INFORMATION SECURITY AND GOVERNANCE POLICY

1. Introduction

This Policy Document encompasses all aspects of security surrounding confidential company and customer information and must be distributed to all company employees. All company employees must read this document in its entirety and sign to say they have read and understand this policy fully via our Breathe HR Portal. This document will be reviewed and updated by Management on an annual basis or when relevant to include newly developed security standards into the policy and distribute it all employees and contracts as applicable.

2. Information Security Policy

Intuitive Thinking Skills handles sensitive customer information daily. Sensitive Information must have adequate safeguards in place to protect it, to protect customer privacy, to ensure compliance with various regulations and to guard the future of the organisation.

Intuitive Thinking Skills commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end management are committed to maintaining a secure environment in which to process customer information so that we can meet these obligations.

Employees handling sensitive customer data should ensure they:

- Handle Company and customer information in a manner that fits with their sensitivity;
- Limit personal use of Intuitive Thinking Skills information and telecommunication systems and ensure it doesn't interfere with your job performance;
- Do not use e-mail, internet and other Company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;
- Do not disclose personnel information unless authorised;
- Protect customers personal and sensitive information;
- Keep passwords and accounts secure;
- Request approval from management prior to establishing any new software or hardware, third party connections, etc.;
- Do not install unauthorised software or hardware, including modems and wireless access unless you have explicit management approval;
- Always leave desks clear of sensitive customer data and lock computer screens when unattended;
- Never leave equipment or documents in view within an unoccupied vehicle and always remove and equipment or documents from vehicle overnight
- Information security incidents must be reported, without delay, to the individual responsible for incident response locally – and to the company Data Protection Officer

We each have a responsibility for ensuring our company's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from your line manager.

Please note, the company reserves the right to monitor, access, review, audit, copy, store or delete any electronic communications, equipment and network traffic for any purpose.

3. Acceptable Use Policy

The Management's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Intuitive Thinking Skills established culture of openness, trust and integrity. The company is committed to protecting the employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Intuitive Thinking Skills provide all IT technologies and devices to staff, detailed and issued through the asset register, and staff are not permitted to utilise personally provided hardware and/or software solutions in any circumstance. Use of any unauthorised technologies is covered in our disciplinary procedure.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should take all necessary steps to prevent unauthorized access to confidential data which includes all customer data.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature.
- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- Because information contained on portable computers is especially vulnerable, special care should be exercised. Other than to scan documents onto the network, no customer data WHATSOEVER should be saved to your laptop or other portable device
- Postings by employees from a Company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Intuitive Thinking Skills, unless posting is in the course of business duties.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
- Paper documents containing personal data or sensitive company information must be transported safely and securely and never left in view in unattended vehicles and removed overnight. Paper documents should be scanned at the earliest opportunity, saved to the network drive and destroyed securely

4. Disciplinary Action

Violation of the standards, policies and procedures presented in this document by an employee will result in disciplinary action, from warnings or reprimands up to and including termination of employment. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for non-compliance.

5. Protect Stored Data

Stored data is any data on hard copy paperwork or electronically stored files.

Intuitive Thinking Skills and its employees must securely protect data against unauthorised use at all times.

It is strictly prohibited to store:

1. The contents of the payment card magnetic stripe (track data) on any media whatsoever.
2. The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever.
3. The PIN or the encrypted PIN Block under any circumstance
4. Learner data generated from ANY contract within the Home Office or DWP, either as a prime contractor or sub-contractor. Data generated under these contracts have specified security protocols which must be followed accordingly.

6. Information Classification

Data and media containing data must always be labelled to indicate sensitivity level:

- **Confidential data** might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to Intuitive Thinking Skills if disclosed or modified. **Confidential data includes customer data**.
- **Internal Use data** might include information that the data owner feels should be protected to prevent unauthorized disclosure;
- **Public data** is information that may be freely disseminated.

7. Access to the sensitive customer data

All Access to sensitive customer data must be controlled and authorised. Any Job functions that require access to customer data should be clearly defined.

- Any display of the card holder should be restricted at a minimum of the first 6 and the last 4 digits of the customer data.
- Access to sensitive customer information such as PAN's, personal information and business data is restricted to employees that have a legitimate need to view such information.
- No other employees should have access to this confidential data unless they have a genuine business need.
- If customer data is shared with a Service Provider (3rd party) then a written information sharing agreement that includes an acknowledgement is in place that the Service Provider will be responsible for the customer data that the Service Provider processes.
- Intuitive Thinking Skills will ensure that a there is an established process including proper due diligence is in place before engaging with a Service provider or supplier
- The company will have a process in place to monitor the DSS compliance status of the Service provider.

8. Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining personal or sensitive data.

