HELOA Data Breach Policy

1. Definition

A breach of personal data as defined by the GDPR means: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

2. Reporting a breach

In the event of a breach occurring, HELOA shall promptly assess the risk to people's rights and freedoms. If the breach is considered likely to involve a risk to these rights and freedoms, the breach must be reported to the ICO without undue delay. This should be within 72 hours of becoming aware that a breach has occurred, wherever possible.

Further details on how to report a breach to the ICO can be found here: https://ico.org.uk/for-organisations/report-a-breach/

3. Informing individuals and keeping records

HELOA will also inform the individuals affected by the breach as soon as possible and keep a clear record of every breach incident, including the facts related to the data breach, its effects, and the remedial action taken.

4. Reporting a serious incident to the Charity Commission

Under charity law, trustees are required to report any serious incident to the relevant charity commission and explain how it is being managed. A serious incident is an adverse event which risks or results in a significant loss of money or assets or harm to the work of the charity, its beneficiaries or reputation.

This is likely to apply to data breaches that involve fraud, hacking, or the theft or loss of data or equipment. Responsibility for making the decision on whether a serious incident report needs to be made lies with HELOA's trustees.

Further details on how to report a serious incident to the Charity Commission for England and Wales can be found here:
https://www.gov.uk/guidance/how-to-report-a-serious-incident-in-your-charity

Further details on how to report a notifiable event to OSCR can be found here:
https://www.oscr.org.uk/managing-a-charity/notifiable-events/