Data Breach Policy

A personal data breach is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This will include breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. It is a security incident that affects the confidentiality, integrity or availability of personal data. Whenever a security incident takes place, it should be quickly established whether a personal data breach has occurred and, if so, promptly take steps to address it, including informing the ICO if required.

The ICO must be informed if the breach has resulted in a risk to people's rights and freedoms; if this is unlikely then it does not have to be reported. However, if the breach has not been reported then the BPA must be able to justify this decision.

In assessing whether a data breach has created a risk to people's rights and freedoms then Recital 85 of the GDPR should be consulted (see Data Breach Document Log for full details).

Data Breach Process

- Data breach should be reported to either the BPA Chairman or BPA Data Protection Officer. Whichever is informed, they will inform the other with immediate effect.
- Immediate action taken to contain the breach.
- Begin completion of the Data Breach Document Log (see below).
- Any actions from the data breach document log carried out.
- Any actions required for the person causing data breach to be carried out, e.g. training.
- Completed data breach document log signed off by Chairman and Data Protection Officer and copies kept by both.

Responsibility

Overall responsibility for this policy and its implementation lies with the board of trustees and the executive committee.

Review

This policy is reviewed regularly and updated as required.

Adopted on: Mar 2019

Last reviewed: May 2020

Signed: …… J Chamberlayne …… Name ……John Chamberlayne……

Position: ……BPA chair……

Data Breach Procedure

Data Breach Procedure

- A data breach should be reported to either the BPA Chairman or BPA Data Protection Officer. Whichever is informed, they will inform the other with immediate effect.
- Immediate action taken to contain the breach.
- Begin completion of the Data Breach Document Log (see below).
- Any actions from the data breach document log carried out.
- Any actions required for the person causing data breach to be carried out, e.g. training.
- Completed data breach document log signed off by Chairman and Data Protection Officer and copies kept by both.

Data Breach Document Log

1. Date of breach	
2. Who caused the breach?	
3. Who was it reported to?	
4. Details of the breach. E.g. • unauthorised access to or disclosure of personal data or confidential BPA information • lost or stolen laptops, smart phones, memory sticks or other IT equipment containing personal data	
4. Has the breach been contained? How?	
5. Does breach fall under Recital 85 of GDPR? ***A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other***	

significant economic or social disadvantage to the natural person concerned. If yes indicate how, and if no indicate why not. If yes go to question 6, if no this form maybe be complete. However, it may be beneficial to complete other parts for reference.	
6. Indicate the categories and the approximate number of individuals concerned; and the categories and approximate number of personal data records concerned. This is to be provided to the ICO.	
7. Indicate the likely consequences of the personal data breach. This is to be provided to the ICO.	
8. 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. This is to be provided to the ICO.	
9. Has the ICO been informed? If yes, please note the date and method of reporting to ICO.	
10. Have the affected individuals been informed? If yes, please note the date and method of reporting to individuals.	

Form completed by

Print name: _____

Signature: _____

Role: _____

Date: _____