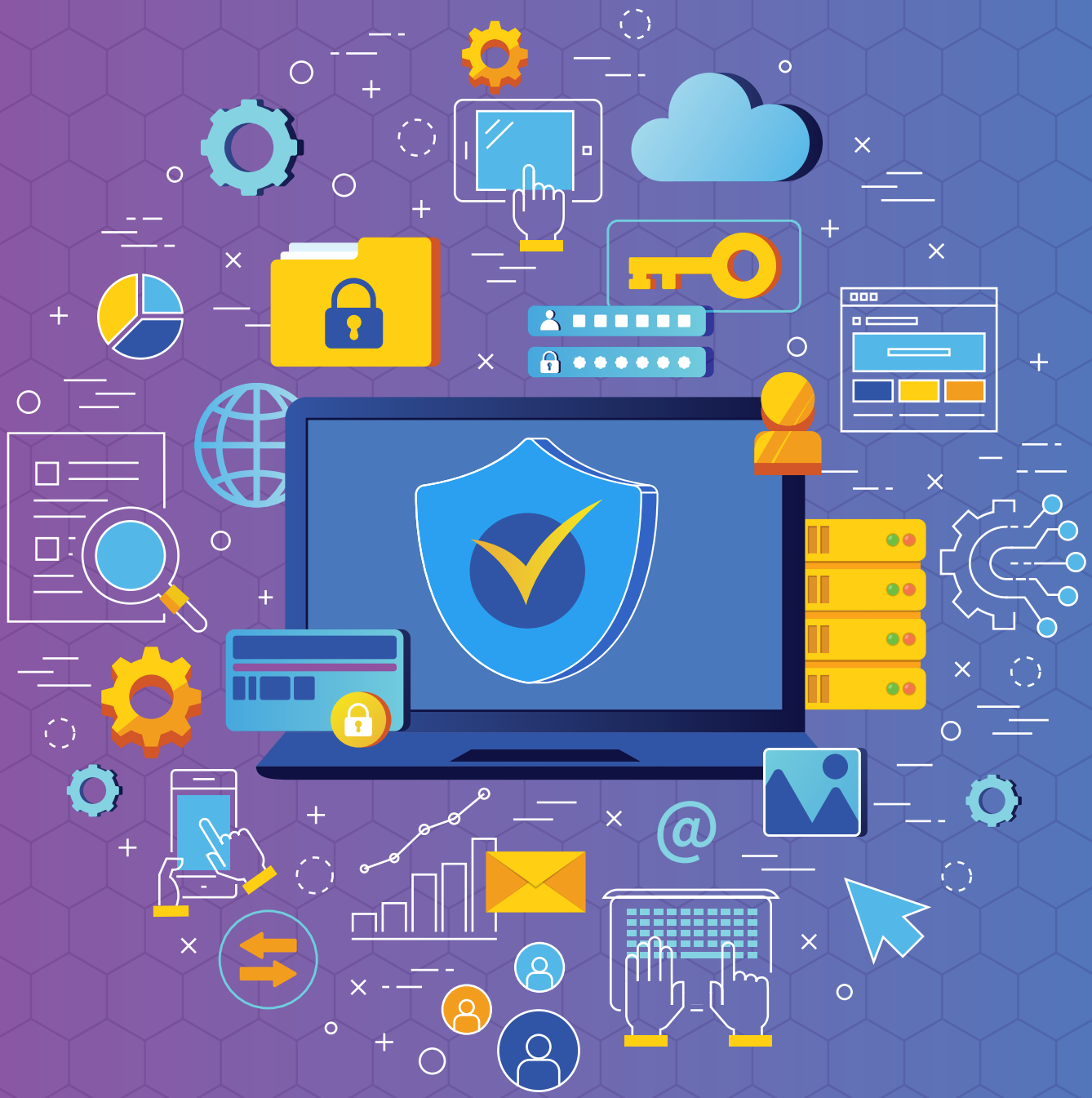
DATA PROTECTION GUIDE FOR CHARITIES:

Managing & Securing Electronic Personal Data



Foreword by the Commissioner of Charities

The *Data Protection Guide for Charities: Managing & Securing Electronic Personal Data* is one of the Commissioner of Charities' initiatives to uplift the digital capabilities of all charities.

