COMPUTING SECURITY POLICY
DUNCOMBE PRIMARY SCHOOL

Reviewed By: Governors Finance Committee

(In conjunction with Data Protection Policy)

Reviewed: February 2018

Next Review Date: February 2019

COMPUTING SECURITY POLICY DUNCOMBE PRIMARY SCHOOL

SUMMARY

The objectives of this Policy, which is intended for all school staff, including governors, who use or support the school's Computing systems or data, are to:

- Ensure the protection of confidentiality, integrity and availability of school information and assets.
- Ensure all users are aware of and fully comply with all relevant legislation.
- Ensure all staff understand the need for information and Computing security and their own responsibilities in this respect.

Definitions

Information – Covers any information, including electronic capture and storage, manual paper records, video and audio recordings and any images, however created.

Personal Data – Any data which can be used to identify a living person. This includes names, birthday and anniversary dates, addresses, telephone numbers, fax numbers, email addresses and so on. It applies only to that data which is held, or intended to be held, on computers ('equipment operating automatically in response to instructions given for that purpose'), or held in a 'relevant filing system'. This includes paper filing systems.

Strong Password – A password that has a minimum of 8 characters. It contains upper and lower case alphabetical characters and numbers or punctuation characters. It should not contain dictionary words, the owner's date of birth or car registration number.

Encryption – Process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

Responsibilities:

- The school shall be registered with the Information Commissioner's Office (ICO) under the 1998 Data Protection Act.
- Users of the school's IT systems and data must comply with the requirements of the Computing Security Policy.
- The School's Leadership Team and Governors shall review this document at least annually.
- Users shall be responsible for notifying the System Manager and Headteacher of any suspected or actual breach of computing security.
- ***The Headteacher shall inform both ICO and the Director of Children & Families, Islington Council if there are any losses of personal data.***
- Users must comply with the requirements of the Data Protection Act 1998, Computer Misuse Act 1990, Copyright, Designs and Patents Act 1988 and the Telecommunications Act 1984.
- Users must be provided with suitable training and documentation, together with adequate information on policies, procedures and facilities to help safeguard systems and data.
- Adequate procedures must be established in respect of the Computing security implications of personnel changes.

- No personal data shall be taken from the school unless it is on encrypted media. This includes, but is not exclusive to, laptop computers, net books, external hard disks, memory sticks and Personal Digital Assistants (PDAs) and other removable media.
- Remote access to information and personal data shall only be provided through an encrypted link and users shall require a strong password that is renewed at least termly.
- Users shall not publish spreadsheets, databases or other documents containing personal data on externally accessible web sites including the London MLE unless these documents are encrypted.

Physical Security:

- As far as practicable, only authorised persons should be admitted to rooms that contain servers or provide access to data.

- All computers must be locked with a steel sable lock.

- Computers should not be relocated without authorisation from the system manager.

- Server rooms must be kept locked when unattended.

- Appropriate arrangements must be applied for the removal of any computing equipment from its normal location. These arrangements should take into consideration the risks associated with the removal and the impact these risks might have.

- All school owned computing equipment and software should be recorded and an inventory maintained.

- Uninterruptible Power Supply (UPS) units are recommended for servers and networks cabinets.

- Computer monitors should be positioned in such a way that information stored or being processed cannot be viewed by unauthorised persons.

    Do not leave sensitive or personal data on printers, computer monitors or desk whilst away from your desk or computer.

    Do not send sensitive/personal information via e-mail or post without suitable security measures being applied.

- Ensure sensitive data, both paper and electronic, is disposed of properly e.g. shred paper copies and destroy disks.

System Security:

Users **shall not** make, distribute or use unlicensed software or data.

Users **shall not** make or send threatening, offensive or harassing messages.

Users **shall not** create, possess or distribute obscene material.

- Users must ensure they have authorisation for private use of the school's computer facilities.

- Passwords should be memorised. If passwords must be written down they should be kept in a secure location.

- Users who regularly access personal data shall have a unique user ID and a strong password that is renewed at least termly.

  Passwords **shall not** be revealed to unauthorised persons.

  Passwords **shall not** be obvious or guessable and their complexity should reflect the value and sensitivity of the systems and data.

- Passwords shall be changed if it is affected by a suspected or actual breach of security e.g. when a password may be known by an unauthorised person.

- Regular backups of data, in accordance with the recommended backup strategy, must be maintained.

- Security copies should be regularly tested to ensure they enable data restoration in the event of system failure.

- Security copies should be clearly marked and stored in a fireproof location and/or off site.

Virus Protection:

- The school should ensure current and up to date anti-virus software is applied to all school computing systems.

- Laptop users shall ensure they update their virus protection at least weekly.

- Any suspected or actual virus infection must be reported immediately to the System Manager/Computing Co-ordinator and that computer shall not be reconnected to the school network until the infection is removed.

Disposal of Equipment:

- The School shall ensure any personal data or software is obliterated from a PC if the recipient organisation is not authorised to receive data.

- It is important to ensure that any software remaining on a PC being relinquished for reuse is legitimate. Care should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently.

- The School shall ensure the requirements of the Waste from Electronic and Electrical Equipment (WEEE) Directive are observed.