DATA BREACH MANAGEMENT POLICY

Approved and signed by the Board of Trustees

09.02.23

DUE FOR RENEWAL: JAN 2025

NOVEMBER 2020

CHANGES

November 2020	Policy implemented
January 2023	Policy reviewed, no changes made

CONTENTS

1. Introduction.. 4

2. Breach definition.. 4

3. Breach classification 4

4. Breach management 5

5. Escalation points 5

6. Closure 5

Appendix A: Data breach reporting process……………………………...…………………6

Appendix B: ICO escalation matrix for health and social care……………………………………7

1. INTRODUCTION

Discovery MAT is the data controller for a large amount of personal data. If any of this information is subject to a data breach, it should be managed according to best practice, as the Trust will have responsibility for the breach and any consequences with organisations such as the Information Commissioners Office, (ICO).

2. BREACH DEFINITION

A breach is defined as:

- Any event where a person gains access to information or data that they are not authorised to access.
  - This includes information in any format, and breaches where someone's job role does not permit them to access specific information.
- Any event where information (or access to information) is lost and cannot be used for its intended purpose by authorised people.
  - This will include information that has been lost, accidentally deleted and cannot be recovered and information that has become corrupt.
- Integrity breaches are defined as any situation where information has been changed by unauthorised people or actions, rendering the information invalid for the intended purpose.
- Any other event which contravenes the Data Protection Act 2018
  - This will include re-identifying people from data which has had personal details changed to conceal the original identity (pseudonymised) & changing data to prevent disclosure.

3. BREACH CLASSIFICATION

Breaches are classified in the following manner:

- Sensitive electronic data disclosure
- Sensitive paper information disclosure
- Electronic data disclosure
- Paper information disclosure
- Data disclosure near miss
- Other data disclosure
  - This includes breaches involving conversations and voicemail
- Third party breach
- Lost sensitive information
  - Both paper and electronic
- Lost non-sensitive information
  - Both paper and electronic
- Integrity threat
- Storing information past the retention date
- Other DPA18 compromise
  - Failure to conduct DPIA

All partners handling information should use the same classifications for clarity. Sensitive information primarily uses the definition included in the Data Protection Act, which includes racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life. However, for this purpose also includes information about 'children's services interactions, free Trust meal status, pupil premium eligibility, elements of special educational need information, safeguarding information and business processes about such data', as there could be a detrimental impact on those affected.

The difference between electronic disclosure and paper disclosure is the format of the information at the time of the breach.

The Trust also records “Near Miss” events, which is where any data is sent to unauthorised people, however, is retrieved before it is accessed. This enables any lessons learnt to be applied and reduce the number of actual breaches and the impact of breaches as a whole for the organisation.

4. BREACH MANAGEMENT

The best practice breach management process should be used which follows the steps below:

- Identification
    - ❖ The ability to identify a breach. This can be from staff reporting, partner reporting, parent or pupil reporting or other monitoring
- Containment
    - ❖ Preventing any further disclosure
    - ❖ Where possible retrieving any lost data
- Impact analysis
    - ❖ Analysing the breach to determine what the impact will be. This will be an assessment of the impact on the data subject of the particular aspect of the breach
- Notification
    - ❖ Notification according to internal reporting process
        - ▪ For detailed reporting process, please see Appendix A
    - ❖ Notification to any data subjects affected
- Remediation
    - ❖ Identification and implementation of any mitigation that prevents a recurrence

More detailed guidance on the breach management steps can be found in the Trust’s Data Breach Management Procedure.

5. ESCALATION POINTS

All breaches must be escalated immediately to the Data Protection Officer & the Chief Executive Officer. In cases of electronic breaches the ICT department must also be notified immediately so that they can address any system issues. If the breach involves one of our partners, any breach must be reported to their data protection officer or contract manager.

