ICT Security Policy

This Policy has been adopted by the Governing Body on the 20TH January 2011 and will be reviewed annually thereafter.

Objectives of the Policy

The purpose of this policy is to protect the School's information asset by ensuring the:

Availability: information is and continues to be accessible and usable as normally required

Integrity: information is assured with regard to version, accuracy, freedom from corruption

Confidentiality: information is restricted to the people and for the purposes intended

Definition and Classification of Information

Information within this Policy means data, programs, documents, spreadsheets, databases, electronic mail messages, images and maps of all types regardless of how or where within the School the information is stored or managed.

Information Backup

The headteacher/nominated officer must make sure that appropriate procedures are in place to maintain the confidentiality of the information and to recover from the temporary or permanent loss of the information or supporting equipment

All information must be protected by a procedure for archiving and copying for security backup. The procedure must incorporate daily, weekly, monthly, year end cycles appropriate to the type of information, frequency of update, legal and operational requirements.

Security back up copies must be stored wherever possible off site from the location at which the operational information is maintained.

The ability to restore information from back-up copies must be tested periodically to ensure that procedures, equipment and storage media are performing correctly.

Compliance With Legal Requirements

All computer media must be stored and disposed of with due regard to its sensitivity and the requirements of the Data Protection Act.

Disclosure of information must be in accordance with the Data Protection Act.

General Compliance

Unlicensed, illegal or unauthorised software or information must not be installed, used, copied, altered or distributed.

Illegal or improper access to external networks, services or facilities is prohibited.

Access Control

In accordance with section 5 of the Financial Regulations the Director of Finance and IT's auditors will have access as necessary to any information and applications systems.

Any method of log-on which nullifies the password control is prohibited

Passwords must not be printed or displayed on input

Each user must have their own user ID and password. The use of another person's user-ID is not allowed.

Passwords must be a minimum of five characters and must be changed in accordance with procedure and immediately it is suspected that the password has been disclosed. The change should be to a previously unused password.

Access rights for all leavers should be removed immediately.

Access rights for all users should be reviewed and updated periodically.

Equipment

Headteachers are responsible for IT facilities installed within the school and for ensuring their proper use. The use of IT facilities not directly concerned with the School's business is prohibited.

All items of equipment must be security marked in accordance with the School's risk management policy and included on the inventory.

Where ever equipment must not be kept in an area that is unsecure, accessed by members of the public or unsupervised representatives of other organisations. The following measures should also be considered for additional protection;

- Fire detection and prevention
- Intruder alarm

Where equipment is located within areas accessed by members of the public or in unsecured offices and left unattended for periods of time, the following measures must be considered to deter the theft of that equipment:

- Steel cable attachments locking equipment the work surface
- Improved security of the outer walls and windows

Terminals and PC's must not be left unattended when logged in to applications. If not in use they must be logged out or protected by a secure screen saver. Users must log out of the systems and the network before signing out of work and also switch off their terminal/PC/printer.

Personal Systems and Portable PCs

No equipment must be removed from its location without the permission of the Headteacher who must be satisfied that appropriate arrangements have been made for insurance of equipment and information.

The removal of this equipment should be recorded and monitored.

Equipment must not be left in unattended vehicles for which insurance is not available.

Disposal of Obsolete Computer Equipment

The disposal of obsolete computer equipment is governed by the Schools ' Scheme of Financial Administration'.

The Governing Body should authorise all write offs and disposals of surplus stocks and equipment in accordance with LEA or DFE regulations.

All information has been physically deleted, corrupted or overwritten so as to make it irrecoverable.

Software is not offered to an external agency unless there is a legal right to do so and licence records are adjusted accordingly.

The inventory is updated to record the disposal.

General

This Policy should be read in conjunction with the School's Internet Security Policy and alongside the Wigan Acceptable Use of IT equipment guidance document.

Reviewed	August 2012
Reviewed	August 2013
Reviewed	August 2014
Reviewed	August 2015
Reviewed	August 2016
Reviewed	August 2017
Reviewed	August 2018
Reviewed	August 2019
Reviewed	August 2020
Reviewed	August 2021
Reviewed	August 2022
Reviewed	August 2023