The JGA Group
Information Security Policy

The Management of The JGA Group, located, Innov8 Vocational Training Centre, Clifton Gardens Uxbridge UB10 0EZ are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout their organisation in order to preserve its competitive edge, cash-flow, profitability, legal, regulatory, contractual compliance and commercial image. Information security requirements will continue to be aligned with The JGA Group's goals, the ISMS is intended to be an enabling mechanism for information sharing, for electronic operations and for reducing information-related risks to acceptable levels.

The JGA Group's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of an ISMS. The Risk Assessment, Statement of Applicability and Risk Treatment Plan identify how information-related risks are controlled. The Head of Risk is responsible for the management and maintenance of the risk treatment plan. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

In particular, business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy. Control objectives for each of these areas are contained in the Manual and are supported by specific documented policies and procedures.

The JGA Group aims to achieve specific, defined information security objectives, which are developed in accordance with the business objectives, the context of the organisation, the results of risk assessments and the risk treatment plan.

All staff of The JGA Group are expected to comply with this policy and with the ISMS that implements this policy in which they will receive training upon

- The consequences of breaching the information security policy are set out in JGA's disciplinary policy and in contracts and agreements with third parties.
- The ISMS is subject to continuous, systematic review and improvement.
- The JGA Group management support the ISMS framework and periodically reviews the security policy.
- The JGA Group is committed to achieving certification of its ISMS to ISO27001:2013.

This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan and at least annually.

In this policy, 'information security' is defined as:

Preserving
This means that management, all full time or part time staff, sub-contractors, project consultants and any external parties have, and will be made aware of, their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches (in line with the policy and procedures identified in Section A16 of the Manual) and to act in accordance with the requirements of the ISMS. All Employees will receive information security awareness training and more specialised staff will receive specialised information security training.

Availability
This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. To protect computer networks during home working all employees are required to ensure all software and virus protection updates are performed automatically and shall be reminded during weekly meetings.

The JGA Group must be able to detect and respond rapidly to incidents such as viruses and other malware that threaten the continued availability of assets, systems and information. In order to ensure continuing availability of business services an in-depth business continuity plan is in place.

Confidentiality
This involves ensuring that information is only accessible to those authorised to access it and therefore to preventing both deliberate and accidental unauthorised access to The JGA Group's information and proprietary knowledge and its systems including its network, website and compliance requirements.

Integrity
This involves safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing accidental or deliberate destruction or unauthorised modification of either physical assets or electronic data.

The JGA Group must ensure that all Office365 accounts are protected by the usage of multifactor authentication.

There must be appropriate contingency including for network, website and data backup plans and security incident reporting. The JGA Group must comply with all relevant data-related legislation in those jurisdictions within which it operates.

The physical (assets)
The physical assets of The JGA Group including, but not limited to, computer hardware, data cabling, telephone systems, filing systems and physical data files.

Information assets
The information assets include information printed or written on paper(use discouraged), transmitted by post, or spoken in conversation, as well as information stored electronically on shared drive, website, PCs, laptops, removeable storage media (use only with specific authorisation), and information transmitted electronically by any means. In this context, 'data' also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc) of The JGA Group.

The ISMS is the Information Security Management System, of which this policy, the Information Security Manual ('the Manual') and other supporting and related documentation is a part, and which has been designed in accordance with the specification contained in ISO27001:2013.

A **SECURITY BREACH** is any incident or activity that causes, or may cause, a break down in the availability, confidentiality or integrity of the physical or electronic information assets of The JGA Group.

Document Owner and Approval

The Information Security Manager is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the requirements in Clause 5.1.2 in the Manual.

A current version of this document is available to all members of staff on the company SharePoint. It does not contain confidential information and can be released to relevant external parties.

This information security policy was approved by the Managing Director (MD) on 27 July 2022 and is issued on a version-controlled basis under the signature of the Managing Director (MD).

Signature:  Date: 27/07/2022

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	R. Goodwin	31/07/2018
2	Review Post Move	R. Goodwin	05/12/2018
3	Pre-Renewal Review	R. Goodwin	01/07/2019
4	Review	R. Goodwin	05/02/2020
5	Corona Virus Measures Review	R. Goodwin	24/03/2020
6	Pre-Renewal Review	R. Goodwin	27/07/2020
7	Pre-Renewal Review	R. Goodwin	20/07/2021
8	Pre-Renewal Review	R. Goodwin	27/07/2022