****

INFORMATION SECURITY POLICY

ISP-01

|  |  |  |
| --- | --- | --- |
| Issue Date: | 21-04-2020 |  |
| Version: | 2 |  |
| Status: | Approved |  |
| Review Period | Yearly |  |
| Author: | Chris Murphy |  |
| Applies to: | Staff / Volunteers / Contractors / Visitors |  |

Pentreath Ltd is committed to achieving a working environment which provides equality of opportunity and freedom from unlawful discrimination on the grounds of race, sex, pregnancy and maternity, marital or civil partnership status, gender reassignment, disability, religion or beliefs, age or sexual orientation.

If you require this document in other formats or languages please contact the author.

|  |  |
| --- | --- |
| **EQUALITY IMPACT ASSESSMENT** |  |
| Who does the policy affect? | Staff / Clients / Referrers / Public |  |
|  | Yes | No |  |
| 1. Will the proposal have any impact on discrimination, equality of opportunity or relations between groups?  |  | X |  |
| 2. Is the proposal controversial in any way (including media, academic, voluntary or sector specific interest) about the proposed work?  |  | X |  |
| 3. Will there be a positive benefit to the users or workforce as a result of the proposed work?  | X |  |  |
| 4. Will the users or workforce be disadvantaged as a result of the proposed work?  |  | X |  |
| 5. Is there doubt about answers to any of the above questions (e.g. there is not enough information to draw a conclusion)?  |  | X |  |

If the answer to any of the above questions is Yes (other than question 3) or you are unsure of your answers to any of the above you should provide further information using the Equality Impact Assessment form

|  |  |
| --- | --- |
| If an equality assessment is not required briefly explain why: |  |

|  |  |
| --- | --- |
| **DOCUMENT CHANGE HISTORY** |  |
| **Version** | **Date** | **Comments (viewed / reviewed / amended etc)** |  |
| 2 | Mar 2019 | New template, GDPR update |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |
| --- | --- | --- |
| Ratification Body | CEO / SMT / Board of Trustees |  |

**1. INTRODUCTION**

Information is a vital asset to any organisation and the management of personal data has important implications for individuals. This policy is concerned with the management and security of Pentreath’s information assets (an information asset is defined to be an item or body of information, an information storage system or an information processing system which is of value to Pentreath) and the use made of these assets by its members and others who may legitimately process Pentreath information on behalf of Pentreath. This overarching policy document provides an overview of information security and lists a hierarchical set of policy documents (sub-policies) which taken together constitute the Information Security Policy of Pentreath.

**2. PURPOSE AND RATIONALE**

An effective Information Security Policy provides a sound basis for defining and regulating the management of information systems and other information assets. This is necessary to ensure that information is appropriately secured against the adverse effects of failures in confidentiality, integrity, availability and compliance which would otherwise occur.

The documents in the Information Security Policy set apply to:

* all employees, volunteers, and trustees of Pentreath and any others who may process information on behalf of Pentreath.
* all information assets which are owned by Pentreath, used by Pentreath for business purposes or which are connected to any networks managed by Pentreath.
* all information which Pentreath processes, irrespective of ownership or form.

**3. POLICY STATEMENT**

Pentreath is committed to protecting our clients and employees from the potential harm that can be caused by data. We will comply with all regulations and also use a best practice system to minimise the data we use and the exposure of that data to risk.

**4. DEFINITIONS**

* GDPR – General Data Protection Regulation: This is the current European regulation on data security and is put into law in the UK by the Data Protection Act.
* DPA 2018 – Data Protection Act 2018: This sets out how the GDPR applies in the UK and additional elements not covered by the GDPR.

**5. DUTIES AND RESPONSIBLITIES**

Board of Trustees

* To review all policies and ensure they are satisfied they meet the company needs

Senior Management Team

* To ensure the compliance of all staff with the Information Security policy set at all times.
* To identify and report any issues that arise with the policies or compliance.

Compliance Manager

* To maintain awareness of regulation updates
* To keep policies up to date
* To report on Information Security matters to the Board of Trustees at every board meeting

All Staff

* To apply the Information Security policies at all times to protect clients, staff, and Pentreath from coming to harm

***6.* POLICY DETAILS**

The Information Security Policy document set is based on the control guidelines set out in the industry standard ISO 27001.

This top level document lists a set of other sub-policy documents which together constitute the Information Security Policy of Pentreath. All of these documents are of equal standing. Although this policy set should be internally consistent, for the removal of any doubt, if any inconsistency is found between this overarching policy and any of the sub-policies, this overarching policy will take precedence.

Each of the sub-policy documents only contain high-level descriptions of requirements and principles. They do not, and are not intended to include detailed descriptions of policy implementation. Such details will, where necessary, be supplied in the form of separate procedural documents which will be referenced from the relevant, individual sub-policy documents.

