

Maple Medical PRU

Acceptable Use Policy

Introduction

This policy summarises the controls to be applied that will ensure Pupils are able to use the computer device and connectivity provided by the Maple Medical PRU in accordance with e-Safety and other appropriate guidelines and relevant legislation.

Aims of the Policy

The aims of this Policy are to:

- Ensure all users are aware of the necessary steps to be taken to ensure their own safety when using the internet through the approved connectivity
- Identify the responsibilities of users in complying with the use of the computer device
- Identify the consequences of inappropriate access to information through the internet
- Identify the consequences of inappropriate use of the computer device supplied

Glossary of Terms

It is necessary to define the terms to be used, for the purposes of this policy, they are as follows:

Processing means obtaining, recording or holding the data or carrying out any operation or set of operations on the data. It includes organising, adapting and amending the data, retrieval, consultation and use of the data, disclosing and erasure or destruction of the data. It is difficult to envisage any activity involving data that does not amount to processing.

Personal Information means information that relates to a living individual who can be identified from that information and other information that is in the possession of, or is likely to come into the possession of, the data controller.

Information Access means information accessed through the computer device

User means someone who has been authorised to use the computer device and has signed and agreed to the terms and conditions, which includes complying with the acceptable use policy and all other associated policies.

Network means the school's computer network.

Computer related equipment refers to equipment that is used in relation to Information and Communications Technology.

General

Use of the computer device by authorised users is permitted and encouraged where such use is suitable for education purposes and supports the goals and objectives of the Maple Medical PRU.

The computer device is to be used in a manner that is consistent with this policy and other supporting policies i.e. The Computer Misuse Act 1990

The device and connectivity are provided to the student with certain filtering restrictions in place. This means that certain sites will not be accessible as they may be deemed unsuitable for Educational purposes, any attempt to bypass these safeguards could result in the device being removed from the user.

Sites such as Facebook, Twitter and Bebo will not be accessible through this connectivity.

The device remains in the ownership of the Maple Medical PRU.

Responsibilities

Pupils

- Adhere to the Acceptable Use Policy
- Ensure that there is no attempt to bypass this policy and other related policies.

Prohibited use of information or equipment:

- Abuse of the acceptable uses of the computer device may be an offence and may result in access being revoked and action being taken by the Maple Medical PRU.
- Any suspicion of misuse of information or equipment must be reported to the Maple Medical PRU as soon as possible.

E-mail (where permitted)

E-mail (electronic mail) is a mechanism to forward / circulate information to people anywhere in the world. In certain circumstances email may be permitted with this computer device.

The following must be considered when using any e-mail system:

Users must not:

- Send, receive, solicit, print, copy or reply to any material that is harassing, discriminatory, menacing, threatening, obscene, or in any way objectionable or offensive or which is intended to annoy, harass or intimidate another person.
This includes:
 - text that ridicules others based on their race, religion, colour, sex, sexual orientation, gender identity, national origin, veteran status, disability, ancestry or age
 - jokes (text or images) based on sex, sexual orientation, gender identity, race, age, religion, size, national origin, veteran status, ancestry or disability
 - messages that are disparaging or defamatory
 - sexual oriented messages or images
 - messages or images that contain foul, obscene or adult-orientated language
 - messages or images that are intended to alarm others, embarrass the Local Authority, negatively impact employee productivity or harm employee morale

- spread gossip, rumours and innuendos about anyone
- transmit business or personally confidential information without authorisation
- forward the work of other people without their consent to anyone
- send or forward electronic chain letters / messages
- send e-mails to large group of email addresses/recipients
- operate a business for personal gain
- transmit harmful software intentionally with any message
- use email during lessons, unless the teacher for that lesson has permitted its use
- open attachments from senders you do not recognise or that look suspicious

Users should:

- Inform a member of the staff at the Maple Medical PRU if they receive an email from an unknown person or if the email is offensive or upsetting. Do not delete the email in question until the matter has been investigated.

Internet Access

The following should be adhered to at all times:

- Users should not copy and use material from the Internet to gain unfair advantage in their studies, for example in coursework. Such actions may lead to disqualification by examination boards.
- Users should ensure that they are not breaking copyright restrictions when copying and using material from the Internet.
- Users should not attempt to bypass the filtering facility in place whilst under this project.
- Users should not attempt to access inappropriate sites – if it is suspected that such activity has taken place then the connectivity and/or device may be removed from the user

Chat Services

Students and staff are not permitted to use the chat services available on the Internet.

