SECURITY & BREACHES

SECURITY POLICY

Our business has an information security policy supported by appropriate security measures.

We will process personal data in a manner that ensures appropriate security. Before we can decide what level of security is right for us, we assess the risks to the personal data we hold and choose security measures that are appropriate to our needs.

Keeping our IT systems safe and secure can be a complex task and does require time, resource and (potentially) specialist expertise. If we are processing personal data within our IT systems we recognise the risks involved and take appropriate technical and organisational measures to secure the data.

The measures we put in place will fit our business's needs. They are expensive and onerous.

We have established and are implementing a robust Information Security Policy which details our approach to information security, the technical and organisational measures that we are implementing and the roles and responsibilities that our staff have in relation to keeping information secure.

BREACH NOTIFICATION

Our business has effective processes to identify, report, manage and resolve any personal data breaches.

GDPR introduces a duty on all organisations to report certain types of personal data breaches to the ICO and, in some cases, to the individuals affected. A

personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
We will notify the ICO of a breach unless it is unlikely to result in a risk to the rights and freedoms of individuals. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, we will notify those concerned directly and without undue delay.

In all cases we will maintain records of personal data breaches, whether or not they are notifiable to the ICO.

We will report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. GDPR recognises that it will not always be possible to investigate a breach fully within that time-period and allows us to provide additional information in phases, so long as this is done without undue further delay.

We will make sure that our staff understand what constitutes a personal data breach, and that this is more than a loss of personal data.

We will ensure that we have an internal breach reporting procedure in place. This will facilitate decision-making about whether we need to notify the ICO or affected individuals.

In light of the tight timescales for reporting a breach we have a robust breach detection, investigation and internal reporting procedure in place.

INTERNATIONAL TRANSFERS
Our business ensures an adequate level of protection for any personal data processed by others on our behalf that is transferred outside the European Economic Area.

GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations.

These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined. We will only transfer personal data outside of the EU if we comply with the conditions for transfer set out in Chapter V of the GDPR.