Marlborough Road Academy

E-safety Acceptable Use Policy
Marlborough Road Academy
April 2016

Introduction

This School E-Safety Acceptable Use Policy applies to staff, pupils, volunteers, visitors and community users who have access to and are users of school ICT systems and mobile technologies, both in and out of school.

Further information and support

For a glossary of terms used in this document:
http://www.salford.gov.uk/d/salford-esafety-glossary-jan2012.pdf

For e-Safety Practice Guidance for those who Work and Volunteer with, and have a Duty of Care to Safeguard Children and Young People:
http://www.salford.gov.uk/d/e-Safety-Practice-Guidance.pdf

R u cyber safe?
E-safety tips about how to stay safe online:
http://www.salford.gov.uk/rucybersafe.htm

DOCUMENT STATUS

Version	Date	Action	Approved by Governing Body	
			Signature	Date
1	September 2012	First		
2	April 2015	Updated		
3				
4				

Mobile phones

Best practice

☑ **DO**

Staff: If you need to use a mobile phone while on school business (trips etc), this is acceptable.

Make sure you know about inbuilt software/ facilities and switch off if appropriate.

Safe practice

Check the e-safety policy for any instances where using personal phones may be allowed.

Staff: Make sure you know how to employ safety measures like concealing your number by dialling 141 first when having to contact parents or get the office to contact them.

Poor practice

☒ **DO NOT**

Staff: Don't use your own phone without the Headteacher/SLT knowledge or permission.

Don't retain service student/pupil/parental contact details for your personal use.

Social networking (e.g. Facebook / Twitter)

Best practice

☑ DO

If you have a personal account, regularly check all settings and make sure your security settings are not open access. Set accounts to the highest privacy settings.

Ask family and friends to not post tagged images of you on their open access profiles.

Safe practice

Don't accept people you don't know as friends.

Be aware that belonging to a 'group' can allow access to your profile.

Amend search options for your profile settings to highest level of privacy.

Use a different screen name to your real name.

Poor practice

☒ DO NOT

Don't have an open access profile that includes inappropriate personal information and images, photos or videos.
Staff:

- Don't accept students/pupils or their parents as friends on your personal profile.
- Don't accept ex-students/pupils users as friends.
- Don't write inappropriate or indiscrete posts about colleagues, students/pupils or their parents.

Webcams

Best practice

☑ **DO**

Make sure you know about inbuilt software/ facilities and switch off when not in use.

Safe practice

Check the e-safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Headteacher/SLT knowledge or permission

Make arrangements for pictures to be downloaded to the school network immediately after the event.

Delete images from the camera/device after downloading.

Poor practice

☒ **DO NOT**

Don't download images from organisation equipment to your own equipment.

Don't use your own equipment without Headteacher/SLT knowledge or permission – and in accordance with the e-safety policy.

Don't retain, copy or distribute images for your personal use.

Incident Management

Incidents (pupils):	Refer to class teacher	Refer to E-safety Officer	Refer to Headteacher	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 eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)			x	x		x	x	x	x
Unauthorised use of non-educational sites during lessons	x							x	
Unauthorised use of mobile phone/digital camera / other handheld device	x					x		x	
Unauthorised use of social networking/ instant messaging/personal email	x					x		x	
Unauthorised downloading or uploading of files	x							x	
Allowing others to access school network by sharing username and passwords	x				x	x	x	x	
Attempting to access or accessing the school network, using another student's/pupil's account	x				x	x		x	
Attempting to access or accessing the school network, using the account of a member of staff	x		x		x	x		x	x
Corrupting or destroying the data of other users	x							x	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	x					x		x	x
Continued infringements of the above, following previous warnings or sanctions			x			x	x	x	x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	x		x				x		
Using proxy sites or other means to subvert the school's filtering system	x		x				x	x	x
Accidentally accessing offensive or pornographic material and failing to report the incident	X				x			x	
Deliberately accessing or trying to access offensive or pornography	x		x	x	x	x	x	x	x
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	x		x	x	x	x	x	x	x

