MATTHEW MOSS HIGH SCHOOL
Learning for Life

Policy No.: 31

Policy: ICT Acceptable Use

Review Date: June 2017

Policy Name: ICT Acceptable Use Policy for Staff
Including: Staff Mobile Device Agreement
Twitter Guidance

Nominated Lead Member of Staff: ICT Manager

Review Cycle: 2 Years

Authorisation: Headteacher

Review Date: June 2017

ICT Acceptable Use Policy for Staff

The use of the latest technology is actively encouraged at Matthew Moss. With this comes a responsibility to protect users and the school from abuse of the system.

All staff, therefore, must adhere to the policy set out below. This policy covers all computers, laptops and electronic devices (such as iPads) within the school, irrespective of who owns the device.

Staff and learners are expected to behave responsibly on the school computer network and with the ICT equipment.

1) Access

As a staff member at Matthew Moss, I have access to the following ICT facilities:

1.01 Computers throughout the school.
1.02 Interactive whiteboards or projector screens with Apple TV in teaching rooms.
1.03 A secure username and password for logging into school computer systems.
1.04 An accredited, filtered Internet connection from any computer in school or wi-fi connected device.
1.05 Personal user space on the school network.
1.06 Personal Google Apps user space with 30Gb of online storage.
1.07 Internal and external remote access to the school network and the Cloud site to store and share learning resources.
1.08 Personal @mmhs.rochdale.sch.uk and @mmhs.co.uk email accounts.
1.09 Access to network printers and copiers. Usage is monitored by Equitrac software and charged to departmental budgets.
1.10 Access to resources such as scanners, digital cameras, visualisers, iPads and microphones.
1.11 Access to the School Management Information Systems (SIMS.net) as appropriate to role in school.
1.12 If I bring in my own ICT equipment I can see ICT support personnel to connect it to the school wireless guest network.

2) E-safety

2.01 I will ensure that I am aware of e-safety issues affecting staff and learners. Visit our e-safety page on the Cloud site for more information.
2.02 I will regularly remind learners of key e-safety messages such as ‘never give out personal details online’.

2.03 I will report any accidental access to inappropriate material to my line manager.
2.04 I will report any inappropriate websites to the IT Support team.
2.05 I will be vigilant when asking learners to search for images.
2.06 If a learner accesses inappropriate material I will report it following the correct procedures.
2.07 If I suspect a child protection issue I will report it following the correct procedures.
2.08 I will always be myself and will not pretend to be anyone or anything that I am not on the internet.

3) Computer Security

3.01 I will use computers with care and leave ICT equipment as I found it. I will not tamper with computer systems or devices (e.g. printers and projectors) and their cabling.
3.02 If I notice that ICT equipment or software is damaged or not working correctly, I will report it to the IT Support team straight away.
3.03 I will use the IT Support team to rectify ICT related issues whenever possible.
3.04 I will never try to bypass security features or systems in place on the network, or try to access resources or a user account that I do not have permission for (hacking).
3.05 I will never attempt to install software on school computers or mobile devices myself (unless I have the ICT Manager's permission) and will request a software change through the IT Support team.
3.06 I will always keep my user account credentials secure and not tell them to anyone else.
3.07 I understand that my staff logon gives me access to systems and information that learners and other staff are not entitled to access and I will not under any circumstances allow anyone else access to a computer under my logon credentials.
3.08 I will not attempt to go beyond my authorised access. This includes attempting to log on as another person, sending email whilst pretending to be another person or accessing another person's files. If I find that I do have access to an area that I know I should not have access to, I will inform ICT support personnel immediately.
3.09 If I think someone else has obtained my logon details, I will report it to ICT support personnel as soon as possible to get my logon credentials changed.
3.10 I will never knowingly bring a computer virus, spyware or malware into school.
3.11 If I suspect a school computer or a removable storage device that I am using contains a virus, spyware or other malware, I will report this to ICT support personnel.
3.12 I will not attempt to connect to another user's laptop or device while at school. I am not permitted to establish my own computer network.
3.13 I will take care if I eat or drink whilst using ICT equipment.
3.14 I will not reply to spam emails as this will result in more spam. Delete all spam emails.
3.15 If I lose or misplace any portable ICT equipment I will inform ICT support personnel immediately.
3.16 I will not 'jailbreak' a school iPad, iPhone or iPod touch.

