Milton Abbot School

Security Incident Management Policy

Governors Committee: Finance Committee
Review Required: on Change of Model Policy
Current Policy: April 2021

Security Incident Management Policy

1.0 Introduction

1.1 This policy outlines the responsibility of staff, agents, Governors, contractors and partners of the School, to ensure that an information security incident is reported, monitored and handled appropriately. It is intended that this policy will help ensure that the School is able to respond to an information security incident appropriately and in a way that lessens the impact on a data subject. This policy is also in place to help the School to ensure appropriate learning from incidents takes place, and to ensure that reoccurrences do not happen in future.

1.3 This policy is supported by the School's Security Incident Management Procedure. This policy and procedure have been approved by Milton Abbot Governing Body.

2.0 What is a security incident?

2.1 An information security incident can occur when the confidentiality, availability and or integrity of the School's information is put at risk. Examples of activities considered an information security incident might include; information being at risk of or being lost; stolen; disclosed to the wrong recipients (accidentally or deliberately); accessed or attempted to be accessed unlawfully and/or without the permission of the School; sold or used without the permission of the School or a system containing personal data or sensitive business data malfunctions and the information is irretrievable indefinitely or for a long period of time.

2.2 Other examples of information security incidents might include;

- losing paper files or documents containing personal or sensitive business data, when travelling to or from meetings;
- faxing or emailing personal or sensitive business data to the wrong recipients
- posting personal or sensitive business data to the wrong recipients
- deliberately or accidentally disclosing personal or sensitive business data to people who are not legally entitled to the information
- using or selling personal or sensitive business data without the permission of the School
- deliberately or accidentally sharing a password or entry code to an office, computer system or files containing personal or sensitive business data, to someone who is not ordinarily entitled to see the information.
- computer equipment containing personal or sensitive business data is lost or stolen.
- a business critical system containing personal or sensitive business data malfunctions and the information cannot be retrieved quickly

- computer viruses, malware attacks or phishing scams against the School's IT systems
- Unauthorised access or attempted access to IT systems or secure areas

2.3 An information security incident can compromise business operations resulting in embarrassment to the School or loss of trust in the organisation, by clients or members of the public. Information security incidents involving personal data can also result in a breach of the General Data Protection Regulation (GDPR) and other relevant data protection laws, which can lead to the School being fined up to 20 million euros or 4% of our turnover by the Information Commissioners Office. Such breaches can also adversely affect someone's privacy causing them damage and/or distress, which can lead to successful law suits as a result. The School therefore takes all security incidents very seriously.

3.0 Reporting a security incident

3.1 Every information security incident must be reported to the Data Protection Officer. You should also report any "near misses" as it is important that the School is aware of any risks that might expose our information to future incidents.

3.2 The School has a responsibility to monitor all incidents that occur within the organisation that may adversely affect the confidentiality, availability and or integrity of our information. All information security incidents need to be identified, reported, investigated and monitored. It is only by adopting this approach that the School can ensure that incidents of a particular nature do not keep re-occurring.

3.3 If you suspect a member of staff, contractor or governor is accessing or disclosing personal data or sensitive business data inappropriately, you must also report this to the Data Protection Officer and your manager immediately.

4.0 Security incident handling procedure

4.1 The Data Protection Officer is responsible for investigating and managing security incidents in accordance with the School's Security Incident Handling Procedure.

5.0 Monitoring security incidents

5.1 All security incidents will be monitored and re-evaluated at regular intervals by the Data Protection Officer, to ensure that recommendations to improve security have been followed. Any risks identified following an information security incident investigation will be handled in accordance with the School's Information Assurance Policy (add hyperlink).

6.0 Staff training and awareness

6.1 Staff who are required to process personal data, in whatever format, must ensure that they follow guidance on information security. If it is found that this guidance has not been followed, this will be treated as an information security incident and will be investigated in accordance with the Security Incident Management Policy and Procedure. Where such actions are considered negligent, reckless or malicious, this will be referred to Human Resources for consideration as to the merits of disciplinary action.

6.2 Contractors and agents working on behalf of the School must also be made aware of their security obligations and must agree to comply with the School's Data Protection Policy, Cyber Security Policy and our guidance on information security as part of their contract.

6.3 Contractors who identify an information security incident which involves the School's data, must notify the Data Protection Officer immediately so that the School can satisfy its obligations under article 33 of the GDPR.

7.0 Security incident notification

7.1 In accordance with article 33 of the GDPR, the School is committed to notifying the Information Commissioner's Office or relevant supervisory authority within 72 hours, of being notified of information security incident that might adversely affect the rights and freedoms of a data subject. Notifications of this nature are the responsibility of the Data Protection Officer, who will ensure that the risks associated with information security incidents are recorded, monitored and where appropriate escalated in accordance with the School's Information Assurance Policy.

7.0 Theft or loss of computer equipment

7.1 All incidents involving the theft or loss of computer equipment, including smartphones, laptops and other mobile equipment, must be reported to the Data Protection Officer.

8.0 Staff disciplinary action

8.1 If during an information security incident investigation, it has become apparent that the actions of the staff member who caused an incident, were negligent, malicious or were unreasonable in the circumstances, the investigating officer will consult the Human Resources Department who will decide if a conduct investigation is necessary. Staff found to have acted in a negligent or malicious manner will be disciplined in accordance with the School's Disciplinary Policy.

8.2 Where the actions of a staff member are found to constitute an offence under data protection legislation and or the Computer Misuse Act 1990, the matter will be referred to Devon and Cornwall Police.

9.0 Policy review

9.1 This policy will be reviewed annually by the Data Protection Officer.

Policy history

Policy Date	Summary of Change	Contact	Implementation Date