KNOW THE LAW

MCMC is not the only agency in Malaysia with the authority to investigate complaints regarding content on the internet. Content provision on the internet is bound by all relevant laws in the country and reports / complaints can be made to relevant enforcement agencies in relation to matters that fall within their own jurisdictions as follow:

TYPE OF OFFENCE	NATIONAL LAWS	ENFORCING AGENCIES
Sedition	Sedition Act 1948	Royal Malaysia Police
Threats to National Security	Penal Code	Royal Malaysia Police
Fraud/Finance/Trade	• Companies Act 1965 • Financial Services Act 2013 • Direct Sales Act 1993 • Consumer Protection Act 1999 (online sales and purchase transactions) • Capital Markets and Services Act 2007 • Electronic Commerce Act 2006 • Penal Code (Section 420)	• Companies Commission of Malaysia • Bank Negara Malaysia • Ministry of Domestic Trade, Co-operatives and Consumerism • Ministry of Domestic Trade, Co-operatives and Consumerism • Securities Commission Malaysia • Royal Malaysia Police
Copyright	Copyright Act 1987	Ministry of Domestic Trade, Co-operatives and Consumerism
Defamation	• Penal Code • Defamation Act 1957	Royal Malaysia Police
Gaming/Betting	• Common Gaming Houses Act 1953 • Betting Act 1953 • Pool Betting Act 1967	Royal Malaysia Police
Threats to life/property	Penal Code	Royal Malaysia Police
Hacking	Computer Crimes Act 1997	Royal Malaysia Police

The Personal Data Protection Act 2010 (PDPA) is an Act that regulates the processing of personal data in regards to commercial transaction. The Act contains 7 Personal Data Protection Principles to protect the integrity of personal data:

The General Principle - Data users are not allowed to process an individual's personal data without his / her permission. The collection of the data to be processed must be adequate and not excessive for legitimate purposes with the consent of the individual.

The Notice and Choice Principle - Data users must inform a data subject by written notice of the purpose and use of his/her collected personal data.

The Disclosure Principle - A data subject's consent must be obtained for the disclosure of his / her data for the purpose consented and any other related purpose, and to any party.

The Security Principle - Data users need to take the necessary steps to protect the personal data during its processing from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.

The Retention Principle - Personal data shall not be kept longer than the necessary period of time required.

The Data Integrity Principle - Existing personal data must be accurate, complete and not misleading and kept up-to-date having regard to the purpose it was collected and processed.

The Access Principle - Data users must give a data subject the right to access his/her own personal data and to correct the data which is inaccurate, incomplete, misleading or outdated.