DATA BREACH POLICY

The General Data Protection Regulation (GDPR) is based around six principles of handling of personal data. We comply with all six principles as a business to ensure that we take good care of your data and meet our legal requirements under the regulations.

The GDPR specifically requires that we must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data. While this is unlikely and we take all possible steps to prevent data breaches this policy sets out how we would respond if a data security breach did occur.

What is a personal data breach?
A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable (for example by a hacker encrypting it or a server going down) and this unavailability has a significant negative effect on individuals.

Role of the DPO
In the event of a security incident or suspected breach, our Data Protection Officer will be notified. They will make decisions about whether there has been a breach, what steps to take and whether the breach is notifiable to the ICO, the data subjects and/or anyone else.

ACTION WE WILL TAKE IN THE EVENT OF A DATA BREACH

1. Containment and Recovery
The immediate priorities will be to:

- contain the breach;
- assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen; and
- limit the scope.

Where personal data has been sent to someone not authorised to see it, the following steps will be taken:

- Immediately inform the recipient not to pass on the relevant information or discuss it with anyone else;
- Inform the recipient to immediately destroy or delete the personal data that they have received and get them to confirm in writing that they have done so;
- Explain to the recipient the implications if they further disclose the data;

- Notiofy the DPO so that they can consider whether it is appropriate to inform the data subjects whose personal data is involved and/or the ICO.

2. Assessing the Risk

On becoming aware of any potential personal data breach, we will make an assessment of potential adverse consequences for the individuals whose personal data is involved, how serious or substantial these are and how likely they are to happen.

When assessing the risk, our DPO will consider the following questions:

What type of data is involved?	
How sensitive is it?	
If data has been lost or stolen, are there any protections in place such as encryption?	
What has happened to the data?	e.g. If the data has been stolen, could it be used for purposes which are harmful to the individuals to whom the data relate? If the data has been damaged, this poses a different type and level of risk
Estimate how many individuals' personal data is affected by the breach	
Who are the individuals whose data has been breached?	Are they staff, customers, clients or suppliers? This may to some extent determine the level of risk posed by the breach and, therefore, our actions in attempting to mitigate those risks
What harm can come to those individuals?	Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
Are there wider consequences to consider such as a risk to public health or loss of public confidence in a service? Is there a risk of reputation damage to the company?	
Is there anything we can do to recover any losses and limit the damage the breach could potentially cause?	

3. Notifying the ICO and individuals, where relevant

The DPO is responsible for notifying the ICO and individuals (where applicable) of relevant personal data breaches.

When a personal data breach has occurred, we need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then we will notify the ICO; if it's unlikely then we don't have to report it.

If we decide we don't need to report the breach, we will justify this decision and document it.

Notifiable breaches will be reported to the ICO without undue delay, but not later than 72 hours after we become aware of it.

If a reportable breach occurs we will provide the following information to the ICO:

- a description of the nature of the personal data breach including, where possible:
    - the categories and approximate number of individuals concerned; and
    - and the categories and approximate number of personal data records concerned;
- the contact details of the DPO;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Where notification to individuals may also be required, the DPO will assess the severity of the potential impact on individuals as a result of a breach and the likelihood of this occurring. Where there is a high risk, we will inform those affected as soon as possible, especially if there is a need to mitigate an immediate risk of damage to them.

The breach need not be reported to individuals if:

- We have implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach such that the data in question no longer identifies individuals;
- We have taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
- It would involve disproportionate effort (in this case a public communication may be more appropriate).

In certain instances, the DPO may need to consider notifying third parties such as the police, insurers, professional bodies, bank or credit card companies who can assist in reducing the risk of financial loss to individuals. The DPO will document all decisions that we take in relation to security incidents and data breaches, regardless of whether or not they need to be reported to the ICO.

4. Evaluate our response and mitigation steps

We will investigate the cause of any breach, decide on remedial action and consider how we can mitigate it. As part of that process we also evaluate the effectiveness of our response to incidents or breaches. To assist in this evaluation we consider:

- What personal data is held, where and how it is stored
- Risks that arise when sharing with or disclosing to others
- This includes checking the method of transmission to make sure it's secure and that we only share or disclose the minimum amount of data necessary
- Weak points in our existing security measures such as the use of portable storage devices or access to public networks
- Whether or not the breach was a result of human error or a systemic issue and determine how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps
- The group of people responsible for reacting to reported breaches of security