In an increasingly digitalised world, charities have to quickly adopt new technologies and solutions to ensure that they are not left behind. Managing personal data properly is critical as the communities which the charities are serving expect their personal data to be treated with care. In addition, any data breach can disrupt charities' operations and decrease public confidence in the charity sector.

Developed by the Commissioner of Charities in partnership with Harry Elias Partnership LLP, this data protection guide is kept simple and concise to ensure charities of any size will be able to appreciate the importance of taking the relevant measures to protect data and implement them. By putting in the good practices outlined, it shows your commitment to protect and secure the data of your stakeholders, and together, we can build a flourishing charity sector that is digitally resilient.

I would also like to express my appreciation to K.K. Lim, Natasha Goh and Valencia Soh who have contributed their time and expertise in partnership with the COC's office in the development of this Data Protection Guide for Charities: Managing & Securing Electronic Personal Data.

Regards,

Dr Ang Hak Seng, FCA (Singapore)

Commissioner of Charities

Table of Contents

PART I:
INTRODUCTION AND CONTEXT

PART I: INTRODUCTION AND CONTEXT

1 INTRODUCTION

1.1 Charities are not immune to malicious cyber activities. Like businesses, charities are increasingly reliant on Information Communication Technology ("**ICT**") systems to carry out their operations to meet their charitable purposes. With this increasing reliance, a charity's loss of access to technology or funds, or a breach of personal data, can result in financial or reputational loss.

1.2 Personal data is data from which an individual can be identified[1]. Charities often hold significant amounts of critical personal data of their stakeholders. This relates to donors, staff, volunteers, beneficiaries, and their own members.

1.3 In a qualitative research commissioned in 2017 by the United Kingdom's Department for Digital, Culture, Media and Sport ("**UK DCMS**"), charities "felt less at risk of cyber attacks than businesses"[2]. This was because some charities were of the view that they had less funds and less critical data to be stolen as compared to profit-making businesses. Notwithstanding these perceptions, the 2019 Cyber Security Breaches Survey commissioned by the UK DCMS shows that 22% of charities surveyed in the United Kingdom have identified cyber breaches or attacks in the last 12 months[3].

1.4 In Singapore, while qualitative and quantitative research have not been carried out specifically for the charities sector, it is clear that the number of cyber threats and attacks in general were on the rise in 2018 and 2019. This shows that individuals and corporations carrying out such cyber-attacks are indiscriminate in their approach, and they do not necessarily reserve their efforts in targeting businesses where there is perceived to be specific data that they can profit from.

1.5 In the Singapore Cyber Landscape 2018 prepared by the Cyber Security Agency of Singapore, the statistics for 2018 were reported. For instance, it was reported that there were 16,100 phishing URLs with a Singapore-link detected, 605 incidents of website defacements, 21 ransomware cases, and 6,179 cases of cybercrime in Singapore[4].

---

1 See s.2 of the PDPA for the definition of "personal data".

2 Report by the United Kingdom Department for Digital, Culture, Media and Sport, titled "*Cyber security amongst charities: Findings from qualitative research*", August 2017.

3 Report by the United Kingdom Department for Digital, Culture, Media and Sport, titled "*Cyber Security Breaches Survey 2019*", July 2019.

4 Report by the Cyber Security Agency of Singapore titled "Singapore Cyber Landscape 2018", June 2019.

1.6 It is clear that cybersecurity should be a priority for all charities, irrespective of their size. Charities rely upon donors and their funds for their operations and to meet their charitable purposes.

1.7 Charities hold significant amounts of personal data of their various stakeholders, and should place importance on protecting the information and the resources of the people that help support them. This is to ensure that the trust in the charity sector is maintained, so that donors continue to give generously[5].

1.8 This should be a sufficiently strong impetus to ensure that donors' information is adequately protected, so as to maintain public confidence in these charities.

