<u>Introduction</u>

It is the intent of this policy to establish guidelines for <u>all users</u> (staff / students / guests) using Pavilion Study Centre's ICT facilities, including computer hardware, printers, fax machines, voice-mail, software, e-mail, and Internet, intranet access and telephony collectively called "Information Communication Technology".

The policy supports Data Protection legislation in general terms, with the right to privacy protected where this is not contrary to any guidelines put forth by the School, the Government and the law in the UK.

All Users share the Information Communication Technology facilities at Pavilion Study Centre. These facilities are provided for the purpose of conducting School business and promoting learning.

The School does permit a limited amount of personal use of these facilities (including computers, printers, e-mail and Internet access). However these facilities must be used responsibly by everyone.

All Users are expected to behave responsibly and ethically when using the School's Information Technology facilities. Any action that may expose the school to risks of unauthorized access to data, disclosure of information, legal liability, or potential system failure is prohibited and may result in disciplinary action up to and including termination of employment and/or criminal prosecution.

Guidance is provided to support the implementation of this policy.

POLICY:

- The use of the School's Information Communication Technology facilities in connection with school business and limited personal use is a privilege but not a right, extended to all users.
- Users of Pavilion Study Centre's computing facilities are required to comply with all policies/guidance referred to in this document.
- Users must also agree to comply with the applicable country and local laws and to refrain from engaging in any activity that would subject the company to any liability.
- It is the responsibility of any Pavilion Study Centre employee, student, contractor, or third party to protect the school's assets. (Stolen assets are a direct cost to the school and not automatically recovered via insurance, and depending upon the circumstances, you may be asked to pay for any loss).
- Pavilion Study Centre reserves the right to amend this policy, guidance and practices at any time without prior notice and to take such further actions as may be necessary or appropriate to comply with new legislation and guidelines.
- In order to protect the integrity of Pavilion Study Centre's computing facilities and its users against unauthorized or improper use of those facilities, and to investigate possible use of those facilities in violation of school rules and policies, Pavilion Study Centre reserves the right, without notice, to limit or restrict any individual's use, and to inspect, copy, remove, or otherwise alter any data, file, or system resource which may undermine the authorized use of any computing facility or which is used in violation of school rules or policies.
- Pavilion Study Centre also reserves the right periodically to examine any system and other usage and authorization history as necessary to protect its ICT facilities.
- Pavilion Study Centre reserves the right to use monitoring software to ensure that the system is being used responsibly.
- Pavilion Study Centre disclaims any responsibility for loss of data or interference with files resulting from its efforts to maintain the privacy and security of those computing facilities or from system malfunction or any other cause.

This policy and guidance covers the usage of all of the school's Information Technology and communication resources, including, but not limited to:

- All computer-related equipment, including desktop personal computers (PCs), portable PCs, terminals, workstations, PDAs, wireless computing devices, peripheral hardware (cameras etc), telecommunications equipment, networks, databases, printers, servers and shared computers, and all networks and hardware to which this equipment is connected
- All electronic communications equipment, including telephones, pagers, radio communicators, voice-mail, e-mail, fax machines, PDAs, wired or wireless communications devices and services, Internet and intranet and other on-line services
- All software including purchased or licensed business software applications, school applications, employee or vendor/supplier-written applications, computer operating systems, firmware, and any other software residing on school-owned equipment
- All intellectual property and other data stored on school equipment
- All of the above are included whether they are owned or leased by the school or are under the school's possession, custody, or control
- These policies also apply to all users, whether on school property, connected remotely via any networked connection, or using school equipment.

Guidance for Staff and other adult users

<u>General issues</u>

❖ All users must keep user names and passwords secure and change them when prompted.
❖ The use of memory sticks and other storage devices is permitted but please use them sensibly and appropriately.
❖ Theft is a real concern. Always lock classroom doors and secure equipment where possible.

<u>Portable appliances (including laptops)</u>

❖ Do make sure you always lock portable computers away overnight in a secure, predetermined location. You may want to check with your line manager, or contact the ICT department to make sure.
❖ Do carry your laptop with you as hand luggage, if you are travelling by airplane.
❖ *Do keep the laptop password protected using a strong and challenging password (8 characters minimum including lower and upper case letters, numbers and/or prefixes). Enable the password protected 'lock out'.*
❖ Laptops do not like water so keep them away from any exposure to water or being left in wet places.
❖ Return your laptop regularly to the ICT department for antivirus updates and security check up.
❖ Do not attempt to install any software or hardware into your laptop without checking with the ICT department before hand and having approval or guidance to do so.
❖ Your laptop should not be used for any purpose that is prohibited by the school even outside the school network.
❖ Do make sure to back up and secure local data on your laptop in case of it being stolen and or the data being lost. *All 'sensitive' data should be password protected.*
❖ Do report any loss immediately to the police and obtain a crime reference number. Notify your line manager detailing all systems you have access to, so that immediate action can be taken to restrict unauthorised access.
❖ Do not leave school assets unattended in public places or in your car overnight.

<u>Software</u>

Software is the systems program or application which runs on your PC. When you buy software you are buying the right to use it. Using unlicensed software is against the law. Copyright laws and licences may cover all fonts, graphical images, texts, and manuals.

❖ Only use Pavilion Study Centre approved software which is certified to be used on your laptop (or other portable equipment) and or PC. This includes tools and applications.
❖ The use of shareware or freeware that is not approved by the school's ICT department may cause harm or expose the school's ICT network to security risk or damage. Do not attempt to download any software from the internet (even if you are tempted by being advised that it is free).
❖ All software must be approved and installed by Pavilion Study Centre's ICT department.
❖ Do not underestimate the potential seriousness of using unlicensed software. It is a disciplinary offence. You may incur a fine and will be personally liable for any civil or criminal damages if you are caught using unlicensed software.

