Data Controller documentation

**Data Security, international transfers and breaches**

**we have an information security policy supported by appropriate security measures (4.1 )**

Information Security Policy created.

**we have effective processes to identify, report, manage and resolve any personal data breaches (4.2)**

The 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 destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

We only have to notify the ICO of a breach where it is likely 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 must notify those concerned directly and without undue delay.

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

A notifiable breach has to be reported to the ICO within 72 hours of the business becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows us to provide additional information in phases. We should make sure that our staff understand what constitutes a personal data breach, and that this is more than a loss of personal data.

We should ensure that we have an internal breach reporting procedure in place. This will facilitate decision-making about whether we need to notify the relevant supervisory authority or the public.

In light of the tight timescales for reporting a breach - it is important to have robust breach detection, investigation and internal reporting procedures in place.