1.9 The hope for this guide is that it will be a useful starting point to assist charities to begin taking steps to protect donor information that is in their possession.

2 LEGISLATIVE FRAMEWORK

2.1 The primary piece of legislation that governs the protection of personal data in Singapore is the Personal Data Protection Act (No. 26 of 2012) (the "**PDPA**"). The PDPA applies generally to charities because charities are "organisations" under the definition of the PDPA.[6]

2.2 While the Charities Act (Cap. 37) (the "**CA**") does not explicitly deal with a charity's obligation to protect personal data, the subsidiary legislation of the CA require charities to keep information relating to donors confidential, with disclosure of such information only to be done with the consent of the donor or as permitted by the PDPA.

2.3 In the table below, we set out the following data protection obligations that are applicable to charities and the corresponding legislation imposing such an obligation.

[5] See for example the report by the Ministry of Culture, Community and Youth, titled "*Commissioner of Charities Annual Report 2018*", June 2019, p.4.

[6] See s.2 of the PDPA for the definition "organisation".

9 Data Protection Obligations[7]	PDPA	CA and subsidiary legislation
Consent Obligation – An organisation must obtain consent of the individual before collecting, using or disclosing the personal data for a purpose.	s.13 to s. 17 of the PDPA	-
Purpose Limitation Obligation – An organisation may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances and, if applicable, such purposes have to be notified to the individual concerned.	s.18 of the PDPA	-
Notification Obligation – An organisation must notify the individual of the purpose(s) for which it intends to collect, use or disclose the individual's personal data on or before such collection, use or disclosure of the personal data.	s.20 of the PDPA	-
Access and Correction Obligations – An organisation must, upon request, (i) provide an individual with his or her personal data in the possession or under the control of the organisation and information about the ways in which the personal data may have been used or disclosed during the past year; and (ii) correct an error or omission in an individual's personal data that is in the possession or under the control of the organisation.	s.21 – 22 of the PDPA	-
Accuracy Obligation – An organisation must make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete if the personal data is likely to be used by the organisation to make a decision that affects the individual concerned or disclosed by the organisation to another organisation.	s.23 of the PDPA	-

[7] Advisory by the Personal Data Protection Commission Singapore, titled "*Advisory Guidelines on Key Concepts in the Personal Data Protection Act*", October 2019, p. 32 – 33.

9 Data Protection Obligations[7]	PDPA	CA and subsidiary legislation
Protection Obligation – An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. Such Protection Obligation is implied in the subsidiary legislation of the CA in their requirement for charities to keep information relating to donors confidential, with disclosure of such information only to be done with the consent of the donor or as permitted by law.	s.24 of the PDPA	r.8(1)(c) of the Charities (Institutions of A Public Character) Regulations; r.4(1)(c) of the Charities (Fund-raising Appeals for Local and Foreign Charitable Purposes) Regulations 2012
Retention Limitation Obligation – An organisation must cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular individuals as soon as it is reasonable to assume that (i) the purpose for which the personal data was collected is no longer being served by retention of the personal data, and (ii) retention is no longer necessary for legal or business purposes.	s.25 of the PDPA	-
Transfer Limitation Obligation – An organisation must not transfer personal data to a country or territory outside Singapore except in accordance with the requirements prescribed under the PDPA.	s.26 of the PDPA	-
Accountability Obligation: An organisation must implement the necessary policies and procedures in order to meet its obligations under the PDPA and shall make information about its policies and procedures publicly available. This includes the appointment of one or more individuals to be responsible for ensuring that the organisation complies with the PDPA. The person(s) appointed is the Data Protection Officer.	s.11 – 12 of the PDPA	-

[7] Advisory by the Personal Data Protection Commission Singapore, titled "*Advisory Guidelines on Key Concepts in the Personal Data Protection Act*", October 2019, p. 32 – 33.

3 PURPOSE AND SCOPE OF THIS GUIDE

3.1 This guide is a general guide that is applicable to **all** charities regardless of the size and the nature of the operations. Like the 9 data protection obligations under the PDPA that are applicable to all charities, there are no exceptions based on the specific traits of each charity.

