MANCHESTER
SECONDARY PRU

Data Breach Policy

Date of Adoption: September 2024
Date of Next Review: September 2026

Contents

Policy Statement

Manchester Secondary PRU is committed to the protection of all personal data and special category personal data for which we are the data controller.

The law imposes significant fines for failing to lawfully process and safeguard personal data and failure to comply with this policy may result in those fines being applied.

All members of our workforce must comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary or other action.

About this policy

This policy informs all of our workforce on dealing with a suspected or identified data security breach.

In the event of a suspected or identified breach, MSPRU must take steps to minimise the impact of the breach and prevent the breach from continuing or reoccurring.

Efficient internal management of any breach is required, to ensure swift and appropriate action is taken and confidentiality is maintained as far as possible.

MSPRU must also comply with its legal and contractual requirements to notify other organisations including the Information Commissioners Office ("the ICO") and where appropriate data subjects whose personal data has been affected by the breach. This includes any communications with the press.

Failing to appropriately deal with and report data breaches can have serious consequences for MSPRU and for data subjects including:

- identity fraud, financial loss, distress or physical harm;
- reputational damage to Education Learning Trust and
- fines imposed by the ICO.

Definition of data protection terms

All defined terms in this policy are indicated in bold text, and a list of definitions is included in Appendix 2 to this policy.

Identifying a Data Breach

a. A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

b. This could be the result of a breach of cyber security, such as a hack or virus, or it could be the result of a breach of physical security such as loss or theft of a mobile device or paper records. A data breach includes loss of data and so does not have to be the result of a conscious effort of a third party to access the data. Some examples of potential data breaches are listed below:

- Leaving a mobile device on a train;
- Theft of a bag containing paper documents;
- Destruction of the only copy of a document; and
- Sending an email or attachment to the wrong recipient; and
- Using an unauthorised email address to access personal data; and
- Leaving paper documents containing personal data in a place accessible to other people.

Internal Communication

Reporting a data breach upon discovery

If any member of our workforce suspects, or becomes aware, that a data breach may have occurred (either by them, another member of our workforce, a data processor, or any other individual) then they must contact the School Business Manager who will organise for this breach to be shared with the Data Protection Officer ("the DPO")] immediately at: admin@sataswana.com

The data breach may need to be reported to the ICO, and notified to data subjects. This will depend on the risk to data subjects. The DPO must always be consulted in making a decision as to whether to report a data breach to the ICO. Initial investigations will inform as to whether the data breach should be reported.

If it is considered to be necessary to report a data breach to the ICO then MSPRU must do so without undue delay , and where feasible within 72 hours of discovery of the breach.

MSPRU may also be contractually required to notify other organisations of the breach within a period following discovery.

It is therefore critically important that whenever a member of our workforce suspects that a data breach has occurred, this is reported internally to the DPO immediately.

Members of our workforce who fail to report a suspected data breach could face disciplinary or other action.

Investigating a suspected data breach

In relation to any suspected data breach the following steps must be taken as soon as possible. These do not have to be carried out as individual tasks, and the most appropriate way of dealing with any breach will depend on the nature of the breach and the information available at any time.

Breach minimisation:

The first step must always be to identify how the data breach occurred, the extent of the data breach, and how this can be minimised. The focus will be on containing any data breach, and recovering any personal data. Relevant departments must be involved, such as IT, to take technical and practical steps where appropriate to minimise the breach. Appropriate measures may include:

- remote deactivation of mobile devices;
- shutting down IT systems;
- contacting individuals to whom the information has been disclosed and asking them to delete the information; and
- recovering lost data.

A data breach is notifiable unless it is unlikely to result in a risk to the rights and freedoms of any individual. The DPO will make an assessment of the data breach against the following criteria taking into account the facts and circumstances in each instance:

- the type and volume of personal data which was involved in the data breach;
- whether any special category personal data was involved;
- the likelihood of the personal data being accessed by unauthorised third parties;
- the security in place in relation to the personal data, including whether it was encrypted;
- the risks of damage or distress to the data subject.

If a notification to the ICO is required then see section below on producing a breach notification report to the ICO.

Other supervisory authorities

If the data breach occurred in another country or involves data relating to data subjects from different countries then the DPO will assess whether notification is required to be made to supervisory authorities in those countries.

Data subjects

When the data breach is likely to result in a high risk to the rights and freedoms of the data subjects then the data subject must be notified without undue delay. This will be informed by the investigation of the breach by the Education Learning Trust.

