) Line managers within Penderels Trust promote compliance within operational areas
iii) Data users are appropriately trained in the handling of personal data and the rights of data subjects
iv) Data users know how to handle suspected or actual information security breaches
v) Records are maintained in accordance with legislative, regulative and best practice requirements to support the efficient processing of personal data

13.6 Any person (or external organisation) who is authorised to process personal information, for or on behalf of Penderels Trust, must comply with this policy statement and associated documents

13.7 The Director of Operations will clearly define and communicate roles and responsibilities for processing personal data as required.

14 Security and Retention of Personal Data

14.1 Where applicable, privacy impact assessments will be conducted to:

i) Cost effectively identify technical and organisation controls to manage risks
ii) Support and maintain public trust and confidence
iii) Support compliance with the Act

14.2 Personal data will be subject to appropriate classification as outlined in Penderels Trust's Standard for Information Classification

14.3 Manual and electronic records containing personal data will be stored securely

14.4 The retention and disposal of records containing personal data will be in accordance with Penderels Trust's Corporate Retention and Disposal Schedule and Standard for Information Classification

14.5 Suspected or actual breaches of the principles of this Act will be investigated by the Director of Operations or other suitable individual(s), and reported to the Information Commissioners Office (ICO) as appropriate.

15 Training and Awareness

15.1 Penderels Trust will provide appropriate training and awareness for data users during their induction, which will be updated on a regular basis as required.

16 Data Processing and Information Sharing Agreements

16.1 Penderels Trust will develop, implement and maintain a corporate information sharing protocol

16.2 Contractual and/or data processing agreements, which are compliant with this policy, will be established and maintained when an external person or organisation is processing personal data on behalf of Penderels Trust

16.3 Information sharing agreements, which are compliant with this policy, will be established and maintained for multi-agency working when personal data may be shared

17 Preventing and Managing Information Security Incidents

17.1 Data users must immediately report any actual or suspected breaches of information to their line manager and to the Director of Operations.

17.2 Reported incidents will be investigated and reported on by the Director of Operations, or other appropriate members of staff.

17.3 Users must immediately report IT equipment that has been lost or stolen to their line manager and a member of the Business Support Team.

18 Monitoring

18.1 Auditing of Penderels Trust compliance with this policy and supporting framework will be undertaken by a combination of methods, including but not limited to:

- ad hoc quality checks by the Director of Operations
- the use of internal and/or external auditors
- day to day operational activities

19 Legal Requirements

19.1 Data controllers are responsible for information that is held not only on equipment owned by them, but personal equipment that they know is being used by its data users or other authorised people/organisations.

19.2 Consequently the use of privately owned equipment or removable media devices for processing personal data (as defined by DPA) on behalf of Penderels Trust is prohibited unless a Documented Risk Assessment has been undertaken and appropriate controls are implemented to prevent personal data from being stored on non-company owned equipment prior to the processing commencing.

19.3 This policy supports Penderels Trust in fulfilling its legislative responsibilities for information and ICT governance.

19.4 It must be read in conjunction with other relevant information/ICT governance policies and procedures. It also has been based on best practice guidance from 'ISO/IEC 27001: Security Techniques – Code of Practice for Information Security Requirements'.

20 Consequences of Not Following Policy

20.1 Penderels Trust views the protection of data and information security seriously. Compliance with information security policies is monitored and reported on by the Director of Operations, supported by the management team. The nature and particular circumstances of any non-compliance will influence the course of action to be taken which may include disciplinary action. Issues involving Trustee or Executive Board members will be referred to the Chief Executive or Chair of Trustees as appropriate. Third party issues e.g. contractors or third party suppliers will be handled via contractual arrangements etc.

21 Policy Statement Review

21.1 The Director of Operations has direct responsibility for coordinating the maintenance and review of this policy statement and supporting framework. Such documentation is reviewed as a minimum every two years, and may be amended to reflect changes in best practice and lessons learned. Reviews will take into account changes in legislative practices, guidance from the Information Commissioner's Office, and input from specialist areas within Penderels Trust.

22 Notes

22.1 Enquiries regarding this policy statement should be directed to the Director of Operations or in his absence the Chief Executive.

Document Control:

Version History

Version	Status	Date	Author	Summary of Changes
1.0		27 January 2015	Gary Jones	

Reviewers

Name	Role	Business Area

Management Approval

Name	Date	Version No.
Jackie Wakelin	27 January 2015	1.0

Distribution

Name	Organisational Department	Format