Bring Your Own Device (BYOD)

Students wishing to connect their personal devices to the school's wireless network must firstly seek permission and accept that, where appropriate, they must comply with the requirements and terms of this policy

Privacy and Personal Protection

Privacy will be respected unless there is reason to believe that this Acceptable Use Policy or school guidelines are not being followed.

Please ensure that as a user you should:

- respect the privacy of other users at all times
- not forward private data without permission from the author.

- not supply personal information about yourself or others via the web, email or instant messaging.
- not attempt to arrange meetings with anyone met via the web, email or instant messaging.
- realise that the school has a right to access the device or request its return.
- realise that the device belongs to the Maple Medical PRU and that any procedures or guidelines provided through them must be adhered to.
- never use the webcam inappropriately
- report any situation where you are made to feel uncomfortable online to a responsible adult
- be aware of e-safety – There is a link at the end of this document for information and also loaded on to all machines is information regarding e-safety.

Security Incidents

What is a Security Incident?

A security incident is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations and Information Security.

All users are encouraged to report anything they consider suspicious. This could include

- passwords being written down
- passwords being shared
- authorised users logging into applications on behalf of non-authorised user
- failure to report a security breach.

Serious security incidents could include:

- loss of data through inappropriate handling / transfer e.g. using memory sticks to transfer data without virus checking
- file contents amended without file owner being aware
- files deleted or moved without file owner being aware
- e-mail being used for inappropriate purposes

Reporting Security Incidents

All security incidents must be reported to staff at the Maple Medical PRU. This will provide statistics to, for example, aid identification of common security issues that may indicate a need for further training.

All serious security incidents must be reported to the Maple Medical PRU.

Security of Information and Security of Equipment

Equipment Security

Laptops and iPad's are locked away when not in use

Account Security

Users are responsible for the protection of their own computer device and its security. It is a requirement of accepting this device that users do not:

- leave the device unattended
- leave it on display i.e. back seat of a car
- give passwords to anyone not authorised to use the device
- leave it in any way vulnerable to misuse or theft

Information and network security

Information exists in many formats, for example:

- printed or written on paper
- stored electronically
- transmitted by post
- transmitted using electronic means

All pupils are responsible for the security of information when using their computer device.

Users are reminded to back up their data i.e. school essays etc... as no responsibility can be accepted by the Maple Medical PRU for any loss of essential data.

Technology that can be used to store, transmit or manipulate data, such as media rich phones, MP3 players, Personal Digital Assistants (PDAs) and USB media, should be used responsibly and in accordance with this Acceptable Use Policy.

Users shall not:

- intentionally interfere with the normal operation of the computer device i.e. uploading computer viruses
- leave equipment logged into the internet for any length of time whilst unattended
- leave equipment logged in without screensaver password protection
- share usernames and passwords
- attempt to download, store or install software to the computer device without permission from the Maple Medical PRU e.g. iTunes
- attempt to bypass network or system security.
- attempt to access another user's account.
- attempt to gain access to an unauthorised area or system.
- attempt to use any form of hacking/cracking software or system.
- connect any device to the network that acts as a Wireless Access Point (WAP) or router – unless authorised by the teacher within the school setting.
- access, download, create, store or transmit material that is indecent or obscene, material that could cause annoyance, offence or anxiety to other users, or material that infringes copyright or is unlawful.
- engage in activities that waste technical support time and resources.
- store personal files such as music, video, photographs or games on IT equipment.

Viruses

The IT department has implemented centralised, automated virus detection and virus software updates. All PCs have antivirus software installed to detect and remove any virus automatically.

Individuals must not:

- Remove or disable anti-virus software.
- Attempt to remove virus-infected files or clean up an infection, other than by the use of the approved anti-virus software and procedures.

Disciplinary Procedures

Those who misuse the computer facilities and break this Acceptable Use Policy will be subject to disciplinary procedures. In extreme cases this might include police involvement. Misuse should also be reported to the IT department at the hospital. In the hospital pupils must have their device PAT tested and log in using the hospital wifi. Any serious incident must be reported to the ict department of the hospital

Further Information

Useful links:

Copyright laws: <http://www.ipo.gov.uk/copy.htm>

Data Protection Act: <https://ico.org.uk/>

e-Safety <http://www.thinkuknow.co.uk>

Parents/ carers or pupils who have any concerns regarding online safety please use the following link to CEOP(Child Exploitation and Online Protection <http://ceop.police.uk/>)

Date of Policy March 2019

Date of Review March 2021

Signed

Head teacher

Chair Management Committee