Information Security Policy

Company Overview

Company name	HENWICK PROPERTIES
Who are the Directors?	PARTNERSHIP
Site address	3 HIGH STREET THATCHM RG19 3JG
Overview of business activities	PROPERTY MANAGERS
Who is responsible for Information Security?	GARRYKAXE
Does this person have appropriate authority and resources?	YES

Physical Security

Description of building	**TWO STOREY OFFICE**
What are the points of access to your building?	**FRONT AND REAR DOORS**
How is access controlled and how are visitors supervised?	**ACCESS THROUGH ALL DOORS MONITORED AT ALL TIMES**
Who has access to the building and equipment who is not from our organisation? (e.g. Cleaner, IT support)	**CLEANERS**
What is the quality of our doors and locks and is there any additional protection i.e. entry systems, security cameras, CCTV?	**ALARM**
How do we dispose of paper waste?	**CONTROLLED DISPOSAL THROUGH GRUNDONS**
What is our policy on locking filing cabinets?	**LOCKED WHEN OFFICE IS CLOSED**
What is our policy on desk diaries, physical documents on desks and visibility of PC or device screens to members of the public?	**PC LOCKS AFTER 5 MINS**
How often do we test our systems and policies?	**ONCE A YEAR**

Staff

Staff may commit a criminal offence if they access or disclose data without authority.

Training and policy demonstration

How many staff do we have?	**5**
Do we provide data protection training to all staff?	**YES**
Who has the ability to access, alter, disclose and delete data and how do we ensure that those people only act within the scope of the authority we give them?	**ONLY THE CONTOLLER CAN ALTER INFORMATION ON THE DATA BASE**

What are our procedures to identify phone callers providing personal information?	**A WRITTEN NOTE IS PLACED ON THE FILE AND DETAILS ENTERED INTO THE DATABASE**
What is our policy concerning email usage including bulk emails and email forwarding?	**EMAILS ARE ACCESSED AND CHECKED ON A REGULAR BASIS**
What is our policy on personal use of our systems to prevent viruses and spam?	**NO PERSONAL USE IS ALLOWED**
What is our policy concerning homeworking and what measures can we put in place to ensure this does not compromise security?	**ONLY THE ADMINISTRATOR CAN ACCESS REMOTELY**
What is our policy on mobile device security including staff personal devices such as tablets, phones, laptops, memory sticks?	**WE DO NOT ALLOW DATA TO BE COPIED FROM THE OFFICE**
How have we trained our staff to recognise the danger of deception, recognition of phishing attacks and complying with a request to change data when they should not do so?	**ALL STAFF HAVE ATTENDED APPROPRIATE COURSES**
How do we demonstrate that our staff and new staff have been given information security training?	**THEY WILL UNDERGO AN INDUCTION DAY**
How often do we carry out refresher training and how do we evidence this?	**IT WILL BE UNDERTAKEN GOING FORWARD**

Employee leaver checklist

If we wish an employee to work their notice, do we restrict their access whilst on notice?	**YES**
Change passwords on PC and devices.	**YES**
Remove access to the bank.	**THEY DO NOT HAVE IT**
Change office entry code, change lock	**NO**
Close email and change website passwords	**YES**

IT Security

Do we have a plan for cyber resilience including anti-virus, malware protection and software updates integrated into our systems?	**YES**
What are our data backup and offsite backup arrangements?	**A HARD COPY DRIVE IS REMOVED EVERY EVENING FROM THE PREMISES**
What is our policy for storage of emails incl: inbox; sent items; deleted folder; archive?	**EMAILS NO LONGER REQUIRED ARE DELETED**
How frequently do we require passwords to be changed?	**ONLY WHEN NECESSARY**
How is our internet connection protected?	**VIRUS SOFTWARE**
Are our website and other applications secure?	**YES**
How do we dispose of electronic waste?	**REMOVAL AND REPLACEMENT**
What are our plans for business continuity and disaster recovery?	**WE HAVE OFF SITE BACKUPS**
Have we considered pseudonymisation or	**NO**

encryption of our data?	

Processors

Have our processors provided sufficient guarantees about their security measures?	**YES**
Have our processors signed our Data Processing Agreement (DPA)?	**NO**
Can our processor make available to us all information necessary to demonstrate their compliance with the GDPR?	**NO**
Have we or a third party had the opportunity to audit this information?	**NO**

Deletions

What is our policy concerning the retrieval or deletion of personal data from a processor?	**WE DELETE IT**