3.2 This guide is for the person that is responsible for data protection in a charity. It focuses on the protection of the personal data of the charity's stakeholders in electronic medium, that is within the charity's possession, by implementing controls to limit access and to protect such donor information. To this end, this guide takes the following approaches:

(a) **Risk-Based:** Each charity must assess its own level of risk and pick from the suite of measures to be implemented. Each charity will have a different level of risk – what is necessary for one charity may not be applicable to another.

(b) **Practical:** This guide functions as a starting point for basic practices to be implemented. This is intended to be a cost-efficient guide that is capable of being followed, even by charities of limited means, and by persons who are not technically trained to supervise or work with ICT systems.

3.3 In view of the wide-ranging topic of implementing a system and deploying measures for the protection of personal data in the context of ICT systems, this guide is limited in some respects. For instance, it does not deal with the development of ICT systems for collecting and maintaining personal data, the development of a personal data protection policy, or the policies in relation to the notification and obtaining of consent in relation to personal data. It also does not deal with ongoing maintenance and testing of existing ICT systems.

3.4 Depending on the specific nature of each charity's operations, charities should seek legal advice and technical expertise to protect the personal data based on the uniqueness of each charity's ICT system and the specific risks faced by each charity.

PART II: PRACTICES FOR THE PROTECTION OF ELECTRONIC PERSONAL DATA

PART II: PRACTICES FOR THE PROTECTION OF ELECTRONIC PERSONAL DATA

4 OVERVIEW

4.1 These guidelines are prepared in line with the following applicable standards that reflect the best practices in information security management:

(a) ISO-IEC 27001, the standard applied in respect of information security management system;

(b) ISO-IEC 27018, the standard applied in respect of Code of practice for protection of personal data in public clouds; and

(c) *Guide to Securing Personal Data in Electronic Medium* published by the Personal Data Protection Commission.

4.2 First, the document will deal with implementing controls to limit access to the personal data that is in the charity's control or possession.

4.3 Thereafter, the guide will look at ICT systems commonly used by charities, and review how controls are implemented to limit access and to protect personal data from being exposed. Commonly used ICT systems are as follows:

(a) Personal computers, portable computing devices and removable storage media;

(b) Email;

(c) Websites and web applications; and

(d) Relevant cloud services.

4.4 To ensure that the guide remains practical for the end-user, each section will explain why the subject it addresses is necessary, and set out the steps that can be easily taken to protect personal data in a charity's possession.

5 PRACTICES IN DETAIL

A. Implementing controls and limiting access to personal data

5.1 **Why necessary:** If controls limiting access are not implemented, there is a risk of vulnerability resulting in hackers getting access to personal data that ought to be protected by charities. This is important since charities typically have both employees and volunteers[8] involved in their operations. Charities need to ensure that there are sufficient controls and systems limiting access by unauthorised personnel to personal data.

5.2 There are two aspects to be considered in this process of implementing controls and limiting access to personal data in a charity's possession:

(a) Authentication: The process of identifying the user who is entitled to access such personal data; and

(b) Authorisation: The process of verifying whether such a user is permitted to access the personal data sought.

5.3 A common and cost-efficient way to implement controls to limit access is to maintain good password management. This can be considered from two perspectives:

(a) Administrator: Administrators should impose conditions on users to create passwords that meet certain criteria; and

(b) Users: Users should ensure that the passwords set follow the Administrator's policies and are kept secure by not sharing passwords with third parties or writing their passwords on paper and leaving the paper lying around the physical office premises.

Administrator's Responsibilities: Authentication and Authorisation	
(a)	Determine a suitable 2-Factor authentication ("2FA") method for accessing personal data based on the risk of damage to the individual in case of a data breach. 2FA is recommended as this is a common industry standard for authentication.
(b)	Determine a suitable maximum number of attempts allowed for a user to authenticate his or her identity based on the type of data to be accessed.
(c)	Implement account lockout when the maximum number of attempts is reached, to prevent dictionary or brute-force attacks, which refer to methods of systematically checking all possible keys or passwords until the correct one is found. This is particularly important for any system that does not implement 2FA.

