Charlton Kings Infants' School

Data Storage Policy

Governor Committee Responsible:	Finance and Operations	Governor Lead:	Alan Waller Alan.Waller@ckis.org.uk
Status	Non-Statutory	Review Cycle	Bi-Annual
Last Review	1.06.2019	Next Review Date	June 2021

Designation	Name	Date	Signature
Chair of Governors	Henning Schmidt	12.06.19	
Head Teacher	Katie James	12.06.19	

Introduction

This policy sets out the general principles for storage of individuals' data by the school.

Legislation

Under the Education (Pupil Information) (England) Regulations 2005, pupils and their parents have a right of access to their educational record. Under the Data Protection Act 1998 a pupil or their nominated representative has a right to see information held about them. This right exists until the point that the file is destroyed. Therefore, it is important to remember that all information should be accurately recorded, objective in nature and expressed in a professional manner. It is important that the data is held securely.

General principles

Personal data should be stored in an encrypted form to protect against unauthorised access or processing, especially if the loss of the personal data is reasonably likely to occur and would cause damage or distress to individuals.

Encrypting data whilst it is being stored (eg on a laptop, mobile, USB or back-up media, databases and file servers) provides effective protection against unauthorised or unlawful processing. It is especially effective to protect data against unauthorised access if the device storing the encrypted data is lost or stolen.

Forms of encryption

(a) Full disk encryption

Most modern operating systems have full disk encryption built in, which will encrypt the entire contents of the drive. The data is decrypted when the user accesses the device. Unfortunately, it may not be enabled by default, requiring it to be activated, for example by accessing the relevant settings options within the operating system of their device.

Some data controllers have considered setting a PIN or requiring users to provide a username/password in order to access a device. Whilst this can offer assurance that the user is authorised to perform certain functions this approach offers little protection to the underlying data which is commonly stored in plain text on the disk and must not be considered as equivalent to encryption. The data can also be easily accessed by an attacker with physical access to the device. (We need to tailor this to the guidance we want to give – we need to discuss this)

Passwords used to decrypt the hard disk or for access control must be sufficiently complex in order to provide an appropriate level of protection.

(b) Individual file encryption

Alternatively, files can be encrypted individually, or groups of files can be placed within encrypted containers. In the event of loss or theft of the device an attacker might gain access to the device and to some data but not to the encrypted files (assuming the key remains secure).

The ability to create encrypted containers may be part of encryption or other archive software or be built-in to the operating system. Once a container is created, files can be placed within it and encrypted and the container itself can be moved and/or copied.

(c) Application or database encryption

Some software applications and databases can also be configured to store data in an encrypted form. The benefit here is that the application controls the encryption so can access the keys when needed without relying on the underlying IT infrastructure.

When data is shared between applications then processes are required to share keys securely.

Residual risks with encrypted data storage

There are still occasions where data can be accessed by an unauthorised person, even if a system uses encrypted data storage and it is important to be aware of these. For example:

- If an encrypted device is left unattended whilst a user is logged in, then an attacker can gain access to the decrypted material;
- devices that store data in encrypted volumes or containers must mount or open these containers in order for the data to be accessed. If the volumes are not closed or unmounted once the user has finished, the data may be accessible to others;
- if a device is infected with malware which has appropriate permissions to access the data, full disk encryption or use of secure containers will offer little protection once that data is decrypted;
- if applications on the device are compromised by an attacker then any data which can be accessed by the application is vulnerable. For example, successful exploitation of a website vulnerable to an SQL injection attack could expose data whether or not the device itself is encrypted; and
- APIs which permit web content to read and write files on the underlying file system may pose additional security considerations.

Addressing these types of risks is therefore an important part of an encryption policy which can also include employee awareness training.