MANCHESTER HEALTH ACADEMY

E-SAFETY POLICY

Version 3: November 2016

E-SAFETY POLICY

Approval History

Approved By:	Date of Approval	Version Approved	Comments
	January 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
27/11/14		V2	Policy update and put into standard Academy format	N	DO/DC
28/09/15		V2.1	Policy updated to include 'Radicalisation and Violent Extremism' under section '5.11. - Unsuitable / inappropriate activities'.	N	DC
08/01/16		V2.2	Section 5.11 updated.	Y*	DC
11/11/16		V3	Section 5.1, 5.4 and 5.6 updated.	Y*	DC

1. Purpose

This E-Safety policy aims to protect all members of the Academy community (including staff, students, volunteers, parents / carers, visitors, community users) by clearly stating safe and appropriate use while using the Internet and other communication technologies for educational, personal and recreational use.

2. Scope

This policy applies to all members of the Academy community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of the Academy ICT systems, both in and out of the 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 Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the Academy's e-safety provision. Children and young people need the help and support of the Academy to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned e-safety programme will be provided as part of ICT lessons and should be regularly revisited – this will cover both the use of ICT and new technologies inside and outside of the Academy.
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.
- Students will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students will be helped to understand the need for the *ICT Acceptable Usage Policy* and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside of the Academy.
- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- **Rules for use of ICT systems / the Internet will be displayed on log-on screens.**

- Staff will act as good role models in their use of ICT, the Internet and mobile devices.

5.2 Education – Parents / Carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the Internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The Academy will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, MHA website, VLE.
- Parents evenings.

5.3 Education - Extended Schools

The Academy will offer family learning courses in ICT, media literacy and e-safety so that parents and children can together gain a better understanding of these issues. Messages to the public around e-safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

5.4 Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the **Academy E-Safety and ICT Acceptable Usage policies.**
- The E-Safety Coordinator will receive regular updates through attendance at LA / other information / training sessions and by reviewing guidance documents released by BECTA / LA and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days and with the governing body as part of its policy review cycle.
- The E-Safety Coordinator will provide advice / guidance / training as required to individuals as required.

5.5 Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in ICT / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association.
- Participation in Academy training / information sessions.

5.6 Academy Infrastructure / Network

The Academy will be responsible for ensuring that the Academy infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- Academy ICT systems will be managed in ways that ensure that the Academy meets the e-safety technical requirements outlined in any relevant Local Authority E-Safety Policy and guidance.
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to Academy ICT systems. Details of the access rights available to groups of users will be recorded by the ICT Network Manager and will be reviewed, at least annually, by the E-Safety Coordinator.
- All users will be provided with a username and password. Users will be required to change their password regularly.
- The “master / administrator” passwords for the Academy ICT system, used by the ICT Network Manager must also be available to the Principal and kept in a secure place.
- Users will be made responsible for the security of their username and password, and must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The Academy maintains and supports the managed filtering service.
- Any filtering issues should be reported immediately to the ICT support team.
- Requests from staff for sites to be removed from the filtered list will be considered by the ICT Network Manager.
- The ICT support team regularly monitor and record the activity of users on the Academy ICT systems and users are made aware of this in the **ICT Acceptable Usage Policy.**
- **Remote management tools are used by staff to control workstations and view user’s activity.**
- An appropriate system is in place for users to report any actual / potential e-safety incidents to the ICT support team or other relevant persons.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the Academy systems and data.
- Guidance is in place for the provision of temporary access of “guests” (e.g. trainee teachers, visitors) onto the Academy system, managed by the ICT Network Manager.
- Guidance is in place regarding the downloading of executable files by users.
- Guidance is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on laptops and other portable devices that may be used out of the Academy.
- Guidance is in place that allows staff to / forbids staff from installing **programs** on Academy workstations / portable devices.

- Guidance is in place regarding the use of removable media (e.g., memory sticks / CDs / DVDs) by users on Academy workstations / portable devices.
- The Academy infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the Academy site unless safely encrypted or otherwise secured.

5.7 Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT support team can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

5.8 Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the Internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the Internet. Those images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out Internet searches for information about potential and existing employees. The Academy will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the Internet e.g. on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow Academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Academy equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the Academy into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.

- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's photographs and work can only be published with the permission of the student and parents or carers.

5.9 Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Kept no longer than is necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer personal data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected).
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with Academy policy once it has been transferred or its use is complete.

