Silverhill Primary School

Information Security Policy

Policy No.	Issue date	Review date
	January 2019	January 2020

Contents

1 Introduction and scope

This Policy forms part of the Schools Information Governance Framework.

The purpose of information security is to protect the highly valued information assets of the school. The objective is to reduce the risk of security incidents and be able to demonstrate to pupils/students, parents and employees that we collect, handle and store their information securely. It also shows a commitment by the school to process information in line with relevant legislation and e-Government requirements.

The policy applies to all school employees, including contractors and agency workers who have authorised access to school IT systems.

2 Definition

The International Standard ISO/IEC 27001:2005 standard specification for Information Security Management defines Information Security as protecting three aspects of information:

- ***confidentiality-*** making sure that information is accessible only to those authorised to have access
- ***integrity-*** safeguarding the accuracy and completeness of information and processing methods
- ***availability-*** making sure that authorised users have access to information and associated resources when required.

Information comes in many forms. It can be:

- stored on computers
- sent across networks
- printed out
- written
- spoken
- visual

Information Security covers the safekeeping of all forms of information to protect its confidentiality, integrity and availability.

This is put into practice through appropriate controls, which will be a combination of policies, procedures, standards, guidelines, common sense and physical or hardware/software measures.

3 Responsibilities and accountabilities

The Head Teacher has responsibility for defining and setting the school's information security policies, standards and procedures. Every IT system user who has access to school information is responsible and accountable for putting into practice these policies, standards and procedures.

Information Security is not an option. We are all required to keep a minimum level of security to meet our legal and contractual obligations.

4 Compliance with legal and contractual requirements

The school has an obligation to make sure that all information systems and processes meet the terms of all relevant legislation and contractual requirements, including the:

- General Data Protection Regulations (GDPR) 2018
- Data Protection Act 1998
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Freedom of Information Act 2000

Jason Coupland, School Business Manager, has specific responsibility for the Data Protection Act and notifications to the Office of the Information Commissioner.

5 Actions required to maintain confidentiality, integrity and availability

- Everyone has a responsibility to make sure that personal information is only collected, used, stored and shared for the purpose it was provided.
- Make sure any requests for personal information are handled in accordance with the GDPR. Information should only be disclosed on a need to know basis. Always make checks on the identity of callers.

- Make sure printed or hand written personal information is kept secure at all times.
- Make sure printed or hand written personal information is disposed of in a secure manner.
- Never dispose of personal information in general waste.
- Always use the computer screen lock facility where personal information may be held on the hard drive of a PC or laptop when the device is logged in and unattended.
- Never share user names and passwords. Never encourage others to anyone else's personal ID and password to log into a PC, the network, individual system or email.
- It is a criminal offence under the Computer Misuse Act 1990 to access a computer system without authority to do so.
- Be aware that emails are not usually a secure method of sharing personally identifiable information external to the school.
- To avoid introducing viruses into the School network never open email attachments from unknown external sources.
- Make sure you set your password to the minimum standard required. Keep them secure and change them regularly.

6 Other relevant policies, procedures and standards

This policy should be read in conjunction with the following policies:

- *Data Protection Act (GDPR) policy*
- *Off site working policy*

7 Compliance with the Information Security 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.

8 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 about this policy or any other referenced policy, procedure or law.