CHAPTER 6
DATA SECURITY

6.1 Information Classification

6.1.1 Before determining security measures, the data to be protected need to be identified and classified. Data should be classified based on the level of sensitivity of that data. In a school, data may be categorised to the following categories according to the requirements of the school's security policy:

(a) Confidential

(b) Internal

(c) Public

6.1.2 Definition of the above categories:

(a) **Confidential**: Information and materials, the unauthorised disclosure of which would be prejudicial to the interests of the school.

(b) **Internal**: Information and materials, the unauthorised disclosure of which would be undesirable in the interests of the school.

(c) **Public**: Information and materials to be published or made available to the public access.

6.1.3 Schools should develop procedures for labelling classified information and handling information in accordance with the classification.

6.1.4 Schools should always bear in mind to protect the confidentiality, integrity and availability of data. Security measures should be considered and implemented as appropriate to preserve the confidentiality, integrity, and availability of information while it is being processed, in transit, and in storage.

6.2 Cryptography

6.2.1 Schools should ensure proper and effective use of cryptography to protect the confidentiality, authenticity and integrity of information.

6.2.2 Encryption techniques should be used to protect the sensitive data and enforce confidentiality during transmission and storage. Many schemes exist for encryption of files such as using the program's own encryption feature, external hardware device, secret key encryption, and public key encryption.

6.2.3 For information classified as confidential, the symmetric encryption key length are recommended to be at least 128-bit for the advanced encryption standard (AES) encryption or equivalent, whereas the asymmetric encryption key length are recommended to be at least 2048-bit for the Rivest-Shamir-Adleman (RSA) encryption.

6.2.4 It is very important to ensure the protection and management of keys. For keys that are used for the processing of information classified confidential, they shall be stored separately from the corresponding encrypted information. These keys may be stored inside chips of smart cards, tokens, or disks, etc., and are used for authentication and/or decrypting information. Furthermore, it is dangerous to distribute the decryption key along with the encrypted file during file distribution since one may obtain the decryption key and easily open the file.

6.2.5 It is risky to store data to mobile device and removable media as they are small and can be easily lost or stolen. Storing classified information to these devices should be avoided. Staff should justify the need to store classified information to these devices. Mobile device and removable media provided by the school should be used. Staff should seek proper authorization before storing minimum required classified data to the mobile device and removable media. To minimise the risk of data leakage, devices with encryption feature suitable to protect classified data should be used. Schools are recommended to remove classified information from the mobile device and removable media as soon as it no longer needs to be stored there to minimize the exposure.

6.2.6 Data encryption is a way to enhance data confidentiality. Schools should confirm that encryption capabilities provided on cloud service are in alignment with the cryptographic policy on the use of cryptographic controls. Classified data should be protected using strong encryption method both at rest and in transit in accordance with school's security requirements and needs.

6.2.7 The primary use of an application's password-protection feature is to provide protection on the file and prevent unauthorised access. Users should encrypt the file instead of using only password in order to protect the information for confidentiality as appropriate.

6.3 Backup

6.3.1 School should carry out backups at regular intervals and should establish and implement backup and recovery policies for their information systems. Users should perform backup for the data stored in their workstations, mobile devices and removable storage media regularly. The backup frequency should be based on the impact of loss of availability of the data. Backup restoration tests shall be conducted regularly. Schools should follow the best practices when establishing their backup and recovery policies:

(a) Backup copies should be maintained for all operational data to enable reconstruction should they be inadvertently destroyed or lost.

(b) The backup copies should be taken at regular intervals such that recovery to the most up-to-date state is possible.

(c) Backup activities should be reviewed regularly. Procedures for data backup and recovery should be well established. Wherever possible, their effectiveness in real-life situations should be tested thoroughly.

(d) It is advisable to store backup copies offline at a safe and secure location remote from the site of the systems. In case of any disaster which destroys the systems, the systems could still be reconstructed elsewhere.

(e) Multiple generations of backup copies should be maintained. This would provide additional flexibility and resilience to the recovery process. A "grandfather-father-son" scheme for maintaining backup copies should be considered such that two sets, viz, the last and the last but one, of backup copies are always maintained together with the current operational copy of data and programs. The updates to bring the backup copies to the current operational state shall, of course, also be maintained and stored with the backup copies.

