Data Breach Policy

Introduction/Policy statement

Tudor Jones Properties collects, holds and processes personal information and data which has been provided to us by our clients, customers, landlords and tenants. Every care is taken to protect personal information and data from incidents (whether accidentally or deliberately) and to avoid a data protection breach that could compromise personal information and data.

A data breach means a breach of security which can lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. A data breach may result in harm to an individual, reputational damage, financial loss, a loss of confidentiality and integrity of personal data. It is therefore vital that Tudor Jones Properties takes the necessary steps to minimise any associated risks following a data breach.

Purpose and scope

This Data Breach Policy sets out the course of action that will be followed by Tudor Jones Properties in the event of a data breach to ensure a consistent and effective approach in dealing with a data breach. Under the 'General Data Protection Regulation' (GDPR), Tudor Jones Properties are obliged to have in place a policy and framework designed to ensure the security of all personal information and data.

This policy relates to all personal information and data collected, held and processed by Tudor Jones Properties regardless of the format the data is in.

The objective of this policy is to contain any breaches, minimise the risk associated with the breach and to consider what action is necessary to secure personal information and data to prevent further breaches.

Definitions/Types of breach

For the purpose of this policy, data breaches include both confirmed and suspected incidents. A data breach means a breach of security which can lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. A data breach may result in harm to an individual, reputational damage, financial loss, a loss of confidentiality and integrity of personal data. It is therefore vital that Tudor Jones Properties takes the necessary steps to minimise any associated risks following a data breach.

Data protection breaches and incidents of a data breach could be caused by a number of factors and can include, but are not restricted to, the following:

- The loss or theft of personal information and data and/or the loss or theft of equipment on which personal information and data is stored (for example a USB stick, mobile phone, tablet or other electronic device, computer, paper files)
- The failure of such equipment as detailed above
- A system failure
- Unauthorised use, access to or modification of data and/or information systems
- Hacking attack
- Human error
- Cyber attack

- Website defacement
- Unauthorised disclosure of sensitive and confidential data
- Attempts (failed or successful) to gain unauthorised access to information systems
- Phishing emails or phone callers
- Scam email addresses and callers
- A brake in/robbery at our office
- Unforeseen circumstances such as a fire, flood, earthquake etc
- Poor data destruction procedures

Reporting a data breach

Tudor Jones Properties only has one Data Controller due the business being run by a sole trader. As a result of this, the Data Controller is the only person who can discover and report a data breach. If a data breach occurs outside of office hours, the breach will be reported and acted on as soon as is practical.

If a data breach occurs, a report will be written detailing full and accurate details of the breach, when the breach occurred, who is reporting it, if the data relates to people, the nature of the information and how many individuals are involved. As part of the reporting process, a data breach form will be completed and logged.

Managing a data breach, containment and recovery

The Data Controller must ascertain whether the breach is still occurring and if so, steps must be taken to minimise the effect of the breach immediately. The Data Controller will initially assess the severity of the breach and will establish what impact the data breach has had. The Data Controller will also establish if there is anything that can be done to recover any losses and limit the damage the breach could cause/has caused. The Data Controller will establish who may need to be informed of the breach and this could include the Police if illegal activity has occurred.

The Data Controller will quickly take the necessary steps to recover any losses or limit the damage that could occur from a data breach. Steps may include:

- Attempting to recover lost, damaged or stolen equipment
- Contacting the data subjects to inform them of the data breach
- Using back ups to restore/recover any lost, damaged or stolen data
- Contacting the relevant organisations to inform them of a data breach
- If the data breach includes any entry codes or IT system passwords, these passwords will be changed immediately

Investigation

An investigation will be immediately undertaken or at least within 24 hours of the data breach occurring/being discovered by the Data Controller. The Data Controller will investigate the breach and will ascertain and asses the risks associated with the data breach, for example whose data has been compromised, the potential adverse effects on the data subject, how serious or substantial those effects are, how likely they are to occur and what further steps need to resolve the breach.

The investigation will need to take in to account and consider the following:

- The type of data involved
- The sensitivity of the data
- What protections were in place, like for example encryption and passwords
- What has happened to the data, so if it has been lost, stolen or damaged
- Whether the data could be put to any illegal or inappropriate use
- What data subjects and how many data subjects are affected by the breach and the potential effects on those data subjects
- Whether there are any wider consequences to the data breach

A clear, concise and full record of the investigation will be made in regards to the nature of the breach and the actions taken to resolve it. The investigation will be completed as a matter of urgency due to the requirements to report data breaches to the Information Commissioners Office (ICO) if the data breach is significant enough to do so.

Notification

Once the investigation has taken place, individuals and/or agencies will need to be notified of the breach. In the case of significant/severe breaches, the ICO must and will be notified within 72 hours of the breach. Every incident should be considered on a case by case basis however the following will be considered for every data breach:

- Whether the breach is likely to result in a high risk of adversely affecting individuals rights' and freedoms under Data Protection legislation
- Whether notification would assist individuals affected
- Whether notification would help to prevent the unauthorised or unlawful use of personal information and data
- Whether there are any legal and/or contractual notification requirements

Not every incident demands notification and over notification may cause inappropriate and disproportionate enquiries and work.

Where a data breach has occurred and is considered to result in a high risk of adversely affecting individual's rights and freedoms, the individual will be informed without undue delay. When notifying an individual, a full description of how and when the breach occurred and what data was involved will be given and clear advice will be given on what they can do to protect themselves following the breach and what action has been taken to mitigate the risks. Individuals will also be provided with contact details for further information and to ask any further questions on what has occurred following a data breach.

Tudor Jones Properties will consider notifying third parties (to include but not restricted to Police, insurers, banks etc.) if it is appropriate to do so. It would be appropriate to do so where illegal activity is known to or is believed to have occurred or where there is a risk that illegal activity might occur in the future.

A record will be kept, safely and securely, of any data breach regardless of whether notification was required.

Evaluation

As soon as the initial data breach has been contained, Tudor Jones Properties will fully review the causes of the breach, the effectiveness of the response and a review of any changes to systems, policies and procedures will be undertaken to determine their adequacy and whether any corrective action should be taken to minimise the risk of similar incidents occurring again.

Policy Review

This data breach policy may need to be reviewed after a data breach or after legislative changes, new case law or new guidance.

This data breach policy will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments or relevant legislation.

This data breach policy was last reviewed in February 2026.