Silverhill School

8.04

Policy for Secure Use of Confidential Information on Portable Media

Silverhill School recognises that the loss or theft of personal data and other confidential information can have devastating consequences for individuals and severe financial, legal and reputational costs to the school, including significant fines from the UK Information Commissioner.

Policy Statement
This policy has been developed to enable staff, and other authorised users to use, share and communicate confidential information appropriately and securely when it is necessary for them to do so in relation to their role within the school. This policy reflects good practice and is in line with The General Data Protection Regulation (GDPR) which replaces the EU's 1995 Data Protection Directive 95/46/EC.

This policy and the procedures that support it have been developed to reduce the Risks associated with the loss of confidential data held on portable media.

Silverhill School recognises that in the vast majority of cases, losses of confidential information are caused by human error- a USB stick or paper file is lost or mislaid, or in circumstances beyond the individual's immediate control e.g. a laptop is stolen from someone's flat or their car.

To reduce this risk, all staff and other users given access to school information must take the simple common sense precaution of not downloading confidential data to portable media or taking it out of paper filing systems and away from the workplace unless this is absolutely necessary to conduct school business.

Information held on a portable device must always be a ***copy*** of an original held on the school IT system. This is necessary to ensure that this information remains accessible to authorised users even if the portable device is lost, damaged or stolen.

If you suspect that confidential information in your care has been lost, stolen, tampered with or disclosed without authorisation, you ***must*** report the incident immediately.

Email
Many staff are required to use and communicate confidential information in the course of their work, by using the school email systems.

This policy is not intended to stifle the vital flow of confidential data necessary to keep the school working effectively. However, all users of confidential school information have a responsibility to take appropriate measures to minimise the risk of this data falling into the hands of people who do not have the right to see it. (See **'Email Best Practice Guidelines for Staff'**.)

Memory Sticks
This document is based upon good practice principles and is intended to minimise the risks associated with the use of memory sticks.

A memory stick (also known as a pen drive, thumb drive, USB stick, etc.) is a small device that connects to the USB port of a computer and is used to store information.

A memory stick should not be used as a primary data storage device; it should only be used as a secondary or transporting device. In this case it may require backing up; this should be done regularly, preferably to a network drive.

When working on a home or non-school computer, ***do not*** copy files onto the computer; work on them directly on the memory stick – this will avoid leaving copies of the files on the PC; files can often be retrieved on a computer's hard disc even after they have been deleted.

Deleting Files
As a matter of good practice, information on memory sticks should be removed/deleted as soon as it is no longer required.

When files are deleted from a memory stick, it is sometimes possible to retrieve them. The only way to be sure that files are permanently deleted and cannot be retrieved is to format the memory stick; this will not normally be necessary for memory sticks that are encrypted, however if you need to do this, please ask for help from the Front Office.

Encrypted Memory Sticks
If an encrypted memory stick is lost or stolen the contents are protected against unauthorised access.

The school has a limited number of encrypted memory sticks which are available for staff to use should they need to take sensitive data (including pupil reports) off-site.

A Silverhill School issued memory stick is identifiable and its issue will be recorded. It must not be left in the possession of any person other than the individual it was issued to.

School issued memory sticks (not encrypted)
These are available for all staff to copy and use for non-sensitive information. Staff should ensure that if they are copying non-sensitive information that they will only use these sticks. This is to help reduce the possibility of infected material being transferred to the school's IT system.

It is permissible to use a school issued memory stick in conjunction with a home or third party computer for school work being undertaken by a staff member. Where children are asked to deliver a project which may require the use of a memory stick, staff should ensure that these children use a school-issued memory stick and are instructed that these are for use with school work only.

When teaching or delivering a presentation and there is no viable alternative to using a memory stick, you ***must*** ensure that a school-issued memory stick is used.

Laptops
The school has one laptop which is not connected to the intranet. It is used solely as a vehicle to display information on the overhead projectors.

Laptops used for children with additional needs are the responsibility of the owner but will be checked by our IT provider for existing malware and checked to ensure that they have up-to-date anti-virus software.

IPads
The School has a number of IPads which are managed by our IT provider. These are password protected and have restricted access. These IPads have been enabled with 'Find my IPad' which will allow for our IT provider to remote delete data from the device if they are notified of its loss.

Permission must be sought from a manager if a member of staff needs to take an IPad off-site. Where staff have been granted permission, they ***must*** ensure that all photos have been downloaded and that no photos are stored on the device before taking the IPad off-site.

The School has a separate policy for their software 'Tapestry' (5.08) and Early Years staff are required to sign a 'Use of Technology Devices by Staff Agreement'.

Accessing school emails via mobile phones
Most staff will have their work email uploaded on their personal mobile phone. Whereas the school recognises that it cannot insist, we ask that staff ensure all personal mobile phones are password or fingerprint protected.

Remote Access
Remote access is available to a very limited number of staff. Where remote access has been granted we require the user to have a computer which is password protected and updated with the latest protection software. Silverhill School acknowledges that access of data in this manner has a level of risk, and that we depend on the integrity of the member of staff concerned to ensure that they will use this service in a responsible manner. Remote access must only be used via a personal network over which the user has complete control.

Teaching staff have access to our Pupil Management system via a secure portal.

Failure to comply with this policy is a disciplinary offence which may include action up to and including dismissal. Serious breaches of the policy, whether intentional or nonintentional, and which place Silverhill School at serious financial, commercial or reputational risk or actual loss may be considered as gross misconduct offences, for which summary dismissal may be an outcome.

This policy was adopted by	Silverhill School
Date	June 2018
Review Date	January 2019
Name of signatory	Jenifer Capper
Role of signatory	Head Mistress