The Knapp Foundation
Registered Charity Number: 1200294

Data breach policy

Introduction

1. The Foundation collects, holds, processes, and shares personal data, a valuable asset that needs to be suitably protected. Every care is taken to protect personal data from incidents (either accidental or deliberate) which would constitute a data protection breach. Such as breach may result in harm to individuals, reputational damage to the Foundation, detrimental effects on our service provision, legislative non-compliance, and/or financial costs.

Scope

2. The Foundation is obliged under Data Protection legislation to have an institutional framework designed to ensure the security of all personal data, including clear lines of responsibility. This policy sets out the procedure to be followed to ensure a consistent and effective approach is taken in managing data breaches and other information security incidents. It relates to all personal and special categories of data held by the Trust regardless of format. It applies to all staff and Trustees, including temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of, the Foundation.

3. The objective of this policy is to contain any breaches, to minimise the risk associated with any breaches and set out the action necessary to secure personal data and prevent further breaches. It will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation.

Types of breach

4. For the purpose of this policy, data security breaches include both confirmed and suspected incidents. An incident is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and which has caused or has the potential to cause damage to the Foundation's information assets and / or reputation. Examples include:

- loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad / tablet device, or paper record);
- equipment theft or failure;
- system failure;
- unauthorised use of, access to, or modification of, data or information systems;
- attempts (failed or successful) to gain unauthorised access to information or IT system(s);
- unauthorised disclosure of sensitive / confidential data;
- website defacement;
- hacking attack;
- unforeseen circumstances such as a fire or flood;

- human error;
- 'blagging' offences where information is obtained by deceiving the organisation which holds it.

Reporting an incident

5. Any individual who accesses, uses or manages the Foundation's information is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer […….]. If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable. The report must include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, whether the data relate to people, the nature of the information, and how many individuals are involved.

6. All staff should be aware that any breach of Data Protection legislation may result in the Trust's Disciplinary Procedures being instigated.

Containment and recovery

7. The Data Protection Officer (DPO) will first determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach. An initial assessment will be made by the DPO in liaison with the Chairman to establish the severity of the breach and agree who will be the Lead Investigation Officer (this will depend on the nature of the breach; in some cases it could be the DPO).

8. The Lead Investigation Officer (LIO) will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause. The LIO will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate. Advice from experts in the Foundation may be sought in resolving the incident promptly. The LIO, in liaison with the relevant Trustees, will determine the suitable course of action to be taken to ensure a resolution of the incident.

Investigation and risk assessment

9. An investigation will be undertaken by the LIO immediately or within 24 hours of the breach being discovered / reported. The LIO will assess the risks associated with it - for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur. The investigation should take into account the following:

i. the type of data involved;
ii. its sensitivity;
iii. the protections in place (e.g. encryptions);
iv. what has happened to the data (e.g. whether it has been lost or stolen);
v. whether the data could be put to any illegal or inappropriate use;
vi. the data subject(s) affected by the breach, including the number of individuals involved and the potential effects on those data subject(s);
vii. whether there are wider consequences resulting from the breach.

Notification

10. The LIO and/or the DPO, in consultation with relevant colleagues, will establish whether the Information Commissioner's Office will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible. The ICO's website contains a self-assessment function which can be used to assess whether notification is required.

11. Every incident will be assessed on a case by case basis. However, the following will always need to be considered:

i. whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under Data Protection legislation;
ii. whether notification would assist the individual(s) affected (e.g. could they act on the information to mitigate risks?);
iii. whether notification would help prevent the unauthorised or unlawful use of personal data;
iv. whether there are any legal / contractual notification requirements;
v. the dangers of over-notifying. Not every incident warrants notification and over-notification may cause disproportionate enquiries and work (see above re the ICO self-assessment tool).

12. Where the answers to the above questions indicate that individuals whose personal data has been affected by the incident should be informed, this should be done without delay. Such notification will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what the individual can do to protect themselves, as well as what action has already been taken to mitigate any risks. Individuals should also be provided with contact details for the Foundation allowing them to access further information or ask questions about the breach.

13. The LIO and/or the DPO must consider notifying third parties such as the police, insurers, banks or credit card companies, and trade unions. 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. The LIO and or the DPO will also consider the need for any press release or other public statement.

14. A record will be kept of any personal data breach, regardless of whether notification was required.

Evaluation and response

15. Once the initial incident is contained, the DPO will carry out a full review of the causes of the breach, the effectiveness of the response(s), and whether any changes to systems, policies and procedures should be undertaken. Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring. The review will consider:

i. where and how personal data is held and where and how it is stored;

ii. where the biggest risks lie, including identifying potential weak points in existing security measures;
iii. whether methods of transmission are secure, sharing the minimum amount of data necessary;
iv. staff awareness;
v. implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

16. If deemed necessary, a report recommending any changes to systems, policies and procedures will be considered by the Managing Trustee.

Adopted by a meeting of the Trustees on 1st February 2023