Manchester Academy
The best in everyone™
Part of United Learning

e-Safety Policy

2016 – 2017

For Office Use Only

Date of last review:	Sept, 2016		Target Audience:	All staff / governors / parents and carers
Date of next review:	Sept, 2017		Reason for version change:	Updated for 2016 – 17 academic year
Review period:	1 Year		Name of owner/author:	John Velasco, Senior Staff Associate
Version number:	3.0		Name of individual/department responsible:	SLT

Manchester Academy e-Safety Policy

Aims and Scope

Manchester Academy shares the common United Learning mission, in that the use of ICT will be used effectively to improve the learning outcomes and experiences of all students at the school. The aim is that all of the stakeholders associated to Manchester Academy will be committed to a shared responsibility towards achieving this mission. The intention is that ICT will be used to:

- Enhance the learning experience of Manchester Academy pupils.
- Contribute to effective teaching and learning practice
- Allow efficient practices in administrative systems

In order to facilitate the mission, Manchester Academy has policies and procedures in place to guide and support those who utilise ICT. Both pupils and teachers at Manchester Academy have access to computer resources and e-learning materials. ICT is provided by an up-to-date Local Area Networks (LAN) and the Best in Everyone (BiE) Wide Area Network (WAN) that ensure safe, secure and timely access to email, e-learning resources, printing, the Internet and educational software.

It is imperative that safeguarding is incorporated into best practice at Manchester Academy and that all users are responsible and have a secure awareness of E-safety. Therefore, the ICT policy and procedures document used at Manchester Academy are intended to promote a positive ethos and behaviour regarding responsible ICT usage and Internet safety.

All staff members, both teaching and non-teaching will ensure that the policy set out below is implemented across all relevant areas of learning, teaching, administration and support. Manchester Academy is fully committed to ensuring that the application of this acceptable usage policy document for ICT for pupils is non-discriminatory in line with the UK Equality Act (2010). Further details are available in the Equality Objectives documentation. This policy is applicable to all pupils and Manchester Academy seeks to implement this policy through adherence to the procedures set out in the rest of this document.

Acceptable Use of ICT

Manchester Academy provides computing resources for pupils use to enhance teaching and learning. This policy follows national guidelines in order to protect both the pupils and employees of Manchester Academy.

e-Safety

- ICT users at Manchester Academy staff and pupils, must keep all personal information, private when using the internet. They should not share or send personal information (including name, address, email, bank details or telephone) from a Manchester Academy computer.
- Pupils must only access those resources and services that they have been instructed / authorised by a member of staff to use.
- Pupils must inform a member of staff if they feel frightened or threatened by something they have accessed on the internet.

Use of the Internet

- All Internet access is controlled by an Internet Content Filter appliance which constantly monitors and logs all Internet activity.
- The Internet is to be used only for educational purposes during teaching and learning time. Recreational activity during non-teaching and learning time is permitted only when authorised by a member of the teaching staff.
- Pupils should acknowledge and avoid plagiarism when researching information to produce pieces of work of their own.

Use of email

- Pupils must observe the polite and proper use of email at school and elsewhere. Pupils are prohibited from emailing or uploading to social networking sites any material that could cause offence or harm to other individuals and / or Manchester Academy.
- Only Manchester Academy managed email service, must be used. Webmail e.g. Gmail, Hotmail, Yahoo is not allowed during school hours.
- Email use must be directly related to educational use. The forwarding of chain mail, spam, animations, hoaxes, virus warnings or nuisance emails is strictly forbidden.
- Any suspicious email must be treated with care and reported to a member of the teaching staff or Network Manager.

Use of social media, internet messaging and chat rooms

- Access to chat and social networking sites is strictly forbidden during school hours.

Cyber bullying

- Cyber bullying of any form will not be accepted or tolerated at Manchester Academy. Manchester Academy will take immediate and serious action in line with its Bullying Policy.

- Students and staff must inform a member of ICT services, of any incidences of cyber bullying via email or text messaging.

Copyright

- The copyright of material and intellectual property rights must be respected. Pupils should never use material directly from an Internet source or CD and present it as their own work. Plagiarism sanctions will be enforced if pupils are found to have directly copied work.

