## MARPLE BRIDGE SURGERY

## Data Breach Notification Policy

## Data breach definition

A data breach is defined as any incident that has affected the confidentiality, integrity or availability of personal data. The Information Commissioners Office (ICO) guidance is available via this [link](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/).

Examples of data breaches include:

* Unauthorized third-party access to data
* Loss of personal data
* Amending personal data without data subject authorization
* The loss or theft of IT equipment which contains personal data
* Personal data being sent to the incorrect recipient

## Reporting the data breach

Any breach that is likely to have an adverse effect on an individual’s rights or freedoms must be reported. In order to determine the requirement to inform the ICO, to notify them of a breach, the data controller is to follow the flow chart in appendix 1.

Breaches must be reported without undue delay or within 72 hours of the breach being identified.

When a breach is identified and it is necessary to report the breach, the report is to contain the following information:

* Organizations details
* Details of the data protection breach
* What personal data has been placed at risk
* Actions taken to contain the breach and recover the data
* What training and guidance has been provided
* Any previous contact with the Information Commissioner’s Office (ICO)

The [ICO data protection breach notification form](https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/) should be used to report a breach. Failure to report a breach can result in a fine of up to [€10 million](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/).

The data controller is to ensure that all breaches at Marple Bridge Surgery are recorded; this includes:

* Documenting the circumstances surrounding the breach
* The cause of the breach; was it human or a system error?
* Identifying how future incidences can be prevented, such as training sessions or process improvements

## Notifying a Data Subject of a Breach

The data controller must notify a data subject of a breach that has affected their personal data without undue delay. If the breach is high risk (i.e. a breach that is likely to have an adverse effect on an individual’s rights or freedoms), then the data controller is to notify the individual before they notify the ICO.

The Primary reason for notifying a data subject is to afford them the opportunity to take the necessary steps in order to protect themselves from the effects of a breach.

When the decision has been made to notify a data subject of a breach, the data controller at ***Marple Bridge Surgery*** is to provide the data subject with the following information in a clear, comprehensible manner:

* The circumstances surrounding the breach
* The details of the person who will be managing the breach
* Any actions taken to contain and manage the breach
* Any other pertinent information to support the data subject

## Recording a Data Breach

The Practice Data Protection Responsible Officer will record the details and the action taken in the Practice Data Processing, Breach and Staff Register.

**Appendix 1**



Signed off by -----------------------------------------------------

Reviewed May 2023

Review Date May 2024