Acorn to Oaks Financial Services Limited

PERSONAL DATA SECURITY POLICY

Personal Data:
Any information relating to an identifiable person (living individual), who can be directly or indirectly identified by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier.

Sensitive Personal Data:
GDPR refers to sensitive personal data as "special categories of personal data".

The special categories include data relating to: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, health or a natural person's sex life or sexual orientation.

Acorn to Oaks Financial Services Limited holds personal data and recognises that this could be a high value commodity for fraudsters.

In line with Principles 2 & 3 of the FCA's principles for business:

2 skill care and diligence – a firm must conduct its business with due skill, care and diligence;

3. management and control – A firm must take reasonable care to organise and control its affairs responsibly and effectively with adequate risk management systems;

And in accordance with principle 6 of the Data Protection Bill

6. Personal data must be processed in a manner that includes taking appropriate security measures as regards risks that arise from processing personal data. The risks referred to include (but are not limited to) accidental or unauthorised access to, or destruction, loss, use, modification or disclosure of, personal data.

It is **Acorn to Oaks Financial Services Limited's** responsibility to secure customer data.

We have assessed the financial crime risks associated with our customers' data.

As a firm we have put in place systems and controls to counter the risk that the firm might be used to further financial crime.

As a firm we adhere to the requirements of the General Data Protection Regulation (GDPR) and are on the data protection register. This can be checked by visiting https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

Responsibility:
As a firm we take Personal Data Security seriously and have given **Claire Oakley, Managing Director** overall responsibility for the firm's approach to Personal Data Security. This does not diminish each individual's responsibility to ensure that the customer data in their possession is kept secure at all times. As a firm, training is provided to ensure that staff understand their responsibilities and the ultimate risks of a breach of customer data security.

As a firm we recognise that Customer Data Security issues permeate all departments and that it is not restricted to an IT issue.

Security:

We ensure that our premises are secured when unoccupied, and access to the premises is continually monitored with all employees and visitors signing in and out.

The firm has in place physical security to minimise the risk of data theft and/or a break in – for example an Alarm

Visitors are not left unattended with access to Personal Data even when the firm is confident of the visitor's integrity.

Recruitment:

As a firm we are confident that our employees have the integrity to handle Personal Data. The firm undertakes appropriate checks at the point of recruitment and if anything comes to light that questions an employee's integrity the matter is sensitively and promptly reviewed.

Individual Responsibilities:

As a firm we do not leave Personal Data on desks unattended.

Whenever possible, we adhere to a clear desk policy.

We ensure that Personal Data is not shared unnecessarily.

Staff are required to sign and abide by the firm's confidentiality agreement.

The firm encourages staff to raise concerns about customer data security with the Data Protection Champion**,** however insignificant they are felt to be.

The firm only collects the personal information that is needed for a particular business purpose.

Records are updated promptly if information changes (e.g. a change of address).

Personal Data is disposed of in accordance with the firm's Data Retention Policy and in accordance with General Data Protection Regulation once it is no longer required.

We are aware that people may try to trick staff into giving out personal information and therefore identity checks are carried out before releasing personal information to someone over the telephone.

Education and Training:

Training on General Data Protection Regulation is ongoing as the firm recognises the quickly evolving nature of financial and internet crime and the need to ensure that employees awareness on these topics is maintained.

As part of the firm's induction process employees are advised of the importance and relevance of customer data security and are provided with a copy of this policy.

All Staff sign to acknowledge that they have read and understood the firm's Personal Data Security Policy.

IT:

We ensure that each member of Staff has their own user name and password.

We instruct staff not to write passwords down or share them with colleagues.

As a firm we are aware of the importance of strong passwords and the importance of changing passwords regularly.

Staff are advised that passwords must be at least seven characters in length and contain a mix of upper and lower case letters, numbers, and key board symbols.

Staff lock or log off from unattended computer terminals.

Any portable IT equipment issued to an employee is their responsibility and they must do their utmost to keep it safe.

The firm does not permit Sensitive Customer Data to be removed from the premises unless essential.

Staff who work remotely are able to dial into the network and therefore Customer Data is not held on lap tops, memory sticks or CDs.

The IT systems are backed up daily and the data held securely off site.

Data is encrypted.

Any concerns regarding IT and customer data security should be raised immediately with Claire Oakley.

We do not endorse the use of internet based communication sites such as MSN messenger or hotmail. Software is in place to block access to such websites.

Customer data that is removed from the premises is encrypted if it would cause damage or distress if lost or stolen.

To minimise the likelihood of the firm's IT System being hacked into or being affected by a virus, the IT department has installed security software and the firm ensures that this is upgraded regularly.

Disposal of Data:

The firm disposes of Data appropriately depending on its nature / sensitivity.

Our policy is to dispose of data securely and the firm is currently using **Shred-Pro** to dispose of the data.

The firm encourages any concerns that customer data is not being disposed of appropriately to be raised.

Data security Breach Management:

In the event that customer data security is lost or stolen, the matter is to be reported immediately to **Claire Oakley** who will:-

- Contain the security breach and recover data where possible.
- Assess the ongoing risk.
- Notify the persons concerned including the appropriate regulatory body.
- Evaluate the breach and the effectiveness of the firm's response to it.