[8] See also s.2 of the PDPA, where volunteers are also considered to be employees. Charities are responsible for both their employees and volunteers under the PDPA.

Administrator's Responsibilities: Authentication and Authorisation	
(d)	Password used for authentication is encrypted during transmission and also encrypted or hashed in storage. Review the method of encryption (e.g. algorithm and key length) periodically to ensure that it is recognised by the industry as relevant and secure.
(e)	Implement authorisation mechanisms and processes to check if the person accessing the system has appropriate access rights to data requested within the system.
(f)	Define user roles or groups for systems that enable access to personal data. Access rights for each user role or group should be clearly defined and reviewed regularly.
(g)	Grant a user only the necessary access rights to personal data within systems to fulfil their role or function.
(h)	Track and review usage of accounts and their associated access rights regularly. Remove or change access rights for unused or obsolete accounts promptly.
(i)	Log all successful and failed access to systems to help detect unauthorised attempts to gain access to them.

User's Responsibilities: Usage of Passwords for Authentication and Authorisation	
(a)	Password used for authentication has a length of at least 8 characters containing at least 1 alphabetical character and 1 numeric character.
(b)	When password used for authentication is typed in, it is to be hidden under placeholder characters such as asterisks or dots.
(c)	Users are required to change their passwords regularly. The frequency should be based on the risk of damage to the individual if the data is compromised. A good practice to consider would be to require password change once every 6 months.
(d)	Do not use default passwords. Change default passwords to strong passwords at the earliest possible opportunity.

B. Personal computers, portable computing devices and removable storage media

5.4 **Why necessary:** With the convenience of removable storage media and portable computing devices, it is easy for data to be transferred from one device to another within seconds. It is necessary to track the devices that contain personal data, so as to implement the appropriate controls to protect the personal data in the possession of charities.

5.5 As a starting point, it is important to track and inventory devices that contain personal data by carrying out physical asset inventory checks regularly to ensure that all electronic devices are accounted for.

5.6 With respect to each electronic device – personal computer, portable computing devices (e.g. laptops, tablets), and removable storage media (e.g. thumbdrives and hard disks), specific types of controls are set out below to limit access to personal data stored on these devices and to ensure protection.

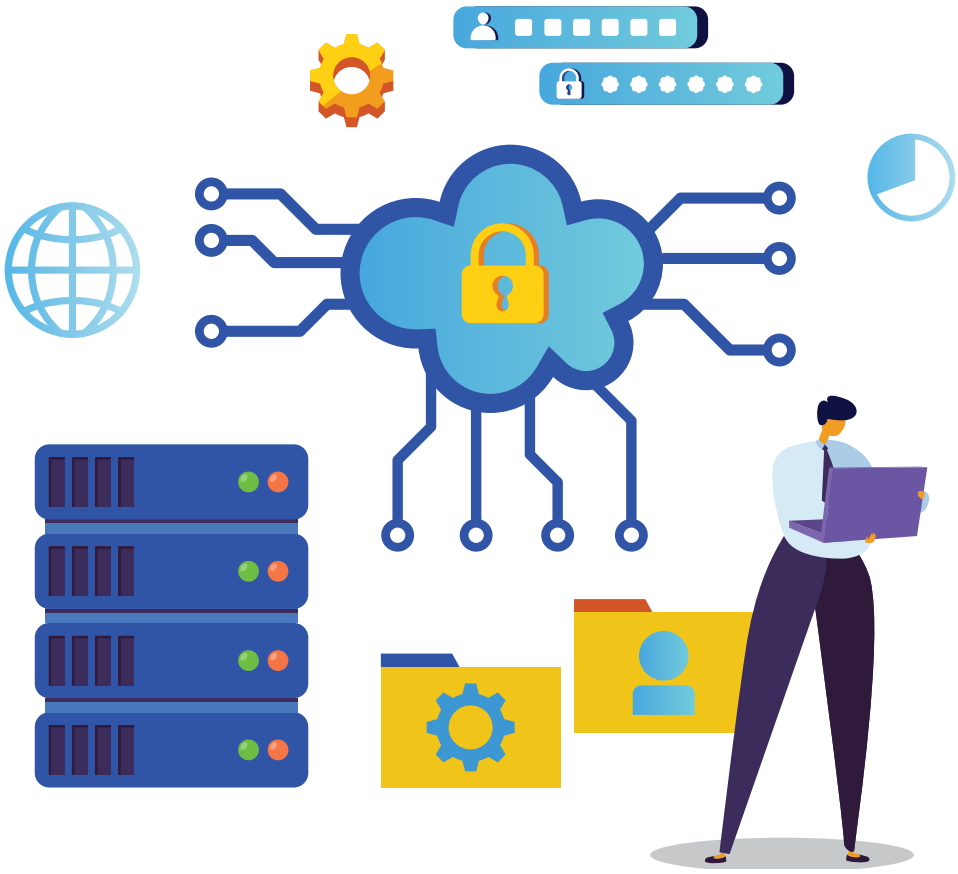
i. Personal computers containing personal data