E-Mail

Only the school email system is permitted to be used to send / receive email messages for school staff and students. It is the only email facility to be used to conduct school business. Messages sent externally are considered formal correspondence and you must ensure that they are of a professional nature and do not contain anything which may breach ICT security policy.

- ❖ Do be wary of email, email attachments, from unexpected sources as it may contain a virus. If unsure, note the details and report to the ICT department.
- ❖ Do avoid sending any unprotected, confidential data by email over the Internet.
- ❖ Do not install or access private personal email services unless approved by the school.
- ❖ Do not send material, illegal messages or messages with contents that may be considered to be offensive, defamatory, that may offend readers on the grounds of their sex, sexual orientation, race, age, colour, nationality, religion, martial status, or disability using school email or ICT facility. Messages of such nature are liable to prosecution even if from a private source.

Internet

The school reserves the right to use monitoring software to ensure that the system is being used responsibly.

- ❖ The Internet is a valuable business and educational resource. The school allows reasonable personal use of the web.
- ❖ Please be aware that viruses can be imported into the organisation's system via the Internet if misused.
- ❖ Software- users should never download, load or install any software, shareware, or freeware, or load any such software from removable storage, unless they have permission from the ICT department. No user should copy other people's work or intrude into other people's files without permission.
- ❖ The use of bit torrenting software and the downloading of multimedia files from inappropriate sources is not allowed.
- ❖ Inappropriate materials or language - Profane, abusive or impolite language should not be used to communicate nor should materials be accessed which are not in line with the school's guidelines.

Data security

The school has a responsibility to keep secure any data (about students, staff, parents and carers) that could be seen as 'sensitive'. Examples of data considered 'sensitive' are names, addresses, SEN data and behaviour logs. Mark books or spreadsheets with grades on are less sensitive.

To achieve this you should:
- Keep any such data password protected using a strong and challenging password which is regularly changed. (8 characters minimum including lower and upper case letters, numbers and/or prefixes).
- Limit and control any data taken away from school on portable devices or sent by email
- Regularly sweep and delete data that is no longer needed form PCs, laptops, pdas and portable memory devices

- Ensure you log off from any machine used to access the data as soon as you have finished using it or ensure that a password protected 'lock out' is enabled.
- Never use private email addresses or personal mobile phones for school business.

N.B: Paper based sensitive data can also be lost or stolen. Take similar precautions with this.

Using ICT @ Pavilion Study Centre
Guidance for students

General stuff!
- Always report any inappropriate use to a teacher. A good rule to follow is never view, send, or access materials that you would not want your teachers or parents to see.
- Never use the computers to engage in activities that may be in violation of the law. This includes any form of 'cyber bullying'.
- No Internet games may be played during school hours.
- Do not download music/video/programmes onto the school network.
- Do not enter an ICT room until you are asked by a teacher.
- Please do not eat or drink in any ICT rooms
- Always behave appropriately in ICT rooms
- To avoid confrontation you are advised to store files on a standard memory stick rather than a phone, iPod or MP3 player.

Equipment
- You must never misuse or damage any of the equipment.
- You must never interfere with another student's computer (pulling out cables, turning screens etc).
- You must never use any of the equipment for inappropriate purposes or for anything other than school work.
- You must never access the network by using other person's User Name and Password.
- Mobile phones, iPods and other MP3 players are <u>not</u> allowed in the School. If they are brought in they must be handed in and will be returned at the end of the day
- Students in Years 7 – 11 must never listen to music in the classroom.

Software
Software is the systems program or application which runs on your PC. When you buy software you are buying the right to use it. Using unlicensed software is against the law.
- Only use Pavilion Study Centre approved software. The use of shareware or freeware that is not approved by the school's ICT department may cause harm or expose the school's ICT network to security risk or damage. Do not attempt to download any software from the internet (even if you are tempted by being advised that it is free).
- All software must be approved and installed by Pavilion Study Centre's ICT department.
- Do not download music, games, videos etc onto the school network.

Internet and email
- Notify your teacher whenever you come across information or messages that are dangerous, inappropriate, or make you feel uncomfortable.
- Be aware that the author of an Email or Web page may not be the person they claim to be.
- Do not use the school system to look at or send material (including inappropriate messages or attachments) with contents that may be considered to be offensive and that would offend readers. Messages of such nature are liable to prosecution even if from a private source.
- You are only allowed in chat rooms with a teacher's permission.
- No Internet games may be played during school hours.
- The use of messaging software other than the school's is not allowed.
- Do be wary of email, email attachments, from unexpected sources as it may contain a virus. If unsure, note the details and report to the ICT department.

E safety
- Never reveal personal information, either your own or others, such as full name, home addresses, telephone numbers and personal Email addresses. Do avoid sending any confidential information by email over the Internet.
- Never use photographs of yourself on Web pages unless a parent or guardian has given permission to do so.
- Never meet people in person that you have contacted on the Internet without parent/guardian permission.
- Always inform a teacher or other adult if you suspect someone of cyber bullying. Cyber bullying is not tolerated at Pavilion Study Centre.

If in doubt – Speak to a teacher!

Updated December 2015

Reference:-

- Regulation of Investigatory Powers Act 2000
- Data Protection Act 1998
  - http://www.opsi.gov.uk/acts/acts1998/19980029.htm
  - http://www.school-resources.co.uk/DataPrivacyandSecurity.htm
  - http://www.acas.org.uk/publications/pdf/CP01.pdf
  - http://www.acas.org.uk/publications/H02.html#1
  - http://www.primary-networks.com/policies/internet.html