Information Governance

Description	**Information Governance Policy**
Author	**Sarah Bolton**
Version	**1.1**
Version date	**11th March 2021**

Introduction

This policy applies to the governance of information stored within the hosted environments and with our company network. This includes information relating to:

- Staff and human resources
- Finance, contracts and administration
- Customer data

Principles

We recognise and understand the importance of confidentiality, and the security arrangements to safeguard, personal information and commercially sensitive information.

For the purposes of this document, Information Governance Policy covers:

- Legal Compliance
- Information Security
- Quality Assurance

Responsibilities

This policy applies to all internal staff that have direct or indirect access to data held both onsite and within our hosted environments.

It is the responsibility of each member of staff to ensure that the policy and its supporting standards and guidelines are adhered to.

Legal Compliance

We undertake to assess and audit its own compliance with legal requirements and will establish and maintain policy to ensure compliance with the governing legislation.

We regard all identifiable personal information as confidential except where legislation on accountability and openness requires otherwise.

Integrity

Integrity in information security means that data cannot be modified without prior authorisation; this is not the same thing as referential integrity in databases.

Integrity is violated when an employee accidentally or maliciously deletes important data files, when a computer virus infects a computer, when an employee is able to access or modify their own staff records, and so on.

Availability

For any information system to serve its purpose, the information must be available when it is needed, to those that need it.

This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly.

High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.

Risk management

Risk is the likelihood that something bad will happen that causes harm to an informational asset (or the loss of the asset).

Vulnerability is a weakness that could be used to endanger or cause harm to an informational asset.

A threat is anything that has the potential to cause harm.

The likelihood that a threat will use a vulnerability to cause harm creates a risk. When a threat does use a vulnerability to inflict harm, it has an impact. In the context of information security, the impact is a loss of availability, integrity, and confidentiality, and possibly other losses. It should be pointed out that it is not possible to identify all risks, nor is it possible to eliminate all risk. The remaining risk is called residual risk.

A risk assessment may use a subjective qualitative analysis based on informed opinion, or where reliable monetary figures and historical information is available, the analysis may use quantitative analysis.

Policy

Information Security

ISO 27000 will be the primary reference for designing and implementing information security within Point Progress Limited.

We will establish, develop and maintain policies and procedures for the effective and secure management of its information assets and resources.

We will regularly assess and improve our information and IT security arrangements.

We will promote effective confidentiality and security practice to our staff through policies, procedures and training and establish and maintain incident reporting procedures.

We will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security

Confidentiality

We regard all identifiable personal information relating to service users as confidential.

Our staff will be made aware of their responsibilities at local induction and through policy and training.

Staff noncompliance with legal and regulatory frameworks will be monitored and managed through the company disciplinary procedure.

Risk assessment will be undertaken to determine appropriate effective and affordable information governance controls are in place with respect to new service developments.

Information Quality Assurance

We will establish and maintain policies and procedures for information quality assurance and the effective management of records.

Wherever possible, information quality will be assured at the point of collection.

Data standards will be set through clear and consistent definition of data items.

Assessment and Improvement Plans

An assessment of compliance with requirements will be undertaken annually. The organisation will identify staff to undertake Administration, Reviewer and User roles as appropriate.

Policy Implementation

The policy will be advised during induction and at various points during employment via email and company handbook. Copies of this policy are available on the company network.

Training

As part of their induction, all staff attends a training programme.

Further in-depth training sessions are delivered upon request and tailored to the demands of the staff.

Audit

This policy will be audited in 12 months to qualify the effectiveness of its implementation and staff knowledge and understanding of the content. This will be by random sample.

Version	Date	Description	Approved By
1.0	24/03/2018	Initial Policy Drafted	
	07/01/2019	Policy updated	
	05/03/2020	Policy reviewed – no changes	
1.1	11/03/2021	Policy reviewed and updated to reflect ISO27k	