Good practices for personal computers	
(a)	Protect computers by using password functions.
(b)	Install end point security such as anti-virus, anti-spyware, and software-based firewall on computers. Keep them updated and perform scans regularly, with scans at least once a week.
(c)	Encrypt all personal data which has a higher risk of adversely affecting the individual should it be compromised[9]. Review the method of encryption (e.g. algorithm and key length) periodically to ensure that it is recognised by the industry as relevant and secure.
(d)	Prevent unauthorised personnel from viewing the screens of personal computers easily, such as by using privacy filters or screens, or through positioning of the personal computer.
(e)	Implement additional controls for shared computers to prevent access to personal data, e.g. those keyed in by another user.
(f)	Consider whitelisting safe URLs or domains to prevent access to phishing websites.

[9] Note that encryption of personal data is considered as almost always necessary under the Protection Obligation of the PDPA.

ii. Portable computing and removable storage media security

Good practices for portable computing & removable storage media security	
(a)	Minimise storage of personal data on portable computing devices and removable storage media. Remove personal data that is no longer required as soon as possible.
(b)	Secure portable computing devices and removable storage media when not in use. This can be done by keeping them under lock and key, attaching them to a fixture by a security cable, hand-carrying, and not leaving them unattended.
(c)	Configure portable computing devices to automatically lock upon a period of inactivity, whereby a password is required to resume usage.
(d)	Assess the applications that users can install and establish a policy for the use and tracking of the organisation's portable computing devices and removable storage media.



C. Emails

5.7 **Why necessary:** Electronic mail (also known as email) is a form of communication that is used by all organisations. Emails are an indispensable part of everyday life now. Confidential and sensitive information are often communicated over email. As a consequence of the prevalent use of emails, it is susceptible to a wide range of threats and attacks. Common cybersecurity attacks on emails are phishing and malware attacks. In the case of charities, Business Email Compromise is also something that they are susceptible to.

5.8 A brief explanation of such cyberattacks are as follows:

(a) Phishing is a technique whereby scammers send fake emails to ask for sensitive information (e.g. bank details, credit card details, NRIC numbers, passwords for certain accounts etc.) or containing links to websites which can obtain such information;

(b) Malware is a form of malicious software, including viruses, that is downloaded from the web that can harm an organisation's ICT system; and

(c) Business Email Compromise is a situation where a hacker obtains control of specific email accounts within an organisation and utilises it to their advantage. For instance, specific email accounts of charities when compromised would likely involve call for donations for fraudulent purposes.

5.9 As such, it is critical to implement security surrounding emails to protect personal data that is often stored in emails.

Good practices for email security	
(a)	Install end point security software for all users. Keep the software updated and perform scans regularly.
(b)	Before sending out emails, review all recipients to ensure there is no unintended recipient.
(c)	Encrypt or password protect attachments containing personal data that have a higher risk of adversely affecting the individual should it be compromised. The password should be communicated separately. For encryption, review the method of encryption (e.g. algorithm and key length) periodically to ensure that it is recognised by the industry as relevant and secure, whereas for password protection ensure a strong password is used. If emails are accessible directly from the internet, 2FA should be incorporated to reduce risk of unencrypted emails with personal data.
(d)	Include a notice in all emails to warn recipients against unauthorised use, retention or disclosure of data, and to inform the recipients to delete and notify the organisation immediately if the email was not intended for them.