5.10 Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the Academy currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Students			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school.	■				■			
Use of mobile phones in lessons.				■				■
Use of mobile phones in social time.	■							■
Taking photos on mobile phones or other camera devices.			■					■
Use of hand held devices e.g. PDAs, PSPs.		■						■
Use of personal email addresses in school, or on school network.				■				■
Use of school email for personal emails.		■						■
Use of chat rooms / facilities.				■				■
Use of instant messaging.				■				■
Use of social networking sites.				■				■
Use of blogs.	■							■

When using communication technologies the Academy considers the following as good practice:

- The official Academy email service is regarded as safe and secure and is monitored. Staff and students should therefore use only the Academy email service to communicate with others when in the Academy, or on Academy systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the E-Safety Coordinator or ICT support team – in accordance with the Academy policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Students will be provided with individual Academy email addresses for educational use.
- Students are taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

- Personal information should not be posted on the Academy website and only official email addresses should be used to identify members of staff.

- In the event of a member of staff having a child protection concern about a student, they must immediately report that concern to the DSP/Safeguarding Officer. The member of staff will be asked by the DSP/Safeguarding Officer to document briefly the events which have given rise to the concern.

- The Academy follows the Manchester City Council guidelines for Child Protection, liaising with the Social Services and other agencies, as appropriate.

- The DSP/Safeguarding Officer will report back to the member of staff who made the initial report on a 'need to know' basis but will inform the member of staff that appropriate action has been taken.

5.11 Unsuitable / inappropriate activities

Some Internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from Academy and all other ICT systems. Other activities e.g. Cyber-bullying would be banned and could lead to criminal prosecution. Students will be reminded, through curriculum activities, assemblies and health-related provision, of expectations around the use of social media and internet sites and acceptable use of mobile phones. Any contraventions of these policies will be dealt with through the Academy's safeguarding proceudres.

There are however a range of activities which may, generally, be legal but would be inappropriate in Academy context, either because of the age of the users or the nature of those activities.

The Academy believes that the activities referred to in the following section would be inappropriate in Academy context and that users should not engage in these activities inside or outside the Academy when using Academy equipment or systems.

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images.
- Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation.
- Adult material that potentially breaches the Obscene Publications Act in the UK.
- Criminally racist material in UK.
- Pornography.
- Promotion of any kind of discrimination.
- Promotion of racial or religious hatred.
- Threatening behaviour, including promotion of physical violence or mental harm.
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the Academy or brings the Academy into disrepute.
- Using Academy systems to run a private business.
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the Academy.
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions.
- Revealing or publicising confidential or proprietary information (e.g. Financial / personal information, databases, computer / network access codes and passwords).

- Creating or propagating computer viruses or other harmful files.
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the Internet.
- On-line gaming (non-educational).
- On-line gambling.
- On-line shopping / commerce.
- File sharing.
- Radicalisation and / or violent extremism.

The Academy considers the below Internet activity acceptable for nominated users (staff) at certain times:

- On-line gaming (educational).
- Use of social networking sites (e.g. to resolve cases of cyber bullying).
- Use of video broadcasting e.g. YouTube.

5.12 Responding to incidents of misuse

It is hoped that all members of the Academy community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity e.g.:

- Child sexual abuse images.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Other criminal conduct, activity or materials.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

It is more likely that the Academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the Academy community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Students / Pupils	Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Safeguarding officer/DSP	Refer to Head of Department / Head of Year / other	Refer to Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal.										
Unauthorised use of non-educational sites during lessons										
Unauthorised use of mobile phone / digital camera / other handheld device										
Unauthorised use of social networking / instant messaging / personal email										
Unauthorised downloading or uploading of files										
Allowing others to access school network by sharing username and passwords										
Attempting to access or accessing the school network, using another student's / pupil's account										
Attempting to access or accessing the school network, using the account of a member of staff										
Corrupting or destroying the data of other users										
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature										
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school										

Using proxy sites or other means to subvert the school's filtering system										
Accidentally accessing offensive or pornographic material and failing to report the incident										
Deliberately accessing or trying to access offensive or pornographic material										
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act										

If any member of staff is found to perform any of the below incidents they will ultimately be referred to the Principal via the E-Safety Coordinator or ICT support team:

- Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).
- Excessive or inappropriate personal use of the Internet / social networking sites / instant messaging / personal email.
- Unauthorised downloading or uploading of files.
- Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.
- Careless use of personal data e.g. holding or transferring data in an insecure manner.
- Deliberate actions to breach data protection or network security rules.
- Corrupting or destroying the data of other users or causing deliberate damage to hardware or software.
- Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature.
- Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils.
- Actions which could compromise the staff member's professional standing.
- Actions which could bring the Academy into disrepute or breach the integrity of the ethos of the Academy.
- Using proxy sites or other means to subvert the Academy's filtering system.
- Accidentally accessing offensive or pornographic material and failing to report the incident.
- Deliberately accessing or trying to access offensive or pornographic material.
- Breaching copyright or licensing regulations.
- Continued infringements of the above, following previous warnings or sanctions.

6. Related Documents

- Safeguarding & Child Protection Policy
- ICT Acceptable Usage Policy