All employees, volunteers, and other persons who may handle Pentreath information must be made aware of Pentreath’s information security policies and of any amendments made to them. Individuals must also confirm that they have read and understood these policies and how they apply to the information they handle.

# Information Security Principles

Pentreath has adopted the following principles:

1. Pentreath will process information in a way which minimises the potential harm to individuals.
2. Information will be collected and processed in a clear, open and honest way and Pentreath will notify all data subjects about the purposes and lawful basis for processing.
3. Information will be protected in line with all relevant Pentreath policies and legislation, notably those relating to data protection, human rights and freedom of information.
4. Personal data will be used in a way that is fair. Pentreath will not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.
5. Pentreath will respect the confidential nature of the data we collect and will abide by the Duty of Confidentiality wherever it may apply.
6. Any personal data collection by Pentreath will only be done for purposes which are part of our documented obligations and will be limited to what is necessary to fulfil those obligations.
7. Each information asset will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset.
8. Information will be made available solely to those who have a legitimate need for access.
9. All information will be classified according to an appropriate level of security.
10. The integrity, accuracy and availability of information will be maintained.
11. It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification.
12. Information will be protected against unauthorised access.
13. Personal data will be erased once it is no longer needed for the purpose it was gathered.
14. Compliance with the Information Security policy will be enforced.

**7. MONITORING COMPLIANCE AND EFFECTIVENESS**

Responsibility for the production, maintenance and communication of this top level policy document and all sub-policy documents lies with Pentreath’s Senior Management Team (SMT).

This Information Security policy set has been approved by Pentreath’s Board of Trustees. Substantive changes may only be made with further approval of the Board.

Each of the documents constituting the Information Security Policy will be reviewed annually. It is the responsibility of the Compliance Manager to ensure that these reviews take place. It is also the responsibility of the Compliance Manager to ensure that the policy set is and remains internally consistent.

Changes or additions to the Information Security Policy may be proposed by any member of staff, via the SMT. Any substantive changes made to any of the documents in the set will be communicated to all relevant personnel.

**8. TRAINING AND COMPETENCY REQUIREMENTS**

The Compliance Manager must ensure an awareness of all data processing tasks carried out by Pentreath and must make sure they comply with current legislation. It is expected that all staff should receive Data Security training and have an annual update to support compliance with this policy.

All managers and board members must be kept up to date on governance requirements

**9. ASSOCIATED DOCUMENTS**

# Sub-Policy Document List

|  |  |  |
| --- | --- | --- |
| **ID**  | **Name**  |  |
| ISP-02  | Business Continuity  | This policy will generate a Business Continuity Plan (BCP) to guide Pentreath through any major incidents so that services can be resumed in an effective and timely manner which minimises the negative impact on clients and staff. |
| ISP-03  | Compliance  | This Policy outlines Pentreath’s requirement to comply with certain legal and regulatory frameworks.  |
| ISP-04  | Outsourcing and Third Party Compliance  | This Policy outlines the conditions that are required to maintain the security of Pentreath’s information and systems when third parties, other than Pentreath’s own staff, are involved in their operation.  |
| ISP-05  | Information Handling  | This Policy sets out the requirements relating to the handling of Pentreath’s information assets including confidential data.  |
| ISP-06  | User Management  | This Policy sets out the requirements for the effective management of user accounts and access rights.  |
| ISP-07  | Acceptable Use  | This Policy sets out the responsibilities and required behaviour of users of Pentreath’s information systems, networks and computers.  |
| ISP-08  | System Management  | This Policy sets out the responsibilities and required behaviour of those who manage computer systems on behalf of Pentreath.  |
| ISP-09 | Software Management  | This Policy sets out the principles and expectations for the security aspects of managing software by IT staff and end users where relevant. |
| ISP-10  | Mobile and Remote Working  | This Policy sets out the additional principles, expectations and requirements relating to the use of mobile computing devices and other computing devices which are not located on Pentreath premises when these devices are used to access Pentreath information assets with a classification of confidential or above.  |
| ISP-11  | Encryption  | This Policy sets out the principles and expectations of how and when information should be encrypted.  |
| ISP-12  | Investigation of Computer Use  | This Policy outlines the circumstances in which it is permissible for Pentreath to access the IT accounts, communications and other data of its members |

# Guidance

|  |  |
| --- | --- |
| **Name**  |  |
| Confidentiality |  |
| Data Protection |  |
| ICT |  |
| Internet and Email |  |
| Records Management |  |
| Skype |  |
|  |  |

**10. APPENDICES**

10.1 For the avoidance of any doubt the appendices in this policy are to constitute part of the body of this policy and shall be treated as such.