The communication will be coordinated by the DPO and will include at least the following information:

- a description in clear and plain language of the nature of the data breach;
- the name and contact details of the DPO;
- the likely consequences of the data breach;
- the measures taken or proposed to be taken by Education Learning Trust to address the data breach including, where appropriate, measures to mitigate its possible adverse effects.

There is no legal requirement to notify any individual if any of the following conditions are met:

- appropriate technical and organisational protection measures had been implemented and were applied to the data affected by the data breach, in particular, measures which render the data unintelligible to unauthorised persons (e.g. encryption);
- measures have been taken following the breach which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise;
- it would involve disproportionate effort to contact individuals. In which case a public communication or similar equally effective measure of communication to the data subjects shall be issued.
- For any data breach, the ICO may mandate that communication is issued to data subjects, in which case such communication must be issued.

Press

Staff shall not communicate directly with the press and shall treat all potential data breaches as confidential unless otherwise instructed in writing by the DPO.

All press enquiries shall be directed to the Headteacher.

Producing an ICO Breach Notification Report

All members of our workforce are responsible for sharing all information relating to a data breach with the DPO, which will enable a Breach Notification Report Form to be completed.

When completing the attached Breach Notification Report Form all mandatory (*) fields must be completed, and as much detail as possible should be provided.

The DPO may require individuals involved in relation to a data breach to each complete relevant parts of the Breach Notification Form as part of the investigation into the data breach.

If any member of our workforce is unable to provide information when requested by the DPO then this should be clearly reflected in the Breach Notification Form together with an indication as to if and when such information may be available.

In the wake of a data protection breach, swift containment and recovery of the situation is vital. Every effort should be taken to minimise the potential impact on affected individuals, and details of the steps taken to achieve this should be included in this form.

The DPO for MSPRU (Satswana) will determine whether a breach needs to be reported to the ICO and will do this on the behalf of MSPRU.

Evaluation and response

Reporting is not the final step in relation to a data breach. MSPRUwill seek to learn from any data breach.

Therefore, following any breach an analysis will be conducted as to any steps that are required to prevent a breach occurring again. This might involve a step as simple as emailing all relevant members of our workforce to reinforce good practice, or providing additional training, or may in more serious cases require new technical systems and processes and procedures to be put in place.

Appendix 1 Data Breach Reporting Form

To be completed by the Investigating Manager

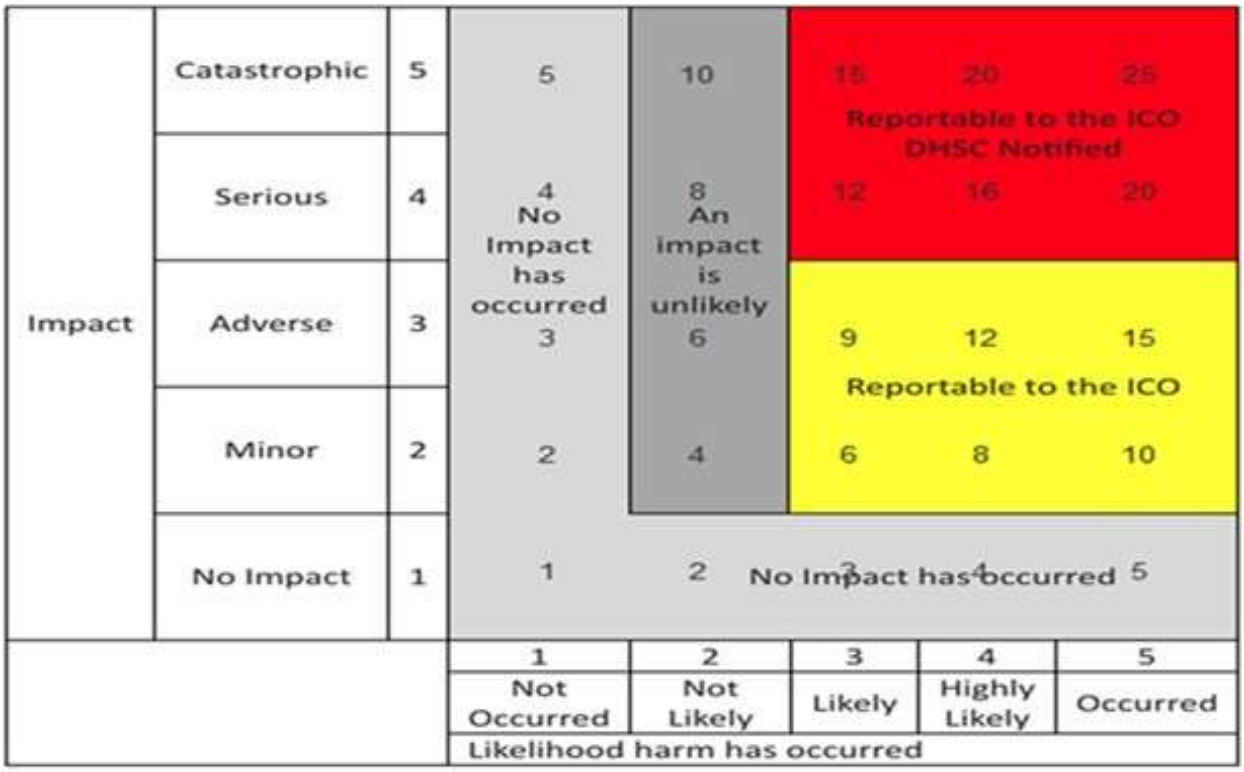
Data Breach Reporting Form	
School name	
Date of incident	
Investigating Officer	
Information Asset Owner	

