

OFFICE COMPUTER SECURITY POLICY



Latest review undertaken on 30th January 2012

By the Finance and General Purposes Sub-Committee

Ratified by the Full Governing Body on 23rd February 2012

Next review: Spring term 2013

Physical Equipment Security

- Where possible computer equipment will be sited so as to reduce the risk of unauthorised access and damage.
- The details of all computer equipment will be recorded in the official inventory record together with relevant serial numbers.
- Computer hardware will be appropriately security marked.
- A record will be kept of any computer equipment taken off site, with the exception of laptops issued under the 'Laptop for Teachers Scheme'. The removal of equipment from the academy's premises must be authorised by the principal.
- The officer responsible for physical equipment security is the principal.

Backup Procedures

- All data held on the academy's computer system will be backed up at least daily and a copy is taken off site.

Virus Detection

- All computers will have virus detection software installed within their start-up procedures. The software should be updated regularly.
- Any disks of uncertain origin must be scanned for viruses before use.
- The use of unlicensed software is prohibited.
- The officers responsible for virus detection procedures are the ICT technicians

Software controls

- All software maintained on the academy's computers must be properly owned by the academy. Software may only be used in accordance with the licence agreements.
- All system disks will be held in a secure area.
- An inventory of all software maintained on the academy's computers will be kept together with relevant serial numbers where possible.
- Access to software will be restricted to authorised staff.
- The Systems Manager and the identified office support are the only persons who may issue passwords and amend access levels.
- Users of the academy's computer system will be issued with individual passwords.
- It should be ensured that passwords are kept confidential. They should be changed regularly.
- Staff should log out of the computer system before leaving the office unattended.
- Staff should lock/log off their machines whenever they are to be left unattended.
- When staff leave, their account will be disabled by the Systems Manager.

- Any suspected breach of security will be immediately reported to the principal.
- The officer responsible for software control is the principal and added to our new e-incident log.

Legal Obligations

- All staff should be made aware of the requirements and their responsibilities in relation to the following legal statutes: 1984 Data Protection Act

Acquisition, Maintenance and Disposal of Hardware

- The principal has overall responsibility for the acquisition, maintenance and disposal of equipment.
- Official orders will be used to make any purchases.
- The write off and disposal of equipment should be authorised by the Governing Body and the principal
- Acquisition and disposal of equipment must be in accordance with the Financial Regulations for Schools.

User Training

- Users should receive appropriate training in the correct use of the school's IT facilities including use of software packages and security arrangements.

Disaster Recovery

- The arrangements in place for disaster recovery are to maintain up to date back-ups and to contact Insight.
- The officer responsible for disaster recovery is the principal.

Internet Access

- There will be adequate procedures in place to ensure that access to the Internet is restricted to authorised staff.
- The officer responsible for ensuring Internet access is restricted is the principal.

Good Password Practice for Users

Difficult-to-Guess Passwords

Passwords are an essential component of Hadrian Academy Trusts computer and network security systems. To ensure that these systems do the job they were intended to do, users must choose passwords that are difficult to guess. This means that passwords must not be related to one's job or personal life. For example, a car license plate number, a spouse's name, or fragments of an address should not be used. This also means passwords should not be a word found in the dictionary or some other part of speech. For example, places, technical terms, and slang should be avoided.

Easily Remembered Passwords

Users can choose easily-remembered passwords that are at the same time difficult for unauthorised parties to guess if they:

- a) String two or three words together (the resulting passwords are also known as "passphrases"). For example, "BILLIS34" or "3BLINDMICE" or "TEA4TWO".
- b) Shift a word up, down, left or right one row on the keyboard. For example, "WALTER" becomes "2QO534" by using the keyboard character from the line above and to the left of the original password.
- c) Bump characters in a word a certain number of letters up or down the alphabet.

- d) Transform a regular word according to a specific method, such as making every other letter a number reflecting its position in the alphabet.
- e) Combine numbers with a regular word.
- f) Create acronyms from words in a song, a poem, or another known sequence of words.
- g) Deliberately misspell a word (but not a common misspelling)
- h) Combine a number of personal facts like birth dates and favourite colours.

Repeated Password Patterns

Users must not construct passwords with a basic sequence of characters that is then partially changed based on the date or some other predictable factor. For example, users must not employ passwords like "XY12JAN" in January, "XY12FEB" in February, etc. Additionally, users must not construct passwords that are identical or substantially similar to passwords they have previously employed.

Password Constraints

No password should be less than six characters long. Passwords of seven or more characters (because they are more difficult to guess) offer greater security. It is recommended that passwords contain at least 3 of the following features: Upper Case, Lower Case, Numbers or Symbols.

Password Storage

Passwords must not be stored in readable form in PC files, automatic log-in scripts, software macros, terminal function keys or in any other locations where unauthorised persons might discover them. Similarly, passwords must not be written down and left in a place where unauthorised persons might discover them. However, all passwords should be written down and stored in the safe in case of emergency.

Sharing Passwords

Regardless of the circumstances, passwords must never be shared or revealed to anyone else besides the authorised user. To do so exposes the authorised user to responsibility for actions that the other party takes with the disclosed password. Additionally, the person using a password disclosed to him/her by the authorised user is automatically using another person's ID; and both of these actions are prohibited. If users need to share computer-resident data, they should use electronic mail, public directories on local area network servers or other secure mechanisms.

Review :

This policy is to be reviewed annually. Next review will be Spring 2013.