KINETON GREEN PRIMARY SCHOOL

ICT SECURITY POLICY

September 2021
(Revise 2024)

Introduction

This is a summary of the ICT Security Policy agreed by the Kineton Green. You should make sure that you read and understand it.

As Kineton Green relies heavily on ICT systems, security becomes ever more important to ensure confidentiality and safety of information.

It is important, therefore, for staff to understand and observe our ICT security policy. These notes are to help you. Training is also available if required.

With some computer crimes carrying a prison sentence, it is important that you know what you should and should not do.

The ICT security policy is designed to help rather hinder us in our work and also applies to confidential and sensitive information on manual files.

ICT Equipment

Make sure that ICT equipment is protected against theft and malicious damage. Is it in a reasonable environment; not too hot (or cold) or dusty? If you are not comfortable working there, neither is a computer!

Do not leave a laptop computer or tablet device e.g. iPad unattended in a vulnerable place, e.g. the boot of a car, or an unlocked, unmanned office. Laptops and table devices will not be left unattended in public view during holidays or events where the school is open to the public e.g. school fayres, these will be placed out of view, ideally in a locked cupboard.

Where possible, place computer screens so that only authorised staff can read them.

Only equipment with ICT Services Help Desk labels is allowed to connect to the Kineton Green's network. Under no circumstances should consultants, contractors or visitors be permitted to connect to the Kineton Green's network with their own equipment. Kineton Green equipment – e.g. desktops, laptops, tablet devices or PDA's used at home – must not be configured to attach directly to the Internet, to other company networks or to home networks, unless configured to do so by ICT Services.

Use of On-Line Systems

Every member of staff authorised to use an on-line system is given a password. It is important that you do not tell anyone else what your password is; you must never allow anyone else to login to a system using your name and password.

If a person leaves or changes jobs, their access to computer systems should be removed or amended immediately.

In order to protect yourself and the system, follow some simple rules:

- The very first time you logon to a system, change your password from the default one you have been given. (If you need help to do this, please contact the Help Desk on ext. 6246).

- Create a **strong password** that is easy for you to remember but difficult for others to guess. A strong password is one that is at least 8 characters, and includes a combination of letters, numbers and symbols. The easiest way to create one is to think of a phrase that is meaningful to you, and then select the

first letter of each word. For example, "My son Aiden is three years older than my daughter Anna", would create the password "MsAityotmdA".

- Do not write your password down, or save it in a file on your computer – select a phrase to create it from that you know you can remember.

- Do not tell anyone your password.

- If you think that other people know your password, change it.

- Change your password at least every 28 days.

- Do not use a selection of passwords in rotation – create a new one each time.

- If you use a laptop, it should be protected by a BitLocker code. The school BitLocker code is managed by the office and Computing co-ordinator. The same rules for password management described above should be followed.

    - If you use a tablet device e.g. I pad you must pin protect the device if it is to be used by a member of teaching staff only. If it is used by children the device any apps that are for staff only must be pin protected. The device must also be "locked down" as per the advice of the ICT services team to prevent children from accessing certain areas of the device e.g. the ability to purchase apps for the device.

    - Do not leave a tablet device unattended without securing it with the PIN if it is PIN protected.

    - Only password protected memory sticks or external hard drives must be used if taking data off the school site. The same rules for password management described above should be followed.

- Do not leave a PC or terminal unattended when "signed on". As soon as you have finished, "sign off".

Privacy

Ensure that confidential information can only be accessed by authorised staff.

Challenge any stranger or unauthorised person who tries to use a PC or terminal in your office, or who is reading printouts.

The Data Protection Act has serious implications for us: make sure that you understand them, and ask for training if you do not.

Software Piracy

Installing unauthorised software on a Kineton Green PC is a disciplinary matter. Software should only be installed by authorised personnel, unless you have the agreement of ICT Services (we will need an audit trail of any such permissions, so log a help desk call if you need any software installed). It is a criminal offence to "pirate" software.

Software Viruses

To minimise the risk of computer "virus" infection, you must make sure that any CD-ROMs from other Directorates or third parties are virus checked before loading on a Kineton Green PC.

Kineton Green laptops must be connected to the network regularly – at least once a month – so that security updates and anti-virus software updates can be applied.

Personnel Policy

Disciplinary offences include:

- Use of another person's password
- Unauthorised disclosure of information
- Loading "pirate" or borrowed software
- Connecting a Kineton Green PC, laptop, tablet device or PDA to any non-Kineton Green network
- Unauthorised access to, copying, altering or interference with programs and data

Laptop Responsibility

Staff will read and sign the school's hardware agreement document when they are assigned a teaching laptop.