4) Inappropriate Behaviour

4.01 I will not store, download or distribute music, video or image files on my personal user space or shared area, unless they are appropriately licensed media files (e.g. Creative Commons licensed files) that I need for school.
4.02 I will not send or post defamatory or malicious information about a person or about school.
4.03 I will not post or send private information about another person.
4.04 I understand that bullying, manipulation or exploitation of another person either by email, online or via text message will be treated with the highest severity.
4.05 I will not use the internet for gambling.
4.06 I will not access material that is profane or obscene, or that encourages illegal acts, violence or discrimination towards other people.
4.07 If I am planning any activity which might risk breaking the ICT Acceptable Use Policy (e.g. research into terrorism for a legitimate project), I will inform the ICT Manager beforehand to gain permission.
4.08 If I mistakenly access material that is profane or obscene, I will inform my line manager immediately or I may be held responsible.
4.09 I will not attempt to use proxy sites on the internet.
4.10 I will not take a photo or video of a learner or another member of staff without their permission.
4.11 I will not load photos or videos of other staff and learners to websites or social networking sites. I will refer this job to ICT support personnel (eg if I wish to put pictures from a trip on a faculty site).

5) Monitoring

5.01 I understand that all Internet and email usage will be logged and this information could be made available to my manager on request.
5.02 I understand that all files and emails on the system are the property of the school. As such, system administrators have the right to access them if required.
5.03 I will not assume that any email sent on the internet is secure.
5.04 I understand that all network access, web browsing and emails on the school systems and laptops are logged and may be routinely monitored on any computer screen without the person's knowledge.

6) Best Practice

6.01 I will not use school printing facilities to print non-work related materials.
6.02 I will only print out work that I need as a paper copy – where possible I will use school systems such as email, the Cloud site and shared folders to share information electronically.

6.03 I will follow the school's procedure and use the IT Support team for requesting printing funds for my learners.
6.04 I will report it to the IT Support team or Reprographics department if I believe a printer is not working or out of toner.
6.05 I understand that my @mmhs.rochdale.sch.uk and @mmhs.co.uk e-mail accounts are work e-mail accounts, and as such will be used for professional purposes.
6.06 I will only use the approved, secure @mmhs.rochdale.sch.uk or @mmhs.co.uk e-mail systems for any school communication.
6.07 I will only open attachments or download files from trusted sources.
6.08 I will not view, download or distribute material that could be considered offensive or pornographic.
6.09 I will use the school iPads or obtain school cameras (or SD cards) from the IT Support team to photograph and video trips and relevant events (I will not use my own cameras without prior arrangement).
6.10 I will pass relevant photographs and videos taken on to the IT Support team for storage on the school network (I will not keep images and videos of learners in my personal user space and will ensure they are on a shared networking area).
6.11 I will save work regularly using sensible folder and file names.
6.12 I will organise my files in a sensible manner and tidy my user space and shared resource areas regularly.
6.13 I will ensure that I regularly back up any work that is not saved onto the school network.
6.14 I will observe health and safety guidelines where possible when using ICT equipment.
6.15 I will leave my computer and the surrounding area clean and tidy.
6.16 When I leave school permanently, I will ensure that I save any files I wish to take with me as my account will be deleted.
6.17 When I leave school permanently, I will ensure that any files I have stored on mobile or external devices and are needed by school are moved back on to the school system.
6.18 I will only empty my recycle bin when I am certain I no longer need the files.
6.19 I will seek advice from ICT support personnel before ordering any ICT equipment for my department.
6.20 I will not send anyone my credit card or bank account details without checking that it is a secure site with https at the start of the web address.
6.21 I will not print on glossy paper, card or acetate on laser printers.

7) Data Protection

7.01 I will not share data protected information (including school images) with third party organisations without seeking advice first.

7.02 I will use an encrypted storage device (such as a USB drive encrypted using Truecrypt software) to transfer data protected files between home and school. Alternatively, I will use remote access rather than move the files.
7.03 If I am preparing a document that contains data protected information I will ensure that the document template I use has the appropriate protective marking (e.g. confidential, protectively marked).
7.04 I will ensure that I am aware of data protection issues and understand what is considered to be 'personal data'.
7.05 I will not display sensitive information or 'personal data' on a public display or projected image (e.g. a Smartboard). This includes learner data in SIMS.net.
7.06 I will never leave a computer logged on and unattended for even a short space of time. I will log off or lock the workstation. I understand that failure to do this may result in a breach of the Data Protection Act and leave 'personal data' unprotected.
7.07 I will ensure that any remote connection session that I have to a school computer is logged off when I have finished and kept secure from other computer users.