Incidents (staff and community users):	Refer to E-safety Officer	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Removal of network / internet access rights	Warning	Further sanction : disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)	x	x	x	x	x	x	x
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	x	x				x	
Unauthorised downloading or uploading of files	x					x	
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	x	x				x	x
Careless use of personal data e.g. holding or transferring data in an insecure manner	x						
Deliberate actions to breach data protection or network security rules	x	x		x	x	x	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	x	x	x	x		x	x
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	x	x					
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	x	x			x		x
Actions which could compromise the staff member's professional standing	x	x					x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	x	x				x	x
Using proxy sites or other means to subvert the school's filtering system	x	x		x		x	
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x					
Deliberately accessing or trying to access offensive or pornographic material	x	x	x	x	x		x
Breaching copyright or licensing regulations	x					x	
Continued infringements of the above, following previous warnings or sanctions	x	x			x		x

Appendix 1

Pupil AUP Pupil Acceptable Use Policy Agreement

This Acceptable Use Policy is intended to make sure:

- That you will be a responsible user and stay safe while using the internet and other technology for learning and personal use
- That ICT systems and users are protected from accidental or deliberate misuse

The school will try to ensure that you will have good access to ICT to enhance your learning and will, in return, expect you to agree to be a responsible user.

The school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. The school however, cannot be held responsible for the nature or content or materials accessed through the internet and, as such, are not liable for any damages arising from the use of the internet. Marlborough Road Academy uses internet filtering provided by Salford City Council.

Please make sure you read and understand the following statements.

☑ **I WILL** and

☒ **I WILL NOT**

If there's anything you're not sure of, ask your teacher.

Permissions

On admission to the Academy, pupils and parents agree to follow the guidelines above by signing the E-Safety/ICT Acceptable Use Agreement Form and the permission slip to allow the Academy to take and use images of their children as outlined in Appendix 3. By signing the forms, pupils and parents are agreeing to support the Academy in this important aspect of the Academy's work.

Staff, Volunteers and Community Users are also required to sign an Acceptable Use Agreement

☑ I WILL:

- treat my username and password like my toothbrush – I will not share it, or try to use any other person's username and password
- immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online
- respect others' work and property and will not access, copy, remove or change anyone else's files, without their knowledge and permission
- be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions
- only use my personal handheld/external devices (mobile phones/USB devices etc) in school if I have permission . Hand in mobile phones to the school office at the start of the day and collect after lessons at 3:15pm.
- understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment
- immediately report any damage or faults involving equipment or software, however this may have happened
- only use chat and social networking sites with permission and at the times that are allowed.

☒ I WILL NOT:

- try (unless I have permission) to make downloads or uploads from the Internet
- take or share images (pictures and videos) of anyone without their permission
- use the school ICT systems for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.
- try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others
- try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- open any attachments to emails, unless I know and trust the person/organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes
- attempt to install programmes of any type on a machine, or store programmes on a computer
- try to alter computer settings
- Create a social networking account illegally. (Facebook etc users must be 13 years of age)
- Try to search for members of staff online or contact them via social networking sites or personal email addresses.

Appendix 2

Staff, Volunteer and Community User Acceptable Use Policy Agreement

School Policy

This Acceptable Use Policy (AUP) is intended to ensure:

- that staff, volunteers and community users will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

- that staff, volunteers and community users are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff, volunteers and community users will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff, volunteers and community users to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.

- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, VLE etc) out of school.

- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.

- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only not use social networking sites in school and only use chat in accordance with the school's policies.

- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner. I will not give out my personal email or phone numbers to contact students or parents and carers. I will contact parents/ carers and pupils using the school telephone.

- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held/external devices (PDAs/laptops/mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules in line with the School's E-Safety Policy set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses. I will scan my devise for viruses.

- I will not use personal email addresses on the school ICT systems unless I have not been allocated a school email address. If I do use my personal email account, it will be for work related purposes.

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.

- I will ensure that my data is regularly backed up, in accordance with relevant school policies.

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies. I will not try to log in on someone else's username who has administrator rights in order to change settings or software.

- I will not disable or cause any damage to school equipment, or the equipment belonging to others.

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School/Local Authority Personal Data Policy Where personal data is transferred outside the secure school network, it must be encrypted.

- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.

- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

- This Policy should be read in conjunction with the E-Safety Practice Guidance for staff T:Policies/Academypolicies/ESafetypracticeguidance

Appendix 3

Use of Images

Use of Digital / Video images

The use of digital/video images plays an important part in learning activities. Pupils and members of staff may be using digital or video cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.