Use of personal laptops and tablets on the school network

- Students are strictly prohibited from connecting to the Wi-Fi to gain access to the Internet at Manchester Academy.
- Students are prohibited from the sharing of passwords with other pupils.
- Pupils may not use mobile devices in lessons unless specifically directed to do so by a member of staff.

Use of portable storage items

- Personal portable media devices should be used under the direction of the teacher for educational use only. Any files brought to school from a home computer (including homework) or downloaded from the Internet should be virus scanned before being used on a Manchester Academy computer. Any misuse of portable storage will result in this privilege being removed.

Use of Staff Passwords / Computers

- The use of staff user names and / or passwords by other members of staff or students is strictly prohibited.
- Pupils must not be allowed to view documents that relate to private data of other students and must not be allowed to work on computers that allow them access to sensitive or official information, registers or records.

Taking Pictures on Mobile Devices

- The taking of pictures with mobile devices (such as mobile phones, iPads or iPods) by students within the Academy and its boundaries is strictly prohibited.

Playing of Games

- The use of school computers to play games, other than those games / activities with a specific educational purpose which are authorised by a member of staff, is strictly prohibited.

Data security

1. Pupils must not give their password to anyone else. All pupils are responsible for the safe keeping of their logon password which must be changed when prompted, to protect the Manchester Academy local network.
2. Pupils are responsible for all activities carried out during a session opened with their logon ID.
3. Pupils cannot download or install any applications.

4. Pupils must never delete the work of other students.
5. Remember, that all data on the network is the property of Manchester and can be viewed by authorised staff if necessary. This does not affect the pupil's privacy rights under the Data Protection Act.

Health and Safety

- Pupils should remember that computers are electrical equipment and therefore drinks must not be consumed in areas where there are laptops or computers.
- Pupils should avoid spending long periods of time on the computer without a break.

How to report misuse or accidental access of inappropriate materials

- If pupils accidentally accesses unsuitable sites, the URL (address) and content must be reported to a member of staff immediately.

Monitoring by the school

- Pupils are personally responsible for the care of any ICT hardware provided and its use must comply with this policy.
- Pupils must make every effort not to waste resources, especially printer ink and paper. The ICT Department retain the right to monitor consumable usage and pupils may be billed accordingly if excessive resources are used through abuse of the system.

Sanctions for Misuse

- The use of computing resources is a privilege and any violation of the terms set out in this policy will result in access to the Internet and/or computing resources being restricted or withdrawn along with any further disciplinary measures deemed necessary.
- The use of computer systems without permission or for purposes not agreed by Manchester Academy could constitute an offence under the Computer Misuse Act (1990).
- Pupils must not engage in any activity that could damage or threaten the functionality of any of the school's computing resources. Manchester Academy will seek financial compensation for any malicious damage caused to ICT equipment.
- Sanctions are in place for deliberate access to inappropriate materials by pupils when using the internet.

Roles and Responsibilities (other than students)

Principal

Reporting to the governing body, the Principal has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated to a member of staff responsible for e-Learning (John Velasco). The Principal will ensure that:

- e-Safety training is provided to where appropriate students, all staff, leadership team and governing body, parents.
- The designated e-Learning person has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.

The Designated e-Learning Person will:

- Keep up to date with the latest risks to children whilst using technology;
- Review this policy regularly and bring any matters to the attention of the Principal;
- Liaise with IT technical support and other agencies as required.
- Ensure ICT Services maintain technical e-Safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support;

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Principal.
- Any e-Safety incident is reported to ICT services and if required the Designated Person responsible for Child Protection.

Governing Body

- The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:
    - Review this policy at least annually and in response to any e-Safety incident to ensure that the policy is up to date and it covers all aspects of technology use within the school;
    - Ensure e-Safety incidents are appropriately dealt with and that the policy was effective in managing those incidents;
- Appoint one governor to have overall responsibility for the governance of e-Safety at the school who will:
    - Keep up to date with emerging risks and threats through technology use.
    - Receive regular updates from the Principal with regards to training, identified risks and any incidents.