CUPAR DEVELOPMENT TRUST

Personal Data Breach Policy 2018

Introduction
The General Data Protection Regulation (GDPR) introduces a duty on all organisations to report certain types of personal data breach to the Information Commissioner's Office ('ICO'). This must be done within 72 hours of CDT becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the individuals concerned ('data Subjects') must be informed without undue delay. A record of any personal data breaches must be kept, regardless of whether it is required to notify.

Policy Statement
CDT is fully committed to compliance with the Data Protection Act (1998), General Data Protection Regulation (GDPR) and Privacy and Electronic Communications Regulations (PECR), and recognises its obligation to document personal data breaches and report certain types of breaches to the ICO.

Aim
This policy sets out CDT's breach detection, investigation and internal reporting procedures to meet the requirements of the legislation. This will facilitate decision-making about whether or not CDT needs to notify the relevant supervisory authority and the affected individuals.

Definitions
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. This includes breaches that are the result of both accidental and deliberate causes. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

When to notify the ICO
When a personal data breach has occurred, the likelihood and severity of the resulting risk to people's rights and freedoms needs to be established. If it is likely that there will be a risk, then the ICO needs to be notified. In assessing risk to rights and freedoms, it is important to focus on the potential negative consequences for individuals, which include emotional distress, and physical and material damage. This should be assessed on a case by case basis. Notifiable breaches must be reported to the ICO no later than 72 hours after becoming aware of it. When reporting a breach, the GDPR states that the following information must be provided:

- a description of the nature of the personal data breach including, the categories and number of individuals concerned; and the categories and number of personal data records concerned;
- the name and contact point where more information can be obtained;
- 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 the measures taken to mitigate any possible adverse effects.

To notify the ICO of a personal data breach, see their pages on reporting a breach:

https://ico.org.uk/for-organisations/report-a-breach/

When to notify the data Subject
If a breach is likely to result in a high risk to the rights and freedoms of individuals, the data Subjects concerned must be inform directly and without undue delay. The nature of the personal data breach needs to be described in clear and plain language; a contact must be named where more information can be obtained; and a description of the likely consequences and measures taken to deal with the personal data breach should be included.

Reporting an incident
All CDT employees are responsible for reporting data breach and information security incidents immediately to the Chair and the Data Manager. If the breach occurs outside working hours, it must be reported as soon as practicable. The report must include a full description of the incident, when is occurred, who is reporting it, what personal data was breached and how many data Subjects are involved. The reporting individual must complete an entry in the Personal Data Security Breach Log.

Containment and risk assessment
The Chair in liaison with the Data Manager will conduct an initial assessment of the severity of the breach, and establish who may need to be notified as part of the initial containment, and inform the police, where appropriate. The Data Manger will investigate whether there is anything that can be done to recover or limit the damage of the breach. They will also assess the risks associated with it and any adverse consequences for individuals, specifically whether there is a high risk of affecting individuals' rights and freedoms under Data Protection legislation.

Notification
The Chair in consultation with the Data Manager will establish whether the Information Commissioner's Office needs to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible; and whether the data Subjects concerned need to be notified.

Evaluation
Once the initial incident is contained, the Data Manager will carry out a full review of the causes of the breach, the effectiveness of the response and whether any changes need to be made to systems, policies and procedures.

Policy Review
This policy was approved by CDT's board on 20th June, 2018 and is operational from that date.

This policy is operational from 20th June 2018 and is due for review in May 2019.

Data Manager
The Company Secretary
Cupar Development Trust
59 Bonnygate
CUPAR, Fife
KY15 4BY