Data Breach Management Policy

1. Context and overview

Key details

● Policy prepared by:	Jo Pritchard
● Approved by:	Board of Trustees
● Policy became operational on:	20.05.2018
● Next review date:	20.03.2021

Introduction

ThePromise captures personal data about individuals so that we can contact them in relation to our charitable work and process any requests made by them to provide support to this work.

The information captured is stored securely and never shard unless requested to by the individual or for legal purposes.

ThePromise stores this personal data for up to 7 years.

Why this policy exists

Data security breaches are increasingly common occurrences whether these are caused through human error or via malicious intent. As technology trends change and the creation of data and information grows, there are more emerging ways by which data can be breached.

This policy is considered to be a robust and systematic process for responding to any reported data security breach, to ensure ThePromise can act responsibly and protect its information assets as far as possible — and to comply with the law.

The aim and scope of this policy

The aim of this policy is to create a standardised consistent approach to all reported incidents.

It aims to ensure that:

- incidents are reported in a timely manner and can be properly investigated incidents are handled by appropriately authorised and skilled personnel
- appropriate levels of management are involved in response management
- incidents are recorded and documented
- the impact of the incidents are understood and action is taken to prevent further damage

- evidence is gathered, recorded and maintained in a form that will withstand internal and external scrutiny
- external bodies or data subjects are informed as required
- the incidents are dealt with in a timely manner and normal operations restored
- the incidents are reviewed to identify improvements in policies and procedures.

Defining a “data breach”

A data security breach is considered to be “any loss of, or unauthorised access to, data”. Examples of data security breaches may include:

- Loss or theft of data or equipment on which data is stored
- Unauthorised access to confidential or highly confidential data
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- ‘Blagging’ offences where information is obtained by deceit

For the purposes of this policy data security breaches include both confirmed and suspected incidents.

2. People, risks and responsibilities

Policy scope

This policy applies to:

- The head office of ThePromise
- All staff, volunteers and trustees of ThePromise

It applies to all data that the company holds relating to identifiable individuals and includes:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- …plus any other information relating to individuals

Responsibilities

Information users:

All information users are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

The Director is responsible for ensuring staff, volunteers and trustees act in compliance with this policy and assist with investigations as required.

The Director is responsible for overseeing management of the breach in accordance with the Management Plan section of this policy.

Suitable delegation may be appropriate in some circumstances.

Contact Details In the event of an incident or suspected incident are as follows:

Jo Pritchard
Director
jo.pritchard@thepromise.org.uk
07825 512154

Data Classification

Data security breaches will vary in impact and risk depending on the content and the quantity of the data involved, therefore it is important that we can quickly identify the classification of the data and respond to all reported incidents in a timely and thorough manner.

All reported incidents will need to include the appropriate data classification in order for assessment of risk to be conducted. Data classification referred to in this policy means the following approved

Data Categories:

1. Public Data: Information intended for public use, or information which can be made public without any negative impact for ThePromise.
2. Internal Data: Information regarding the day-to-day business and operations of ThePromise.
3. Confidential Data: Information of a more sensitive nature for the business and operations of ThePromise, representing the basic intellectual capital and knowledge. Access should be limited to only those people that need to know as part of their role.
4. Highly confidential Data: Information that, if released, would cause significant damage to ThePromise activities or reputation, or would lead to breach of the Data Protection Act. Access to this information should be highly restricted.

3. Data Security Breach Management

Reporting a Data Security Breach

Reporting Confirmed or suspected data security breaches should be reported promptly to:
Jo Pritchard
Director
jo.pritchard@thepromise.org.uk
07825 512154

The report should include full and accurate details of the incident including who is reporting the incident and what classification of data is involved.

Where possible the incident report form should be completed as part of the reporting process. See Appendix 1.

Once a data breach has been reported an initial assessment will be made to establish the severity of the breach and who the lead responsible officer should be. See Appendix 2.

All data security breaches will be centrally logged by the Director to ensure appropriate oversight in the types and frequency of confirmed incidents for management and reporting purposes.