(f) At least three generations of the backups should be kept. However, if daily backups are taken it may be easier administratively to retain six or seven generations. For example, a Monday’s daily backup should be kept until the following Monday when it can be overwritten. Month end and year end copies of files may be retained for longer period as required.

(g) Backup means such as magnetic tapes / optical disks / external hard disk / network attached storage (NAS) / storage area network (SAN) / cloud backup used for backup should be tested periodically to ensure that they could be restored when needed.

6.3.2 In some unexpected situations where data is deleted accidentally before performing a backup, or data resides on a failed hard disk that cannot be accessed through the system, a hard disk data recovery service may be required. If adopting external data recovery service is required, schools are recommended to follow the best practices to mitigate the risk of data leakage:

(a) Use on-site data recovery service as far as practicable and ensure the contractor is aware of the protection requirements for the confidential information during the recovery process.

(b) Escort the contractor’s staff and take due care to ensure the confidential information is not disclosed.

(c) Sanitise the residual user data in the equipment tools and the associated media used for the data recovery.

(d) Obtain non-disclosure agreement from the contractor.

6.4 Personal Data (Privacy)

6.4.1 Schools should ensure compliance with the Personal Data (Privacy) Ordinance, including the Data Protection Principle 4 (on security of personal data) when handling personal data. Appropriate security measures should be adopted to protect personal data from unauthorised or accidental access, processing, erasure or other use. For details of six Data Protection Principles, please refer to Personal Data (Privacy) Ordinance at PCPD’s web site: https://www.pcpd.org.hk/english/data_privacy_law/6_data_protection_principles/principles.html

6.5 Information Erasure

6.5.1 When the data is no longer needed, it should be permanently destructed. A system of checks and balances should be maintained to verify the successful completion of the secure deletion process.

6.5.2 All data must be completely erased before computer equipment, storage media, and electronic office equipment are to be reused, transferred or disposed by means of sanitisation or physical destruction to ensure that the information cannot be recovered.

(a) Sanitisation: refers to the process of removing the data on the media to ensure that the original data cannot be retrieved. Sanitising may be accomplished by overwriting or degaussing.

(b) Physical Destruction: storage media that cannot be sanitised should be physically destroyed by means of shredding, disintegration or grinding.

6.5.3 The table below describes different methods of data destruction for different storage media. Schools are recommended to make risk-based decisions on which method is most appropriate based on the data type, risk of disclosure, and the impact if that data were to be disclosed unintentionally.

Media Types	**Reuse (including transfer for reuse)**	**Disposal (including trade-in, and replacement of faulty media)**
Non-volatile magnetic media such as hard disk drives, floppy disks, tapes, etc.	Overwriting	Overwriting or Degaussing or Physical Destruction
Non-volatile solid state memory such as USB flash drives, memory cards, solid state disks (SSD), etc.	Overwriting	Overwriting or Physical Destruction
Optical media – write once such as CDs, DVDs, Blu-ray discs, etc.		Physical Destruction
Optical media – write many such as CDs, DVDs, Blu-ray discs, etc.	Overwriting	Physical Destruction
Smart devices such as PDAs, mobile phones, tablets, etc.	Overwriting	Overwriting or Degaussing or Physical Destruction

6.6 Promotion of Security Awareness of the Data Security Requirements

6.6.1 In order to promote the security awareness of data security requirements in schools, an effective way is continuous information sharing such as distribution of security news or supplement especially right after major changes of security requirements in IT security documents and/or major security incident that has severe impact to schools and/or public. The followings are suggested tips of distributing security news or supplement for schools:

(a) All requirements are well-documented. Audience should be educated where the related documents including precedence of them could be found.

(b) General principles should be delivered to the audience so that they could understand and remember the main ideas easily.

(c) Do’s and Don’ts with practical examples may also raise the audience’s interest and can solidify their understanding.

(d) The size of the supplement should be kept as short and precise as possible. For example, around five pages for regular issues and one to two pages for a reminder after major incident or any potential incident of high likelihood.

(e) Make use of school communication channels such as email, instant message groups, staff meetings etc. to disseminate the updated news of schools information security information.