D. Websites and web applications

5.10 **Why necessary:** Charities are increasingly taking to public web platforms and utilising web applications to collect donations from members of the public, both domestically and globally. These range from web crowdsourcing members of the public for specific time-sensitive causes, to maintaining a public web platform to collect donations for a specific charity and its daily operations.

5.11 In order to ensure that donors' personal data, such as bank and credit card details, are not compromised, steps need to be taken to ensure the information input on such website and web applications are secure. The failure to ensure that such information is protected can result in breaches of the PDPA[10].

5.12 The steps to ensure that information input on websites and web applications are secure are as follows:

Good practices for websites and web applications: security measures to be taken by developers and website administrators	
(a)	Perform validation of user input.
(b)	Ensure that files containing personal data are not made available through a web application or the web server. Even if the web link to such files is not published, it is still possible to discover and access these files.
(c)	Perform cookie data validation and URL validation to correspond with the session in use.
(d)	Do not allow the bypassing of user authentication to access personal data.
(e)	Perform web application scanning and source code analysis to help detect web vulnerabilities.
(f)	Apply secure connection technologies or protocols to secure the link between a website or web application, and a web browser.
(g)	Configure web servers to disallow the browsing of file directories.
(h)	Ensure that user data is encrypted at all times.
(i)	Carry out regular penetration and/or vulnerability assessment every 12 – 18 months or when there is a major system inclusion or update.

[10] See for instance, Decision of the Personal Data Protection Commission, *[2016] SGPDPC 2*, April 2016.

E. Relevant cloud services

5.13 **Why necessary:** Cloud computing is increasingly seen as an attractive option for users. Examples of cloud computing (Software-as-a-Service) include the use of Google Accounts (together with Google Apps such as Google Drive, Google Docs etc.), and Microsoft Office 365 (together with Microsoft Apps such as Microsoft Word, Microsoft Excel etc.). Cloud computing is now a convenient way for users to use an entire suite of ICT resources based on demand from providers of cloud services, so that users do not need to maintain and develop their own ICT resources on the premises from which they operate. Note that paid services should generally be used instead of free services that are made available for personal use. This is because paid services usually include security software and updates that will better enhance the security to users.

5.14 With the convenience that comes with utilising cloud computing, organisations relinquish control over the personal data that is stored on such cloud storage systems. While control is relinquished, organisations should continue to take steps to ensure that the cloud computing service that is used is compliant with the relevant security standards applicable.

Good practices for cloud computing	
(a)	Ensure cloud service provider is ISO certified for the relevant standards necessary (for example, ISO 27001, 27017, 27018 etc). Obtain a copy of the certification for your records if possible.
(b)	You should be aware of the security measures your cloud service provider has to protect your organisation's data on the cloud, like encryption etc. For example, the cloud service provider may perform their own penetration tests and be willing to share those results.
(c)	You should be aware of the laws applicable to the personal data you store in the cloud and in which jurisdiction this data is stored.
(d)	You should, where possible, negotiate that your cloud service provider conducts on-going third-party audits and provides you with these reports.
(e)	Where organisations wish to outsource electronic data storage, or to store electronic data in the cloud, due diligence should be carried out on the service provider, and there should be a written outsourcing agreement in place.

PART III:
CONCLUDING REMARKS

PART III:
CONCLUDING REMARKS

6 CONCLUDING REMARKS

It is strongly advised that pre-emptive steps be taken when handling personal data to ensure that it remains adequately protected. Be that as it may, each charity should also be prepared to handle data breaches in the event it occurs. In the data protection policies of each charity, there should be a standard operating procedure of what to do in the event of a data breach incident. Charities may find out more in PDPC's *Guide to Managing Data Breaches*.

Commissioner of Charities

HARRY ELIAS PARTNERSHIP