8) Social Networking

8.01 I will not communicate with learners through social networking sites (with the exception of point 8.03 below).
8.02 I will ensure that any personal social networking accounts that I have are secure.
8.03 I will never create a social networking profile, blog or account and use it for school purposes without prior written authorisation from the ICT Manager.
8.04 If I have control over a school Twitter account I will:
8.04a keep it as a protected account at all times.
8.04b only allow learners I know made the request to follow the account and nobody else.
8.04c not follow individuals other than recognised educational professionals.
8.04d only follow professional educational organisations and other organisations as deemed appropriate.
8.04e inform ICT support personnel straight away if I suspect I have lost the password or a device with that account on it.
8.04f never use the account to send Direct Messages to anyone
8.05 I will never create a bogus social networking account or site that is associated with a member of staff, learners or the school.
8.06 If I become aware of misuse of Social Networking accounts or sites that are associated with a member of staff, learners or the school, I will inform the ICT manager immediately.
8.07 I recognise that as an organisation, we do not use social networking sites to communicate with learners, staff and parents (with the exception of our official Twitter and Facebook accounts).

9) Sanctions

9.01 I understand that failure to comply with this Policy could lead to disciplinary action.

Associated Policies:
Internet and E-Safety
Other associated policies

Staff Mobile Device Agreement

In order to justify the significant outlay to provide teaching staff with iPad's, we would ask you to adhere to the requirements set out below.

1. The device is and remains the property of the school. It must be returned to the school whenever requested by the IT department, and during the week of the final term of your employment. If you are likely to be absent from school for an extended period (for example maternity leave) then it should also be returned.

2. The device is subject to routine monitoring by MMHS. Devices must be surrendered immediately upon request from the ICT Manager or any member of the SMT.

3. You will need an account with Apple (an Apple ID) in order to use applications on the device. Although these accounts are free, you are responsible for any charges relating to applications bought through your Apple ID.

4. All data on the device is your responsibility and should be backed up by yourself accordingly. Apple provides the option to back up your data to iCloud. This service is currently free of charge for the first 5Gb of data. As storage space is limited on the device, academic content takes precedence over personal files and apps.

5. A suitable case should be purchased to protect the device. These vary in quality and price. A large number are available through Amazon. The devices are valuable and reasonable care should be taken at all times to prevent theft and damage through misuse.

6. The school IT department will install software on the device to allow it to be managed remotely. This software should not be altered or removed without the permission of the IT department.

7. The device should be protected with a password at all times. You should not give details of this password to any learners.

8. The device should be used appropriately at all times. To safeguard staff and learners iPad users should ensure that they follow the school's 'Guidance on Safe Working Practice' policy.

9. Posting of images relating to the school into a public forum is strictly forbidden without the express permission of a member of the SMT. Access to, or storage of prohibited content is expressly forbidden.

10. As the device is provided for educational purposes it should be used in school regularly.

11. You will be expected to attend initial training sessions provided by the school in order to ensure best use of the device. We will also be seeking feedback on your experience of using the device in order to improve the way in which staff utilise mobile devices.

12. If the device is lost or stolen you should inform the IT department immediately in order for the device to be tracked and remotely wiped to protect confidential data.

13. Staff are responsible for the setting up and use of any home internet connections. No support will be provided for this by the school.

14. Staff are expected to make good any damage to the device that falls outside of the terms of Apple's warranty, and is over and above reasonable wear and tear.

Evaluation:
Ratification:
Review:

I agree to adhere to the terms and conditions set out in the school's ICT Acceptable Use Policy.

Signed: _____

Name (Block Capitals): _____

Date: _____

Twitter Guidance

These accounts should only be used for school business. Teachers who wish to use Twitter for learners to 'follow' must adhere to the rules below:

- They must establish a Twitter account which uses their staff email and password and the user name must be @usernamemmhs e.g. @tsaltermmhs
- Learners may follow teachers but teachers may only follow learners if the learner is also using the naming standards above. The learners Twitter ID should follow the same standard e.g. 08lmorrison
- It is good practice to ensure that you have something to say each day so teachers using Twitter should make sure that they use it daily. If not you will lose your followers and it will become an ineffective tool
- Don't forget you can tweet text, images, links and video but please make sure that learners are not identifiable unless you have their specific permission
- Teachers and learners should not share any personal details via these Twitter Accounts and should only communicate via these 'transparent' accounts
- Since these accounts are used for school business and learning teachers and learners should leave these accounts as 'Public' for the purposes of transparency

For further information please see Mr Tony Salter, E-Safety Co-Ordinator or Mr Dave Leonard, ICT Manager.

Evaluation:
Ratification:
Review:

I agree to adhere to the terms and conditions set out in the school's ICT Acceptable Use Policy.

Signed: _____

Name (Block Capitals): _____

Date: _____