<u>Do not provide the personal details</u> of those involved in the breach or those affected by the breach. Eg. Use 'service user' instead of the name of the subject.

What has happened – Please describe incident in as much detail as possible with NO Acronyms Tell us as much as you can about what happened, what went wrong and how it happened. Indicate who was involved without using people's names e.g. pupil, teacher etc.
How did you find out about the breach?
When did you discover the breach?
Date: Time:

When did the breach happen?			
Date: Time:			
Categories of personal data in the breach	Y	(Indicate all that apply)	Y
Basic personal identifiers e.g. Name, contact		Identification data e.g. username	
Finance e.g. Credit card, bank details		Official docs e.g. Driving licence	
Location data		Criminal convictions, offenses	
Data revealing racial or ethnic origin		Religious or philosophical beliefs	
Political opinion		Trade Union Membership	
Sex life data		Gender reassignment data	
Health data		Genetic or biometric data	
Not known		Other – specify	
Number of personal data records concerned?			
Categories of data subject affected?	Y	(Indicate all that apply)	Y
Pupils		Parents/Guardians	
Governors		Employees	
Not known		Other – specify	
What are the potential consequences? Please describe the possible impact on the data subject, as a result of the breach. Please state if there has been any actual harm to the data subject(s).			

Risk Analysis Grading



Key:

Likelihood

Number	Likelihood	Description
1.	Not occurred	There is absolute certainty that there can be no adverse effect. This may involve a reputable audit trial or forensic evidence.
2.	Not likely or any incident involving vulnerable groups even if no adverse effect occurred.	In cases where there is no evidence that can prove that no adverse effect has occurred this must be selected.
3.	Likely	It is likely that there will be an occurrence of an adverse effect arising from the breach.
4.	Highly likely	There is almost certainty that at some point in the future an adverse effect will happen.
5.	Occurred	There is a reported occurrence of an adverse effect arising from the breach.

Impact

Number	Likelihood	Description
1.	No impact	There is absolute certainty that no adverse effect can arise from the breach – no impact
2.	Minor - Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred	A minor adverse effect must be selected where there is no absolute certainty.
3.	Adverse - Potentially some adverse effect	An adverse effect may be release of confidential information into the public domain leading to embarrassment or it prevents someone from doing their job.
4.	Serious - Potentially pain and suffering/financial loss	There has been reported suffering and decline in health arising from the breach or there has been some financial detriment occurred. Loss of bank details leading to loss of funds. There is a loss of employment.
5.	Catastrophic - Death/catastrophic event	A person dies or suffers a catastrophic occurrence

Scoring – to be completed by Investigating Officer

	Score	Comments
Likelihood		
Impact		
Total		*

**Please detail text from risk analysis grid here e.g. reportable to the ICO*

Describe the measures you have in place to prevent this type of breach occurring in the first place e.g. staff training, changes to processes/procedures, changes to system controls etc.

Has this type of incident happened before? If so, provide a brief summary of when, who was involved, outcome.
What actions have been taken now to minimise risk of recurrence?
Any other actions taken? e.g. where the incident involves the loss of IT equipment have IT been informed? Or if the incident involves social care service user or patient information, have the Council's Caldicott Guardians been informed?
Have you told the data subjects about the breach?
Further action planned – Provide details of all further actions yet to take place

Appendix 2 Definitions

Term	Definition
Data	is information which is stored electronically, on a computer, or in certain paper-based filing systems
Data Subjects	for the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information
Personal Data	means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Data Controllers	are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is, or are to be, processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes
Data Users	are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times
Data Processors	include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions
Processing	is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties
Special Category Personal Data	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data
Workforce	Includes, any individual employed by Education Learning Trust such as staff and those who volunteer in any capacity including Governors and/or Trustees / Members/ parent helpers.

