Information and Security Policy
2017-18

Introduction

The school's investment in the acquisition, storage and use of electronic and paper based information exists primarily to help provide the effective delivery of its services. This information is held about a variety of people and it is essential that the availability and confidentiality of accurate relevant information is maintained in a secure and legal environment.

The school is committed to achieving policy requirements through an Information Security process. To actively demonstrate this, the Council has issued a Commitment Statement which provides assurance to pupils, parents, governors and staff that sound and secure measures are in place to protect the confidentiality, integrity and availability of their information.

Objective

The information security objective is to ensure that the school's information base is protected against identified risks so that it may continue to deliver its services and obligations to the community. It also seeks to ensure that any security incidents have a minimal effect on its business and academic operations.

Policy

The purpose of this policy is to protect the school's information assets from all threats, whether internal or external, deliberate or accidental.

The key aims of the policy are to ensure that:
- information is protected from unauthorised access
- confidentiality of personal or sensitive information is assured
- integrity of information is maintained
- information is disposed of in a timely, appropriate and secure manner
- legislative requirements and school policy and practices are observed
- business continuity plans are produced, maintained and tested
- information security training is available to all school staff
- appropriate monitoring and reporting processes are put in place to identify and act upon breaches of information security

Supporting framework

In order to achieve this, the school will develop and maintain information security standards. Procedures, working practices and protocols will be developed to support this policy. Examples of measures to achieve the above are physical security, virus control and the use of passwords for access control. The development of any new system will include information security analysis and requirements as part of the initial specification.

Responsibilities

The Headteacher has direct responsibility for maintaining this policy and providing advice and guidance on its implementation. The Headteacher will also have responsibility for ensuring that the school's Management Team monitors the implementation and maintenance of the policy and its associated standards.

All staff are responsible for policy implementation and for ensuring that staff they manage also adhere to the standards.

Implementation

This policy will be made available to all pupils, parents, guardians, staff (whether permanent or temporary) and governors.