

Information Security and Data Protection Charter

The delivery of product, service and client satisfaction is the prime objective of Principle and its employees; in order to achieve this in a secure and safe manner, we employ the following information security and data protection principles:

It is the policy of Principle that:

- All information is exchanged securely and treated responsibly.
- Industry best practice is applied to information security handling and storage.
- Auditable policies and procedures are in place to verify handling and storage.
- At a minimum, all legislative requirements for data handling are adhered to.

The purpose of this Charter is to outline our commitment to achieving good governance of information and to handle it responsibly and securely.

INFORMATION SECURITY COMMITMENTS	
We understand our risks	We understand the information security and data protection risks associated with our offering and have implemented appropriate mechanisms to assure a first class service to Principle.
General Commitment	We are committed to ensuring that information handled and exchanged between us is done so securely, responsibly and in accordance with appropriate legislation. Our Senior Managers will lead our approach ensuring that we have the arrangements in place to achieve our aims.
Systems	We have arrangements in place to understand requirements, have auditable controls in place and comply with all legal requirements for information storage, handling and exchange, specifically including the handling of personal data.
We are trained & competent	Our employees are appropriately trained and competent with the necessary industry expertise to carry out their role and understand the requirements of good data governance.
Sub-contracting	We will not sub-contract any service further down the supply chain without the written approval from Principle, as we understand that this introduces additional risk. Where necessary, we will ensure appropriate commercial and legal contracts are in place to enforce and ensure understanding of risk in the context of information security and data protection.
Management of Sub-contractors	We shall evaluate our suppliers prior to any order being placed to ensure they can meet our specifications and support our commitment to good data handling, governance and control.

INFORMATION SECURITY COMMITMENTS

Storage	We have suitable storage conditions to maintain the confidentiality, integrity and availability of our data and understand the processes of risk and breach notifications.
We will resolve issues when something goes wrong	<p>By understanding our risks and responsibilities, we have appropriate arrangements in place to resolve issues such as data breaches, corruption or loss of information. If something goes wrong:</p> <ul style="list-style-type: none"> • We understand that by needing to put things right we have not achieved our commitment to you and so rectification will be at our cost. • We shall take appropriate action to assess the magnitude of the problem and report immediately to Principle's Data Controller. • Where necessary, we will ensure legislative data protection compliance is met by notifying any necessary statutory body within prescribed time limits.
We will keep records	<ul style="list-style-type: none"> • We will maintain adequate internal records to ensure compliance with our obligations. In the event of any pending or threatened legal or regulatory proceeding we will not destroy any relevant records. • Where a legislative body is contacted, we will ensure that full compliance with any requests they or we make, is undertaken without delay.
We fully support audit and inspection	We agree to periodic audits and inspections as we understand the importance of working together to identify areas that require improvement. We shall work with Principle to ensure that root causes of any non-conforming data handling or storage processes are understood so we can continually improve our offering.
We fully support continuous improvement	Only by reviewing our performance and sharing information can we continue to improve and share best practice.

We accept and agree to work to this charter and we will communicate it to our employees

Name	
Signed	
Position	
Date	