Appendix 3 Severity Table

NB: This table only gives broad guidelines on the severity of incidents. Each case may differ depending on other variables e.g. the number of people affected, the type of information concerned etc. The severity of each incident should therefore be considered on an individual basis.

Incident Type	**Breach of** (Confidentiality, Integrity, Availability & Accountability)	**Severity**
Unauthorised access to Network/ Systems/ Applications/ Email	Integrity/ Confidentiality/ Availability & Accountability	Moderate to Major depending on the level of information accessed
Sending information		
Information sent to the wrong recipient (internally), disclosing information that is neither confidential not personal	Integrity	Minor
Information sent to various recipients (including external recipients) disclosing non confidential or non-personal information	Integrity	Moderate
Information sent to an unauthorised recipient(s) containing confidential and sensitive personal information (whether Internal or External)	Integrity/Confidentiality	Major
Loss of equipment		
Loss or theft of equipment containing no confidential and/or personal information	Availability	Minor/ Moderate
Loss and theft of equipment containing confidential and/or personal information but with encryption software installed on the equipment	Availability/ Confidentiality	Moderate
Loss and theft of equipment containing confidential and/or sensitive personal information where equipment has no encryption software installed	Availability/ Confidentiality	Major
Inappropriate material found on PC	Accountability	Minor to Major depending on the type of material found on the PC
Illegal material found on PC	Accountability	Major
Inappropriate/unauthorised use of the network/software leading to a disruption of services	Availability	Major
Inappropriate use of the internet or email as defined within the AUP Policy	Accountability/ Availability	Minor to Major depending on the circumstances
Passwords written down leading to unauthorised access	Integrity/ Confidentiality/ Availability & Accountability	Moderate/ Major depending on the type of information and system and impact of the incident
Offensive emails being sent	Accountability	Moderate to Major depending on content of the email
Spam or ‘phishing’ emails	Availability	Minor to Moderate depending on the impact and number of users affected.

Information sent externally or internally by fax, post or hand (containing no confidential or personal information) is lost	Availability	Moderate
Information sent externally or internally by fax, post or hand (containing confidential or sensitive personal information) is lost	Integrity/ Confidentiality/ Availability & Accountability	Major
Unintentional corruption of data	Availability	Moderate/Major depending on the amount of data and type of data corrupted
Intentional corruption of data	Availability and Accountability	Major
Password sharing	Accountability/ Integrity/ Confidentiality	Moderate to Major depending the type of data in question
Downloading or copying of unlicensed software	Accountability	Major
Information/ data deleted or amended from a database in error	Accountability/ Integrity & Availability	Moderate
Information/ data deleted or amended from a database maliciously	Accountability/ Integrity & Availability	Major
Confidential information disposed of inappropriately	Accountability	Major
Website Hacked	Availability/ Integrity	Moderate to Major depending on the criticality of the system
Misuse of Telephony Service	Accountability	Minor to Major on the level of misuse

Appendix 4 Template Data Subject Notification Letter

Dear XXXXX,

I am contacting you about an information breach that has been discovered at Manchester Secondary PRU, that may have exposed you/your child's personal data to unauthorized external parties.

The circumstances of the incident are as follow:

Explain when the breach happened,what the breach entails, what personal/ special categories of personal information have been affected (be specific) and how the breach has been brought to the school's attention

I can confirm that MSPRU take the security of the Personal Data we control very seriously and steps have been taken to minimize the risk of this incident reoccurring and to mitigate any implications this incident may have on you/your childs and your/their privacy.

The following steps have been taken to ensure this error has been contained and will not be repeated;

Detail the steps taken, or intended to be taken, to ensure that this breach is contained and what action will be/has been taken to ensure that the breach is not repeated. Explain how the error occurred (if known).

Also detail any steps which have been taken to assist the Data Subject in retaining control of their personal data.

Please also detail any additional internal security measures which are available to the Data Subject (renewed passwords, security questions, notes on account detailing additional security may be required) and ask if the Data Subject would like to engage with any of these services.

Should you wish to raise a formal complaint regarding this matter you may do so by contacting the school's Data Protection Officer: dpo@mspru.manchester.sch.uk

I would like to take this opportunity to apologies on behalf of MSPRU for this incident and any inconvenience or undue concern it may have caused you.

If you would like to discuss this matter prior to taking further action please do not hesitate to contact me on enter appropriate contact details.