


# Data Breach Notification Policy and Procedure Manual

*Your Voice in Health & Social Care (YVHSC)*  
45 St Mary's Road, Ealing W5 5RG | 020 3603 2438 | [www.yvhsc.org.uk](http://www.yvhsc.org.uk)

Revision No	Date	Signature
Issue D	14/08/2021	

# DATA BREACH NOTIFICATION POLICY AND PROCEDURE

---

## CONTENTS

1	PURPOSE .....	3
2	SCOPE .....	3
3	POLICY STATEMENT .....	3
4	NOTIFICATION PROCEDURE .....	3
5	RESPONSIBILITIES .....	3
	Compliance, monitoring and review .....	3
	Records management .....	4
6	TERMS AND DEFINITIONS .....	4
7	RELATED LEGISLATION AND DOCUMENTS .....	4
8	FEEDBACK AND SUGGESTIONS .....	5
9	APPROVAL AND REVIEW DETAILS .....	5

---

## **1 PURPOSE**

This policy and procedure establishes an effective, accountable and transparent framework for ensuring compliance with the requirements for data protection impact assessment by the GDPR.

## **2 SCOPE**

This policy and procedure applies across all entities or subsidiaries owned, controlled, or operated by YVHSC and to all employees, including part-time, temporary, or contract employees, that handle personal data.

## **3 POLICY STATEMENT**

Any staff member who suspects that a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data might have occurred, must immediately notify the Data Protection Officer and provide a description of the circumstances. Notification of the incident can be made via e-mail, by telephone, or in person.

The Data Protection Officer will investigate all reported incidents to confirm whether or not a personal data breach has occurred. If a personal data breach is confirmed, the Data Protection Officer will follow the data breach notification procedure based on the criticality and quantity of the personal data involved. For severe personal data breaches, <YOUR COMPANY NAME>'s Executive Team will initiate and chair an emergency response team to coordinate and manage the personal data breach response.

## **4 NOTIFICATION PROCEDURE**

- 4.1 All personal data breaches must be reported immediately to YVHSC's Data Protection Officer.
- 4.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Data Protection Regulator is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.
- 4.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Art 3.2) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.
- 4.4 Data breach notifications shall include the following information:
  - The categories and approximate number of data subjects concerned;
  - The categories and approximate number of personal data records concerned;
  - The name and contact details of YVHSC's Data Protection Officer;
  - The likely consequences of the breach;
  - Details of the measures taken, or proposed to be taken, by YVHSC to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

## **5 RESPONSIBILITIES**

### **Compliance, monitoring and review**

- 5.1 The overall responsibility for ensuring compliance with the requirements of the related legislation in relation to performing Health & Social Care activities at YVHSC rests with the Data Protection Officer.
- 5.2 All operating units' staff that deal with personal data are responsible for processing this data in full compliance with the relevant YVHSC policies and procedures.

## Records management

Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognised YVHSC recordkeeping system.

All records relevant to administering this policy and procedure will be maintained for a period of 5 years.

## 6 TERMS AND DEFINITIONS

**General Data Protection Regulation (GDPR):** the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

**Data Breach:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

**Data Controller:** the entity that determines the purposes, conditions and means of the processing of personal data

**Data Processor:** the entity that processes data on behalf of the Data Controller

**Data Protection Authority:** national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

**Data Protection Officer (DPO):** an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

**Data Subject:** a natural person whose personal data is processed by a controller or processor

**Personal Data:** any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

**Privacy Impact Assessment:** a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data

**Processing:** any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

**Profiling:** any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour

**Regulation:** a binding legislative act that must be applied in its entirety across the Union

**Subject Access Right:** also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

## 7 RELATED LEGISLATION AND DOCUMENTS

- [Regulation \(EU\) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC \(General Data Protection Regulation\)](#)
- YVHSC Data Protection Policy

## 8 FEEDBACK AND SUGGESTIONS

- 8.1 YVHSC employees may provide feedback and suggestions about this document by emailing [info@yvhsc.org.uk](mailto:info@yvhsc.org.uk)

## 9 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Tim Spilsbury – CEO YVHSC
Data Protection Officer	Ian Hughes
Next Review Date	01/08/2022