Bishops Frome Village Centre

Data Security – Data Breach Policy

Introduction

This Policy and Plan aims to help Bishops Frome Village Centre (The Centre) Management Committee (The Committee) manage personal data breaches effectively. The Committee holds Personal Data about our users, hirers, contractors, volunteers, suppliers and other individuals for a variety of operational purposes.

The Committee is committed not only to the letter of the law but also to the spirit of the law and places a high premium on the correct, lawful and fair handling of all Personal Data, respecting the legal rights, privacy and trust of all individuals with whom it deals.

A data breach generally refers to the unauthorised access and retrieval of information that may include organisational and/or personal data. Data breaches are generally recognized as one of the more damaging security failures of organizations. They could lead to financial loss, and cause users and the wider community to lose trust in the way the Village Centre is managed.

The regulatory provisions which govern the way The Centre operates require The Committee to make reasonable security arrangements to protect the personal data that we possess or control, to prevent unauthorised access, collection, use, disclosure, or similar risks.

Scope

This policy applies to all committee members and volunteers. You must be familiar with this policy and comply with its terms.

As our Data Protection Officer, Tony Davis has overall responsibility for the day-to-day implementation of this policy.

Familiarisation

The Committee and volunteers will be made aware of this policy. New committee members and volunteers will receive information about this policy as part of their familiarisation into the role.

Personal Data

According to the European Commission, Personal Data is: "any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address."

Generic information that does not relate to a particular individual may also form part of an individual's Personal Data when combined with Personal Data or other information to enable an individual to be identified.

Causes

Data breaches may be caused by The Committee and volunteers and parties external to the organisation, or computer system errors.

Human Error:

Human Error causes include:

- Loss of computing devices (portable or otherwise), data storage devices, or paper records containing personal data

- Disclosing data to a wrong recipient
- Handling data in an unauthorised way (eg: downloading a local copy of personal data)
- Improper disposal of personal data (eg: hard disk, storage media, or paper documents containing personal data sold or discarded before data is properly deleted)

Malicious Activities:

Malicious causes include:

- Hacking incidents / Illegal access to databases containing personal data
- Theft of computing devices (portable or otherwise), data storage devices, or paper records containing personal data
- Scams that trick The Committee or volunteers into releasing personal data of individuals

Computer System Error:

Computer System Error causes include:

- Errors in computer systems used by The Committee
- Failure of cloud services, cloud computing or cloud storage security / authentication / authorization systems

Reporting Breaches

The Committee and volunteers have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority of any compliance failures that are material either in their own right or as part of a pattern of failures

Under the GDPR, the Data protection Officer is legally obliged to notify the Supervisory Authority within 72 hours of the data breach. Individuals have to be notified if adverse impact is determined. In addition, The Committee must notify any affected people without undue delay after becoming aware of a personal data breach.

Where specific information of the data breach is not yet available, The Committee should send an interim notification comprising a brief description of the incident.

Responding to a Data Breach

Upon being notified of a (suspected or confirmed) data breach, The Committee should immediately activate the data breach & response plan.

<u>Data breach management plan</u>

The Committee's data breach management and response plan is:

1. Confirm the Breach
2. Contain the Breach
3. Assess Risks and Impact
4. Report the Incident
5. Evaluate the Response & Recovery to Prevent Future Breaches

Confirm the Breach

The Committee should act as soon as it is aware of a data breach. Where possible, it should first confirm that the data breach has occurred.

Contain the Breach

The Committee should consider the following measures to contain the breach, where applicable:

- Shut down the compromised system.
- Try to recover lost data and limit any damage caused by the breach.
- Prevent further unauthorised access to the system.
- Reset passwords if accounts and / or passwords have been compromised.

Assess Risks and Impact

Knowing the risks and impact of data breaches will help The Committee determine whether there could be serious consequences to affected individuals, as well as the steps necessary to notify the individuals affected.

Risk and Impact on Individuals

- How many people were affected?
  A higher number may not mean a higher risk, but assessing this helps overall risk assessment.
- Whose personal data had been breached?
  Does the personal data belong to users, hirers, community members or minors? Different people will face varying levels of risk as a result of a loss of personal data.
- What types of personal data were involved?
  This will help to ascertain if there are risk to reputation, identity theft, safety and/or financial loss of affected individuals.
- Any additional measures in place to minimize the impact of a data breach? eg: a lost device protected by a strong password or encryption could reduce the impact of a data breach.

Risk and Impact on organizations

- What caused the data breach?

  Determining how the breach occurred (through theft, accident, unauthorised access, etc.) will help identify immediate steps to take to contain the breach and restorepublic confidence

- When and how often did the breach occur?

  Examining this will help The Committee better understand the nature of the breach (e.g. malicious or accidental).

- Who might gain access to the compromised personal data?

  This will ascertain how the compromised data could be used. In particular, affected individuals must be notified if personal data is acquired by an unauthorized person.

- Will compromised data affect transactions with any other third parties?
  Determining this will help identify if other organisations need to be notified.

Report the Incident

The Committee is legally required to notify affected individuals if their personal data has been breached. This will encourage individuals to take preventive measures to reduce the impact of the data breach.

Who to Notify:

- Notify individuals whose personal data have been compromised.
- Notify other third parties such as banks, credit card companies or the police, where relevant.
- Notify GDPR especially if a data breach involves sensitive personal data.
- The relevant authorities (eg: police) should be notified if criminal activity is suspected and evidence for investigation should be preserved.

When to Notify:

- Notify affected individuals immediately if a data breach involves sensitive personal data. This allows them to take necessary actions early to avoid potential abuse of the compromised data.
- Notify affected individuals when the data breach is resolved

How to Notify:

- Use the most effective ways to reach out to affected individuals, taking into
- consideration the urgency of the situation and number of individuals affected.
- Notifications should be simple to understand, specific, and provide clear instructions on what individuals can do to protect themselves.

What to Notify:

- How and when the data breach occurred, and the types of personal data involved in the data breach.
- What The Committee has done or will be doing in response to the risks brought about by the data breach.
- Specific facts on the data breach where applicable, and actions individuals can take to prevent that data from being misused or abused.
- Contact details and how affected individuals can reach The Committee for further information or assistance.

Evaluate the Response and Recovery to Prevent Future Breaches

After steps have been taken to resolve the data breach, The Committee should review the cause of the breach and evaluate if existing protection and prevention measures and processes are sufficient to prevent similar breaches from occurring, and where applicable put a stop to practices which led to the data breach.

Operational and Policy Related Issues:

- Were audits routinely conducted on data security measures?
- Were there weaknesses in existing security measures such as the use of outdated software and protection measures, or weaknesses in the use of portable storage devices, networking, or connectivity to the Internet?
- Were the methods for accessing and transmitting personal data sufficiently secure, eg: access limited to authorized personnel only?

- Is there a need to develop new data-breach scenarios?

Management Related Issues:

- How was The Committee involved in the management of the data breach?

This effect of this policy will be reviewed annually or with changes of legislation

Adopted: 1 Oct 2020

Reviewed: October 2022 by Tony Davis

Next review: Oct 2023

Reviewed: January 2024