Silverhill Primary School

Off Site Working Policy

Policy No.	Issue date January 2019	Review date January 2020

Contents

1 Introduction and scope

This Policy forms part of the Schools Information Governance Framework.

The school is committed to information security to protect its highly valued information assets, in line with relevant legislation and requirements. This should be read in conjunction with the Data Protection Act (GDPR) Policy and the School Information Security Policy.

This Policy has been developed to promote good information security practices outside the boundaries of school premises. The security issues in this Policy relate to the physical security of mobile computer equipment, mobile storage devices and includes the security of data held on them.

2 Definition

Information security is put into practice through appropriate controls which could be a combination of policies and procedures, guidelines and common sense.

The definition of mobile computer equipment includes all portable equipment that has any data processing capability including but not limited to:

Laptops
Notebooks
Tablets
Personal Digital Assistants – PDA's and smart phones such as iPADs and iPhones.

The definition of mobile storage device includes but is not limited to…

Universal Serial Bus – USB – port devices such as pen drives, flash drives and memory sticks
Hand held wireless devices such as Bluetooth
External hard drives

Personal data means data which relates to a living individual who can be identified from that data.

Occasionally it is necessary for employees to take work off school premises to work remotely, whether that be at home or to another location.

There are many additional risks to information security that result from this. Mobile computing devices are attractive, portable and easy targets for the opportunist thief. They are susceptible to loss, hacking and the distribution of malicious software – viruses. They are often used for storing personal and/or sensitive information, particularly about pupils/students that could be of more value that the device itself, and which if lost or stolen could have very serious financial and reputational implications to the school and its employees.

This Policy relates to physical security and information security when using mobile computing equipment and/or paper records when working off site.

3 Security of mobile computing equipment, mobile devices and data

Personal data must **never** be stored on an unencrypted mobile storage device.

Mobile computing equipment and the data held on them must be protected by adequate security. They must be:

- kept out of sight - for example in the locked boot of the car when being transported
- kept secure and guarded from theft and unauthorised access at all times - if you are working on information involving children at home make sure no other member of the family can access this information
- carried separately and concealed wherever possible by using an ordinary bag or rucksack rather than a laptop case
- protected from 'shoulder surfing' - when in public, make sure no-one can see your password or any other information
- backed up to a local server at the earliest opportunity or to an encrypted external hard drive. File and data housekeeping should be performed to make sure obsolete data is not kept any longer than necessary. Unencrypted external drives **must not** be used.
- locked away or put out of sight when not being used – this includes at home
- They must not be left unattended - for example do not leave them in your boot overnight even if kept in a locked garage
- School pupil/student information must not be loaded onto personal mobile devices without the explicit authority from the Head Teacher

4 Other relevant policies, procedures and standards

This policy should be read in conjunction with the following policies

- *Information security policy*
- *Data Protection Act (GDPR) policy*

5 Compliance with the Off Site Working Policy

The Head Teacher is responsible for monitoring compliance with this Policy.

If employees knowingly or recklessly fail to comply with this Policy, other school policies, procedures or guidelines the school may take appropriate action under the Disciplinary Procedure.

6 Contact Details

Please contact Jason Coupland, School Business Manager with any queries in relation to this Policy.

Please contact the Council's data protection officer on 64 0763 or by email to data.protection@derby.gcsx.gov.uk with enquires in relation to any referenced law or with information governance related queries.