Data Breach Plan for Management

The management response to any reported data security breach will involve the following four elements. See Appendix 3 for suggested checklist.

A. Containment and Recovery

B. Assessment of Risks

C. Consideration of Further Notification

D. Evaluation and Response

- Each of these four elements will need to be conducted in accordance with the checklist for Data Security Breaches. An activity log recording the timeline of the incident management should also be completed. See Appendix 4.
- Any employee, volunteer or trustee who act in breach of this policy, or who do not act to implement it, may be subject to disciplinary procedures or other appropriate sanctions.
- The Director and board of trustees will monitor the effectiveness of this policy annually and carry out regular reviews of all reported breaches.

References: Information Commissioner: https://ico.org.uk/media/1562/guidance_on_data_security_breach_management.pdf

Appendix 1: Incident Report Form:

Description of the Data Breach:	
Time and Date breach was identified and by whom.	
Who is reporting the breach:	
Name/Role	
Contact details:	
Telephone/Email	
Classification of data breached (in accordance with policy)	
i. Public Data	
ii. Internal Data	
iii. Confidential Data	
iv. Highly confidential Data	
Volume of data involved	
Confirmed or suspected breach	
Is the breach contained or ongoing?	
If ongoing what actions are being taken to recover the data	
Who has been informed of the breach	
Any other relevant information	

The following person should be sent this form by email and made further aware via phone of the matter: **Jo Pritchard, Director – jo.pritchard@thepromise.org.uk 07825 512154**.

Appendix 2: Evaluation of Incident Severity

The severity of the incident will be assessed by the Director and/or a member of the board of trustees. Assessment will be made based upon the following criteria:

High Criticality: Major Incident	**Contact:**
Highly Confidential/Confidential Data ❑ Personal data breach involves > 1000 individuals ❑ External third party data involved ❑ Significant or irreversible consequences ❑ Likely media coverage ❑ Immediate response required regardless of whether or not it is contained ❑ Requires significant response beyond normal operating procedures **Example: database hacked**	**Lead Responsible Officer:** The Director or member of the board of trustees **Other relevant contacts** Governance and Information Compliance Board of Trustees Contact external parties as required ie police/ICO/individuals impacted
Moderate Criticality: Serious Incident	**Contact:**
Confidential Data ❑ Not contained within the company ❑ Breach involves personal data of > 100 individuals ❑ Significant inconvenience will be experienced by individuals impacted ❑ Incident may not yet be contained ❑ Incident does not require immediate response **Example: Incorrect personal data shared with external parties**	**Lead Responsible officer** The Director **Other relevant contacts:** Governance and Information Compliance Board of Trustees
Low Criticality: Minor Incident	**Contact:**
Internal or Confidential Data ❑ Small number of individuals involved ❑ Risk to daily business = low ❑ Inconvenience may be suffered by individuals impacted ❑ Loss of data is contained/encrypted ❑ Incident can be responded to during working hours **Example: Email sent to wrong recipient or loss of encrypted storage device**	**Lead Responsible Officer** The Director **Other relevant contacts:** Director to advise and lead on aspects of containment/recovery Director and/or members of the board of Trustees to follow up on policy procedures for managing personal data breaches

Appendix 3: Data Breach Checklists

A. Containment and Recovery

B. Assessment of Risks

C. Consideration of Further Notification

D. Evaluation and Response

Step	Action	Notes
A	**Containment and Recovery:**	**To contain any breach, to limit further damage as far as possible and to seek to recover any lost data.**
1	Reporting individual to ascertain the severity of the breach and determine if any personal data is involved.	See Appendix 2
2	Director to identify who will be responsible for investigating breach and forward a copy of the data breach report	To oversee full investigation and produce report. Ensure lead has appropriate resources including sufficient time and authority. In the event that the breach is severe, all members of the Board of Trustees will be contacted to lead the initial response.
3	Identify the cause of the breach and whether the breach has been contained. Ensure that any possibility of further data loss is removed or mitigated as far as possible	Establish what steps can or need to be taken to contain the breach from further data loss. Contact all relevant individuals who may be able to assist in this process. This may involve actions such as taking systems offline or restricting access to systems to a very small number of staff until more is known about the incident.
4	Determine whether anything can be done to recover any losses and limit any damage that may be caused	E.g. physical recovery of data/equipment, or where data corrupted, through use of back-ups.
5	Where appropriate, the Director or nominee to inform the police.	E.g. stolen property, fraudulent activity, offence under Computer Misuse Act.
6	Ensure all key actions and decisions are logged and recorded on the timeline.	