- Media is defined as any printed or handwritten paper, received faxes, back-up tapes, computer hard drive, database etc.
- Media containing customer personal or sensitive information must be handled and distributed in a secure manner by trusted individuals.
- Visitors must always be escorted by a trusted employee when in areas that hold sensitive customer information.
- Procedures must be in place to help all personnel easily distinguish between employees and visitors, especially in areas where customer data is accessible. "Employee" refers to full-time and part-time employees, temporary employees and personnel, and consultants who are "resident" on Intuitive Thinking Skills sites. A "visitor" is defined as a learner, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- All computers that store sensitive customer data must have a password protected screensaver enabled to prevent unauthorised use.

9. Protect Data in Transit

All sensitive customer data must be protected securely if it is to be transported physically or electronically.

- Card holder data (PAN, track data etc) must never be sent over the internet via email, instant chat or any other end user technologies.
- If there is a business justification to send customer data via email then it should be done after authorization and by using a strong encryption mechanism compliant with specific contract stipulations.
- The transportation of media containing sensitive customer data to another location must be authorised by management, logged and inventoried before leaving the premises. Only secure delivery services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.
- If media is being transported in a company or personal vehicle it must never be left unattended in view and must be removed from the vehicle overnight.

10. Disposal of Stored Data

- All data must be securely disposed of when no longer required by Intuitive Thinking Skills, regardless of the media or application type on which it is stored.
- An automatic process must exist to permanently delete or put beyond use on-line data, when no longer required.
- All hard copies of customer data must be manually destroyed as when no longer required for valid and justified business reasons. A quarterly process must be in place to confirm that all non-electronic customer data has been appropriately disposed of in a timely manner.
- Intuitive Thinking Skills will have procedures for the destruction of hardcopy (paper) materials. These will require that all hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed.
- Intuitive Thinking Skills will have documented procedures for the destruction of electronic media. These will require:
    - All customer data on electronic media must be rendered unrecoverable when deleted e.g. through degaussing or electronically wiped using military grade secure deletion processes or the physical destruction of the media;
    - If secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion.
- All customer information awaiting destruction must be held in lockable storage containers clearly marked “To Be Shredded” - access to these containers must be restricted.

11. Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into company practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and contractors.

- Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day to day company practice.
- Distribute this security policy document to all company employees to read. It is required that all employees confirm that they understand the content of this security policy document by signing the induction checklist. Training is then refreshed annually to ensure new revisions and/or new procedures are communicated across all staff.
- All employees that handle sensitive information will undergo background checks (such as criminal and credit record checks, within the limits of the local law) before they commence their employment with the company.

- All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS).
- Company security policies must be reviewed annually and updated as needed.

12. Security Management / Incident Response Plan

Employees of the company are required to report to the Data Protection Officer for any security related issues. The role of the Data Protection Officer is to effectively communicate all security policies and procedures to employees within the company and contractors. In addition to this, the Data Protection Officer will oversee the scheduling of security training sessions, monitor and enforce the security policies outlined in both this document and at the training sessions and finally, oversee the implantation of the incident response plan in the event of a sensitive data compromise.

Incident Response Plan

1. In the event of a suspected security breach, alert the Data Protection Officer or your line manager immediately.
2. The Data Protection Officer will carry out an initial investigation of the suspected security breach.

Once confirmed all data breach and information security incidents must be responded to as set out in the Data Breach and Information Security Incident policy and procedure

If the data security compromise involves credit card account numbers, implement the following procedure:

- Shut down any systems or processes involved in the breach to limit the extent, and prevent further exposure.
- Alert all affected parties and authorities such as the Merchant Bank (your Bank), Visa Fraud Control, and the law enforcement.
- Provide details of all compromised or potentially compromised card numbers to Visa Fraud Control within 24 hrs.
- For more Information visit: https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf

I agree to the below agreement below which I have read, understood and signed on ITS Breathe HR poratal.

I agree to take all reasonable precautions to assure that company internal information, or information that has been entrusted to the company by third parties such as customers, will not be disclosed to unauthorised persons. At the end of my employment or contract with the company, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal manager who is the designated information owner.
I have access to a copy of the Information Security Policies, I have read and understand these policies, and I understand how it impacts my job. As a condition of continued employment, I agree to abide by the policies and other requirements found in the company security policy. I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties.
I also agree to promptly report all violations or suspected violations of information security policies to the designated security officer.

List of Service Providers

Name of Service Provider	Contact Details	Services Provided	PCI DSS Compliant	PCI DSS Validation Date
Xperience	See SharePoint	Microsoft 365 backup and monitoring OfQual	Yes	18/12/2025
NOCN	See Dynamics	Accreditation body	Yes	01/08/2025 – 31/07/2026
Santander	Restricted	Company Banking	Na	na