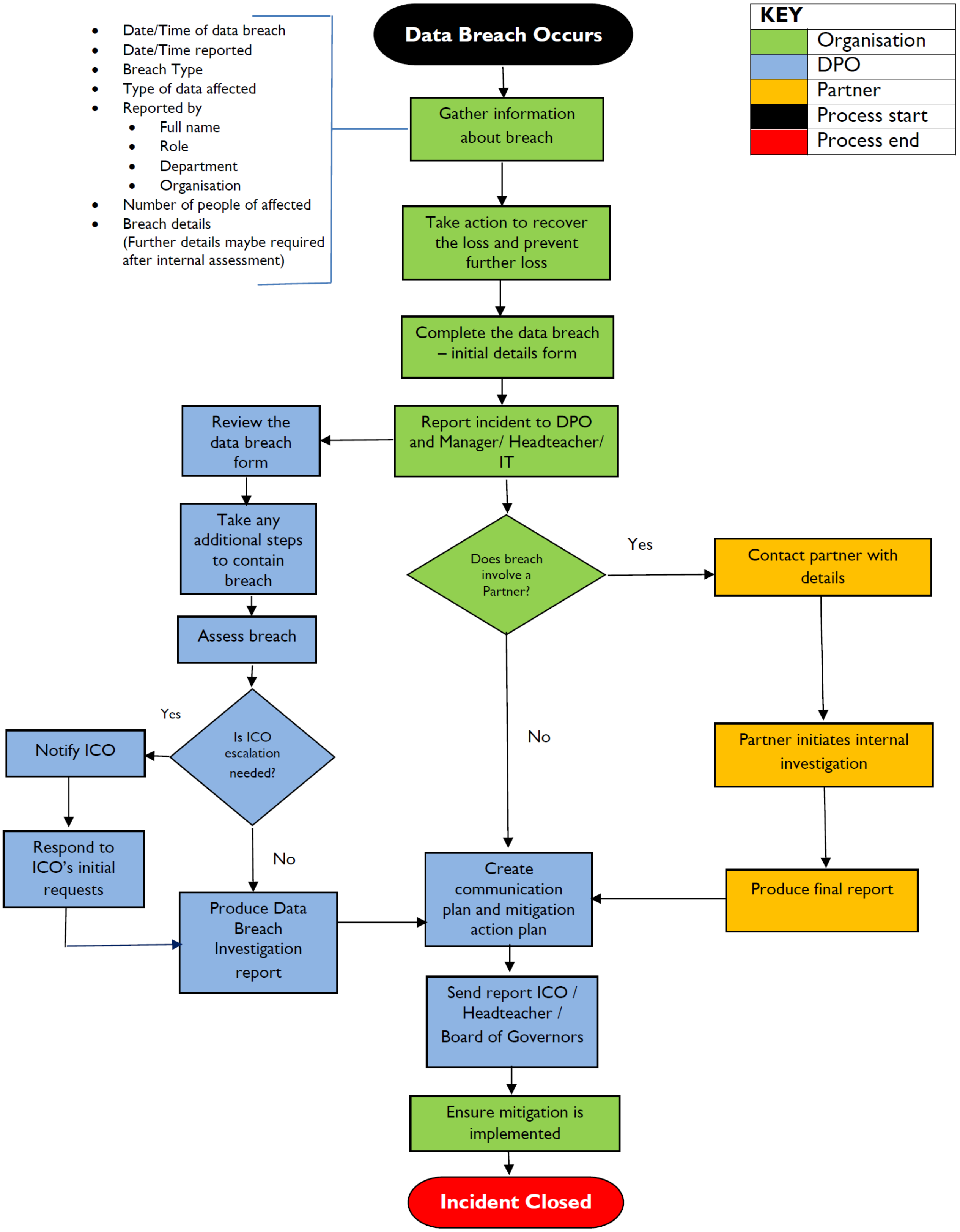
If necessary, the breach will be escalated by the Data Protection Officer to the ICO, using the ICO matrix. An example of the matrix for Health and Social care is in Appendix B, this matrix will be followed by our Trust unless otherwise instructed. In the case of a cyber-compromise, the National Cyber Security Centre & law enforcement will also be notified. Please see the Local Authority Cyber Attacks guidance for handling such matters.

6. CLOSURE

The incident can be closed only on agreement with the Data Protection Officer. This will ensure that both parties are satisfied with the remediation plan, and that any information required for external organisations such as the ICO is provided.

Appendix A

Data Breach Reporting Process



Date/Time of data breach
Date/Time reported
Breach Type
Type of data affected
Reported by
Full name
Role
Department
Organisation
Number of people of affected
Breach details
(Further details maybe required after internal assessment)
KEY
Organisation
DPO
Partner
Process start
Process end
Data Breach Occurs
Gather information about breach
Take action to recover the loss and prevent further loss
Complete the data breach – initial details form
Report incident to DPO and Manager/ Headteacher/ IT
Review the data breach form
Take any additional steps to contain breach
Assess breach
Is ICO escalation needed?
Yes
Notify ICO
Respond to ICO's initial requests
No
Produce Data Breach Investigation report
Does breach involve a Partner?
Yes
Contact partner with details
Partner initiates internal investigation
Produce final report
No
Create communication plan and mitigation action plan
Send report ICO / Headteacher / Board of Governors
Ensure mitigation is implemented
Incident Closed

Appendix B: ICO escalation matrix for Health and Social Care

Stage No	Risk	Stage	Criteria	Value	Score
1	Low	Scale	Less than 10 individuals	0	
1	Low	Scale	11-50 individuals	1	
1	Low	Scale	51-100 individuals	1	
1	Medium	Scale	101-300 individuals	2	
1	Medium	Scale	301-500 individuals	2	
1	Medium	Scale	501-1000 individuals	2	
1	High	Scale	1001-5000 individuals	3	
1	High	Scale	5001-10,000 individuals	3	
1	High	Scale	10,001-100,000 individuals	3	
1	High	Scale	100,001 + individuals	3	
2	Low	Sensitivity Factor	No sensitive personal data (DPA defintion) at risk nor data to which a duty of confidence is owed	-1	
2	Low	Sensitivity Factor	Information readily accessible or already in the public domain or would be made available under access to information legislation	-1	
2	Low	Sensitivity Factor	Information unlikely to identify individual(s)	-1	
2	High	Sensitivity Factor	Detailed information at risk e.g. clinical/care case notes, social care notes	1	
2	High	Sensitivity Factor	High risk confidential information	1	
2	High	Sensitivity Factor	One or more previous incidents of a similar type in the past 12 months	1	
2	High	Sensitivity Factor	Failure to implement, enforce or follow appropriate organisational or technical safeguards to protect information	1	
2	High	Sensitivity Factor	Likely to attract media interest and/or a complaint has been made directly to the ICO by a member of the public, another organisation or an individual	1	
2	High	Sensitivity Factor	Individuals affected are likely to suffer substantial damage or distress, including significant embarrassment or detriment	1	
2	High	Sensitivity Factor	Individuals affected are likely to have been placed at risk of or incurred physical harm or a clinical untoward incident	1	
			Score Total		
			Calculate the score for every factor that is affected by the breach.		
			If Score is above 2, escalate to ICO		