MANCHESTER HEALTH ACADEMY

ICT ACCEPTABLE USAGE POLICY

Version 3: November 2016

ICT ACCEPTABLE USAGE POLICY

Approval History

Approved By:	Date of Approval	Version Approved	Comments
	Jan 2012	V1	
Board of Governors	27/11/14	V2	
Standards Committee	24/11/16	V3	

Revision History

Revision Date	Previous Revision Date	Rev	Summary of Changes	Changes Marked	Owner/Editor
Nov 2014		V2	Policy updated and put into standard policy format	N	DO/DC
Sept 2015		V2.1	Policy updated to include '5.6. - Preventing Radicalisation and Violent Extremism'.	N	DC
08/01/16		V2.2	Section 5.5, 5.6 and 5.8 updated.	Y *	DC
11/11/16		V3	Section 2, 5.5, 5.7, 5.8, 5.9 and Student ICT Acceptable Usage Policy updated.	Y *	DC

1. Purpose

This acceptable usage policy aims to protect students, staff and the Academy by clearly stating what use of the computer resources is acceptable and what is not.

2. Scope

This policy applies to all users of network and ICT services at Manchester Health Academy.

3. Responsibility

All users of network and ICT services at Manchester Health Academy.

It is therefore the users' responsibility to ensure that they comply with the policy.

4. Our approach

Manchester Health Academy assumes the honesty and integrity of its ICT users. The computer system is owned by the Academy and facilities are provided in as unrestricted a manner as possible in order that the best possible services may be provided.

5. General Policy

5.1 Unsuitable / inappropriate activities

Users must not:

- Upload, download, post, email or otherwise transmit or store any content of an unlawful, harmful, threatening, abusive, defamatory, vulgar, obscene, libellous, invasive of anyone's privacy, hateful, discriminatory or otherwise objectionable nature.
- Upload, download, post, email or otherwise transmit or store any content that infringes any patent, trademark, copyright, intellectual property rights or any other proprietary rights of any party.
- Upload, download, post, email or otherwise transmit or store any unsolicited or unauthorised advertising, promotional materials, "junk mail", "spam", "chain letters", "pyramid schemes", etc. except when directly resulting from curriculum work.
- Knowingly upload, download, post, email or otherwise transmit or store any material that contains malicious code, files or programs designed to interrupt, damage, destroy or limit the functionality or any of the academy's computer or communications systems.
- Collect or store personal information about others without direct reference to and compliance with The Data Protection Act 1998.
- Use the Academy's systems to undertake any trading, gambling, other action for personal financial gain, or political purposes unless part of a curriculum project.
- Engage in the use of real-time chat services not supplied or authorised by the Academy.
- Store or use any software not specifically installed on the service by an authorised person.
- Visit, use, download or store any game, either application or browser-based, without permission from the ICT Network Manager.

- Access any website which may be deemed inappropriate, or for which they have not been given specific permission.

Any breach of this agreement may result in the suspension of any or all parts of the services provided and the notification of the Senior Leadership Team.

5.2 Network Services

- Each user shall have their own unique login credentials, in the form of a username and password. Users must not divulge their password to any other user or third party outside the Academy. If a user suspects that their password may have been compromised, they must change their password immediately and inform the ICT support team.
- Users must not share access to network services accessed using their login credentials with anyone else.
- The ICT support team regularly monitor and record the activity of users on the Academy ICT systems.

5.3 Internet Services

- Each user shall have access to the Internet via the Academy's proxy server. Users will be given their own unique proxy credentials and must not divulge their passwords to anyone.
- Users must not share access to Internet services accessed using their login credentials with anyone else.
- The Academy uses filtering software to identify and prevent access to inappropriate Internet content. All Internet activity is logged on a per user basis and will be monitored in order to ensure users' compliance with the acceptable usage policy. We ask that users help us to provide safe and appropriate access to Internet resources by reporting incidents of access to inappropriate content, with as many details as possible.
- Conversely, if users find that legitimate and appropriate Internet learning resources are blocked, we ask that they report this to the ICT support team so that they may be unblocked.

5.4 Email Services

- All users shall be given their own email account. Users must not divulge their passwords to anyone or share access to services accessed using their login credentials with anyone else.
- Email sent and received internally and externally may be filtered for language content and certain file types within attachments.
- All staff have an 'Academy' email address which may be used for communication with children and young people, for Academy related matters.
- It is not permitted for staff to give out their 'own' personal email address. This applies to former pupils and post-16 students also.
- Any correspondence with former students must only be through staff Academy email addresses.

5.5 Social Networking

- It is not permitted for **users** to access social networking for personal use.
- It is not permitted for staff to accept students as 'friends' or to post images of themselves or colleagues, with current students.
- It is not permitted for staff to accept former students as 'friends' nor to post images of themselves or colleagues with former students if these students are under 18 years of age.
- Staff are strongly advised to think very carefully before accepting as friends or posting images of former students who are over the age of 18.
- Adults who work with children and young people up to the age of 18 are not allowed to have a secret or special personal relationship with a child or young person whom they know due to their work. To do so would be a serious cause for concern and if deemed to constitute a breach of trust, could lead to dismissal.
- It is illegal for any adult to have communication which results in a private meeting or with the intent of sexual relations, with children or young people in their care.

