Mosaic Partnership Trust

Data Breach Policy Process (Ref 56MPTDBP)

Data Breach Policy Process (Ref 56MPTDBP)

History of most recent Policy changes

Version	Date	Page	Change	Origin of Change
V1.0	01/02/2024	Whole Document	Adoption by the Mosaic Partnership Trust and Implementation	To support schools in providing clarity through policy on the Data Breach process.

Data Breach Policy Process (Ref 56MPTDBP)

Contents

1	The Data Breach Process	4
2	Immediate Contacts	5
3	Areas to avoid	5

Data Breach Policy Process (Ref 56MPTDBP)

1. The Data Breach Process

For all actual or suspected personal data breaches and near misses

REPORT IMMEDIATELY

Do not wait until all the facts are known. Rapid reporting helps the Trust to contain the incident and protect affected individuals.

1. RECOGNISE

A breach may include information being sent to the wrong person, lost, stolen, accessed without permission, published accidentally, altered, destroyed or made unavailable.

▼

2. REPORT

Notify the Headteacher or relevant senior leader and the Trust Data Protection Lead (Karen Llewellyn) and CEO (Andrew Best) immediately. The incident should then be escalated to the Data Protection Officer (Judicium). Notify the DSL immediately if safeguarding may be involved. The Trust may implement an IMT.

▼

3. CONTAIN

Take safe and proportionate steps to stop further loss or disclosure. Examples include recalling an email, contacting an unintended recipient, removing access, securing records, changing a password, or contacting IT support.

▼

4. RECORD

Complete the Breach Incident Reporting Form. Record what happened, when it was discovered, the information and people affected, action already taken, and any known safeguarding or security concerns.

▼

5. ASSESS

The Trust, supported by the DPO where appropriate and where necessary, the Trust solicitors, assesses the likely risk to individuals. Consider the sensitivity of the information, children or vulnerable people, the recipient, whether the data was protected and possible harm.

▼

6. NOTIFY

Where required and having taken advice from the DPO, the Trust will notify the ICO without undue delay and within 72 hours of becoming aware of the breach. Individuals will be informed without undue delay where the breach is likely to result in a high risk to them.

▼

7. REVIEW AND CLOSE

Record the decision, actions, and outcome in the breach register. Complete remedial actions, identify lessons learned and review procedures, training, systems or DPIAs where necessary.

2. Immediate contacts

Headteacher/relevant senior leader	Report immediately	See school level email
Trust Data Protection Lead/CEO	Escalate immediately	Karen.llewellyn@mosaicpt.org.uk Andrew.best@mosaicpt.org.uk
Data Protection Officer	Seek advice and support with risk assessment	dataservices@judicium.com
Designated Safeguarding Lead	Notify immediately where safeguarding may be involved	See school level email

3. Areas to avoid

- Delay reporting while investigating the incident yourself.
- Delete relevant emails, logs or other evidence.
- Contact affected individuals or the ICO unless authorised to do so.
- Assume that a near miss does not need to be reported.