STAFF IT POLICY

1 – Policy Overview

1.1 – Policy Scope

This policy applies to:

- All Employees within Projecting Success
- Subcontractors employed by Projecting Success
- Clients working with Projecting Success

1.2 – Policy Statement

This policy is designed to provide a set of guidelines and procedures that all employees must follow to ensure the secure handling of sensitive and confidential data and information with Projecting Success. This policy will help to protect against data breaches, unauthorised access to sensitive information, and other security threats.

2 – Staff IT Usage

2.1 – Security Awareness Training

Staff must attend the quarterly mandatory data security training which should be added to the employees CPD log. Where staff are unable to attend, they must communicate this with both the Information Security Manger or Data Protection Officer and follow up by watching the recording within a week after the training event.

Staff are required to complete the data security quizzes when instructed to. Where the score is below the required score (75%), staff will be required to attend a mandatory refresher data security training session to be organised by the ISM OR DPO.

2.2 – Wi-Fi

Staff should avoid using public Wi-Fi where at all possible If public Wi-Fi must be used, then a VPN should be installed and used The VPN software should be checked for potential updates and updated where necessary before using public Wi-Fi to prevent any cyber-attacks. Public Wi-Fi includes the use of personal or company mobiles as 'hot-spots; where no public wi-fi is accessible.

When working from home, staff should reset their router's password every three months, using a strong password. Ensure the routers firmware is kept up to date and use a VPN if your router can be accessed by many people, for example if in a house share. A strong password consists of the following characteristics:

- Length (minimum of 12 characters)
- A mix of letters (upper and lower case)
- Numbers
- Symbols
- No ties to your personal information
- No dictionary words**.**

2.3 – Emails

Staff must not use emails as a way of sending sensitive or confidential information, particularly where not encrypted nor password protected. Alternatively, staff should follow the appropriate methods of sharing data, as discussed below in this policy. When copying an email to multiple individuals which includes external clients, staff must use BCC feature rather than CC to avoid revealing email addresses which contain personally identifiable information.

2.4 – Sharing Data

When sharing data staff must not share locally stored copies of data and instead use SharePoint links which appropriate permissions included. SharePoint links can be generated to share data internally and staff should ensure that when sharing data, it is only shared with individuals who need to access it and limit their access to only the information they require.

When sharing data externally, staff must avoid sending local/hard copies and utilise the SharePoint Extranet site. Folders can be set up by contacting True MSP, and appropriate permissions can be implemented upon request. Again, staff should ensure that when sharing data, it is only shared with those who have a clear and demonstratable need to access it and limit their access to only the information they require.

2.5 – Storing Data

Staff should not store any data on their local drives unless specifically instructed to by management. Staff should not be using the OneDrive feature to store data except for the CEO.

Staff should utilise cloud storage, such as Azure-based systems or SharePoint to store data and use the online editors within O365 to edit documents and collaborate. When using online editors, it is possible to open the document within the Desktop app, which is perfectly acceptable.

2.6 – Third Parties

In some cases, organisations are required to trust third parties with their sensitive data, whether they are vendors, suppliers, or business associates. If one of these third parties were to experience a data breach, the sensitive data they have access to (or store) could be exposed to the public or malicious actors. To restrict the possibility of a cyber-attack which could potentially expose sensitive data, employees must not use third party websites for technical tasks. Examples of such websites include but are not limited to - online data conversion tools, file format validators, regex testers or web-based machine learning platforms to upload sensitive data.

If you wish to install and software or use outsourced suppliers, please contact the Information Security Manager and Data Protection Officer so the appropriate procedures and risk assessments can be carried out.

2.7 – Best Practices:

Staff should follow the Best Practice guide, found in the Whole Teams Resources, to ensure compliance with data security best practices. Where there are any questions, staff should seek guidance from the information security manager.

2.8 – Compliance:

Management is required to enforce this policy. The implications of breaching this policy are potentially extremely severe. Any employees found to have violated this policy may be subject to disciplinary action up to and including termination of employment.

Version History				
Date	Version	Details of Change	Revision By	QA
21/12/2022	1	- Document Created	Tallulah Carter-Kelly	Greg Williams
15/03/2023	1.1	- Comments & revisions suggested	Greg Williams