5.6 Preventing Radicalisation and Violent Extremism

- Manchester Health Academy is clear that exploitation and radicalisation will be viewed as a safeguarding concern and any monitored activity of this nature will be referred to the appropriate safeguarding agencies. All 'websites' promoting or linking to 'radicalisation and / or violent extremism' are blocked as default by the built in policies within the Academy's web filters.
- If users discover any accessible websites which they feel promotes or links to radicalisation and / or violent extremism they must report this to the ICT support team immediately who will ensure that the site is blocked from future access.

5.7 Security

- It is each user's responsibility to ensure that his or her passwords are kept secret and not shared with anyone else. If a user suspects that their password may have been compromised, they must notify the ICT support team immediately, who will assist in changing their password.
- Passwords are one way encrypted so that, whilst they can be reset, even network administrators cannot discover users' passwords. No member of the ICT support team will ever ask a user for their password, nor should any other **user** - users must never divulge their passwords to anyone.
- Only software that has been approved by the ICT Network Manager may be used on Academy equipment. The use of unapproved software may present a security risk and is not permitted.

5.8 Treatment of Equipment

- The ICT department will endeavour to ensure that all ICT equipment is in working order. Should any user find that a piece of equipment does not function correctly, they should report it to the ICT support team and not attempt to repair it themselves.
- Any user who is found to have caused damage to ICT equipment, either intentionally or through neglect, may be refused access to any or all of the Academy's ICT facilities and may be asked to cover the costs of repair or replacement.

- All ICT equipment is the property of the Academy. Damage or loss of ICT equipment must be reported to the ICT support team immediately. Staff and student leaver's must return ICT equipment to the ICT 'support team' or their line manager before they leave.
- **ICT equipment provided to users to facilitate their work must only be used by that user for work related tasks and not for personal use.**

5.9 What Happens if I Breach This Policy

Any breach of this policy may lead to the following sanctions:

- A temporary or permanent ban on Internet use.
- Pupils parents being contacted.
- **Network account temporarily or permanently disabled.**
- Other external agencies being contacted.
- Additional disciplinary action may be added in line with the Academy's own policy.

6. Related Documents

- Safeguarding & Child Protection Policy.
- E-Safety Policy.

Student ICT Acceptable Usage Policy

I will only access the network with my own username and password, which I will keep secure (secret and never shared with others).

- *Passwords cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters.*

- *Passwords must be at least 8 characters in length.*

- *Passwords must contain characters from at least three of the following four categories:*
  - *English uppercase alphabet characters (A–Z).*
  - *English lowercase alphabet characters (a–z).*
  - *Base 10 digits (0–9).*
  - *Non-alphanumeric characters (for example, !$#,%).*

I will NEVER access other people's files, or destroy/damage their work and data.

I will use the Internet only for activities and work set by the Academy, e.g. homework or coursework.

I will only Email other MHA students, or staff or people my teacher has approved, and not use the Internet for personal or private messages.

I will respect the privacy of others. I will not publish their names, addresses, phone numbers or photographs on the Internet. Social networking sites are blocked within the Academy, but if I use them at home, I will do so responsibly and be aware that anything I post can last a lifetime.

I will NEVER give my home address or telephone number, or arrange to meet someone, through the Internet. I will always try to be aware of E-Safety, and will keep my details private; I will only share them in confidence responsibly with people I actually know. "If in doubt, leave it out!"

I will NEVER use work from the Internet as if it was my own (Plagiarism). I will give credit to the sources of materials included in my work.

I will not actively try to find or use unacceptable material from the Internet.

I will report any unpleasant material or messages sent to me to a member of staff, and report any unsuitable Internet sites that are accessible in the Academy to a member of Staff or IT support team. I understand this reporting will be confidential and will help protect other pupils and myself.

I will not use the Academy computers to subscribe to any goods or services, nor buy or sell using the Internet, e.g. EBay etc.

I will not try to download any software from the Internet.

I will not bring in CD's/DVD's or Pen/Flash Drives or Flash Media (Camera SO Cards, PSP Memory Sticks etc) data from outside the Academy unless I have been given permission.

I will not send unsuitable email messages. The messages I send will be polite, responsible, related to my coursework, and only signed in my name.

I will NEVER send anonymous messages to anyone.

I will NEVER try to print out anything unsuitable.

I will not take part in any activity which goes against Academy rules.

I understand that the Academy may check my computer files and may monitor the Internet sites I visit.

I will always use my mobile phone in the same way I would use an Academy computer - responsibly!

I will remember that ICT Internet access is a privilege, not a right and that access requires responsibility.

What Happens if I Break These Rules:-

**Any breach of this policy may lead to the following sanctions:*

- *A temporary or permanent ban on Internet use.*
- *Pupils parents being contacted.*
- *Network account temporarily or permanently disabled.*
- *Other external agencies being contacted.*
- *Additional disciplinary action may be added in line with the Academy's own policy.**

Student Name: _____

Tutor Group: _____

Date: _____