Data Breach Policy and Procedure

Kembhill Park Flood Group
Registered Charity: SC047830

Version 1.0 – May 2018

Policy Statement

Kembhill Park Flood Group (Hear after referred to as KPFG) holds a modest amount of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the unlikely event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This breach procedure applies to all personal and sensitive data held by KPFG]. This procedure applies to all Trustees, Committee Members and volunteers, referred to herein after as 'staff'.

Purpose

This breach procedure sets out the course of action to be followed by all office bearers and staff at KPFG if a data protection breach takes place.

Legal Context

The Data Protection Act 1998 and the General Data Protection Regulations EU 2018 makes provision for the regulation of the processing (use) of information relating to individuals, including the obtaining, holding, use or disclosure of such information. Principle 7 of the Act states that organisations which process personal data must take

"appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".

Types of Breach

Data protection breaches could be caused by a number of factors. Some examples are:

- Loss or theft of any personal data and/ or equipment on which data is stored;
- Iappropriate access controls allowing unauthorised use;
- Equipment Failure;
- Human Error;
- Unforeseen circumstances such as fire or flood;
- Hacking;
- Blagging offences where information is obtained by deception.

Immediate Containment/Recovery

In discovery of a data protection breach, the following steps should be followed:

1. The person who discovers/receives a report of a breach must inform the Secretary of KPFG or, in their absence, to the Chairman. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.
2. The Secretary (or nominated representative) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff.
3. The Secretary (or nominated representative) must inform the Chairman and Trustees as soon as possible. As a Data Controller, it is KPFG's responsibility to take the appropriate action and conduct any investigation. However, should the Secretary (or nominated representative) require any expert guidance and assistance; they can contact the Information Commissioners office.
4. The Secretary (or nominated representative) must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.
5. The Secretary (or nominated representative) must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

    1. Attempting to recover lost equipment.
    2. Contacting any other affected parties.

Whatever the outcome, it should be reported immediately to the Chairman (or nominated representative).

    3. The use of back-ups to restore lost/damaged/stolen data.
    4. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.
    5. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

Investigation

In most cases, the next stage would be for the Secretary (or nominated representative) to fully investigate the breach. The Secretary (or nominated representative) should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data;
- Its sensitivity;
- What protections are in place (e.g. encryption);

- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency and, wherever possible, within 5 days of the breach being discovered/reported. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an investigation has taken place. The Secretary (or nominated representative) should, after seeking expert or legal advice, decide whether anyone should be notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) should be notified. Every incident should be considered on a case by case basis. The following points will help you to decide whether and how to notify:

- Are there any legal/contractual requirements to notify?
- Will notification help prevent the unauthorised or unlawful use of personal data?
- Could notification help the individual – could they act on the information to mitigate risks?
- If a large number of people are affected, or there are very serious

consequences, you should notify the ICO. The ICO should only be notified if personal data is involved. There is guidance available from the ICO on when and how to notify them, which can be obtained at: http://www.ico.gov.uk/for_organisations/data_protection/the_guide/~/media/documents/library/Data_Protection/Practical_application/breach_reporting.ashx.

- Consider the dangers of over-notifying. Not every incident warrants notification and over-notification may cause disproportionate enquiries and work.
- The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach.
- When notifying individuals, give specific and clear advice on what they can do to protect themselves and what you are willing to do to help them. You should also give them the opportunity to make a formal complaint if they wish.

Review and Evaluation

Once the initial aftermath of the breach is over, the Chairman (or nominated representative) should fully review both the causes of the breach and the effectiveness of the response to it. It should be written and sent to the next available Management Committee meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources for advice and guidance. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance. Consideration should be given to reviewing this breach procedure whenever the data protection policy is reviewed.

Implementation

The Secretary should ensure that staff are aware of the Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction and supervision. If staffs have any queries in relation to the policy, they should discuss this with the Secretary.