

Policy & Procedure

Data Breach Procedure

**October 2020**

Review Date: October 2021

Date of Trustee Approval: 7 October 2020

Table of Contents

[1. Introduction 3](#_Toc485725317)

[2. About this document 3](#_Toc485725318)

[3. What constitutes a data breach 3](#_Toc485725319)

[4. Who do we need to notify immediately 3](#_Toc485725320)

[5. Do we need to notify the authorities 3](#_Toc485725321)

[6. Do we need to notify the individual(s) 4](#_Toc485725322)

[7. What information must a breach notification contain 4](#_Toc485725323)

[8. How to notify a breach 4](#_Toc485725324)

# Introduction

The Society of the Holy Child Jesus stores personal information in respect of Employees, Residents, Sisters, and other third parties in order to conduct its lawful business. We have a duty to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected.

# About this document

This document should be read by all staff. Sections 3 and 4 relate to the actions to be taken by all staff. The remaining sections relate to the actions required by the Province Leader.

# What constitutes a data breach?

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Personal data is any data that can identify and individual, this could be a National Insurance number, a picture, an address. The definition is very broad.

**if you suspect a breach has occurred, or are in any doubt raise this with management team immediately.**

# Who do we need to notify immediately?

If you suspect that a breach has occurred, or are unsure, you must inform the Data Controller immediately. The management will evaluate the potential breach and decide if further action is required, and in particular if the authorities need to be contacted. Management will also coordinate the response.

# Do we need to notify the authorities?

We only have to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

This has to be assessed on a case by case basis. For example, we will need to notify the relevant supervisory authority about a loss of employee details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, would not normally meet this threshold.

If for example, a person’s health records were accessed by an unauthorised person, then clearly this would fit the criteria. On the other hand, if the forename of a staff member was incorrectly entered into the payroll system, this would not represent a breach.

The Information Commissioners Office operates a help line if advice is required in evaluating if a breach should be notified. Call 0303 123 1113.

# Do we need to notify the individual(s)?

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you must notify those concerned directly.

# What information must a breach notification contain?

The nature of the personal data breach including, where possible:

* the categories and approximate number of individuals concerned;
* the categories and approximate number of personal data records concerned;
* The name and contact details of where more information can be obtained;
* A description of the likely consequences of the personal data breach;
* A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

Examples. Category could be employee payroll data, 10 individuals concerned. Category could be client payment records, one individual concerned, 30 payment records.

# How to notify a breach

A notifiable breach has to be reported to the relevant supervisory authority (Information Commissioners Office) within 72 hours of the organisation becoming aware of it. It is recognised that it will often be impossible to investigate a breach fully within that time-period and the authority allows for information to be provided in phases.

If the breach is sufficiently serious to warrant notification to the public, the organisation responsible must do so without undue delay. Since we do not engage in large scale processing of personal data, it is unlikely that it will be necessary to inform the public. Nevertheless, this step should be considered.

Policy Prepared by Alan Budd for Field Lane

Adapted for SHCJ 2018