Step	Action	Notes
B	**Assessment of Risks**	**To identify and assess the ongoing risks that may be associated with the breach.**
7	What type and volume of data is involved?	Data Classification/volume of individual data etc
8	How sensitive is the data?	Sensitive by virtue of definition within Data Protection Act (e.g. health record) or sensitive because of what might happen if misused (banking details).
9	What has happened to the data?	E.g. if data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk.
10	If the data was lost/stolen, were there any protections in place to prevent access/misuse?	E.g. encryption of data/device.
11	If the data was damaged/corrupted /lost, were there protections in place to mitigate the impact of the loss?	E.g. back-ups/copies.
12	How many individuals' personal data are affected by breach?	
13	Who are the individuals whose data has been compromised?	Donors, staff, volunteers or trustees?
14	What could the data tell a third party about the individual? Could it be misused?	Consider this regardless of what has happened to the data. Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people.

15	Is there actual/potential harm that could come to any individuals?	E.g. are there risks to:
		physical safety;
		emotional wellbeing;
		reputation;
		finances;
		identify (theft/fraud from release of non-public identifiers);
		or a combination of these and other private aspects of their life?

16	Are there wider consequences to consider?	E.g. a risk to public health or loss of public confidence in an important service we provide?
17	Are there others who might advise on risks/courses of action?	E.g. If individuals' bank details have been lost, consider contacting the banks directly for advice on anything they can do to help you prevent fraudulent use.

Step	Action	Notes
C	**Consideration of Further Notification**	**Notification is to enable individuals who may have been affected to take steps to protect themselves or allow the regulatory bodies to perform their functions.**
18	Are there any legal, contractual or regulatory requirements to notify?	E.g.: PGA/ Charity contractual obligations
19	Can notification help ThePromise meet its security obligations under the seventh data protection principle?	E.g. prevent any unauthorised access, use or damage to the information or loss of it.
20	Can notification help the individual?	Could individuals act on the information provided to mitigate risks (e.g. by changing a password or monitoring their account)?
21	If a large number of people are affected, or there are very serious consequences, inform the Information Commissioner's Office (through the Director).	Contact and liaise with the Director and board of Trustees

22	Consider the dangers of ‘over notifying’.	Not every incident will warrant notification “and notifying a whole 2 million strong customer base of an issue affecting only 2,000 customers may well cause disproportionate enquiries and work”.
23	Consider whom to notify, what you will tell them and how you will communicate the message.	There are a number of different ways to notify those affected so consider using the most appropriate one. Always bear in mind the security of the medium as well as the urgency of the situation. Include a description of how and when the breach occurred and what data was involved. Include details of what has already been done to respond to the risks posed by the breach. When notifying individuals give specific and clear advice on the steps they can take to protect themselves and also what ThePromise is willing to do to help them. Provide a way in which they can contact us for further information or to ask questions about what has occurred (e.g. a contact name, telephone number or a web page).
24	Consult the ICO guidance on when and how to notify it about breaches.	Where there is little risk that individuals would suffer significant detriment, there is no need to report. There should be a presumption to report to the ICO where a large volume of personal data is concerned and there is a real risk of individuals suffering some harm. Cases must be considered on their own merits and there is no precise rule as to what constitutes a large volume of personal data. Guidance available from http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_7.aspx
25	Consider, as necessary, the need to notify any third parties who can assist in helping or mitigating the impact on individuals.	E.g. police, insurers, professional bodies, funders, trade unions, website/system owners, bank/credit card companies.

Appendix 4: Timeline of Incident Management

Date	Time	Activity	Decision	Authority