

Acceptable Use ICT

Mossley Hollins High School

Part of the Tames River Educational Trust

Document Created	Document Owner	Classification
		Confidential (only senior management or only Governors have access)
		Restricted (most employees have access)
September 2025	Rob Pilkington TRET ICT Director	Internal (all employees have access)
		Public Information (everyone has access)

Review cycle	Next Review Date	Approving Body
Annually	September 2026	Governing Body

Contents

Contents	2
1. Acceptable Use of ICT - Staff	3
1.1. Introduction	3
1.2. Acceptable Uses	3
1.3. Unacceptable Uses	4
1.4. Netiquette	5
2. Email.....	6
3. Social Networking Sites/Messaging Software/Apps.....	7
4. Office 365 and One Drive	8
4.1. Cyber Security.....	8
4.2. Bring Your Own Device (BYOD).....	8
5. Disciplinary Action	10
5.1. Advice	10
5.2. Standards for live and recorded lessons	10
5.3. Teaching from home is different to teaching in the classroom	11
6. Communicating with parents, carers and pupils	12

1. Acceptable Use of ICT - Staff

At Mossley Hollins High School we will ensure that at every level, in all our work and throughout all aspects of the school community and its life, all will be treated equally, with respect and dignity, free from discrimination and harassment. Each person will be given fair and equal opportunities to develop their full potential regardless of their age, disability, gender, gender-identity, race, religion or belief, sexual orientation, pregnancy and maternity (refers to staff / employment), socio-economic background and special educational needs. Our school will tackle the barriers which could lead to unequal outcomes for these protected groups, ensuring there is equality of access and that we celebrate and value the diversity within our school community. The school will work actively to promote equality and foster positive attitudes and commitment to an education for equality.

1.1. Introduction

As use of the internet by employees becomes more widespread, for the protection of the school, the pupils and the employees it is necessary to set out some guidelines for internet use. Employees should read these guidelines carefully, in conjunction with the school ICT Security Policy. Abuse of the internet may lead to disciplinary action being taken.

The use of electronic communication and information retrieval is no more than the addition of another medium. The same behavioural and professional standards are expected of employees as are the case with traditional written communications, the telephone and face to face meetings.

The internet as a resource is constantly changing. These guidelines will be updated in the light of experience and developments of the internet itself.

1.2. Acceptable Uses

As a general principle, internet access is provided to employees to support work related activities. The following list is not intended to be a definitive list, but sets out broad areas of use that the school considers to be acceptable uses of the internet:

- To provide communication within the school via email or the school website
- To provide communication with other schools and organisations for educational purposes
- To distribute electronic copies of the weekly bulletin and newsflash

- To distribute details regarding school meetings
- To provide electronic methods of communication
- Any other use that directly supports work related functions.

1.3. Unacceptable Uses

The following uses will be regarded as not acceptable:

- Using the computer to perpetrate any form of fraud, or software, film or music piracy
- Use for racial, sexual, homophobic or other harassment.
- Use of non-educational games.
- To solicit personal information with the intent of using such information to cause emotional or physical harm.
- Entering into a commitment on behalf of the school (unless you have explicit permission to do this).
- Visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material.
- Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence.
- Hacking into unauthorised areas.
- Publishing defamatory and/or knowingly false material about MHHS, your colleagues and/or our pupils on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format.
- Use of school email address for personal purposes
 - Revealing confidential information about Mossley Hollins High School in a personal online posting, upload or transmission - including financial information and information relating to our pupils, staff and/or internal discussions
 - Use of personal email to communicate with or about any MHHS students
 - Undertaking deliberate activities that waste staff effort or networked resources.
 - Introducing any form of malicious software into the corporate network
 - To disrupt the work of other users. This includes the propagation of computer viruses and use of the internet.
 - Use of any Bit torrent systems
 - Use for personal or private business purposes.

1.4. Netiquette

The following general principles should be adopted:

- Be polite. Do not be abusive in messages to others.
- Use appropriate language. Remember that you are a representative of the school and that you are using a non-private network.
- Do not disrupt the use of the internet by other users: e.g. downloading large files during lesson times and other high-volume activities.

2. Email

- Whenever e-mail is sent, the sender's name, job title, e-mail address and the school's name must be included.
- Every user is responsible for all mail originating from their user ID (e-mail address).
- Forgery or attempted forgery of electronic mail is prohibited.
- Attempts to read, delete, copy or modify the e-mail of other users are prohibited.
- Attempts to send junk mail and chain letters are prohibited.
- If you receive e-mail from outside the school that you consider to be offensive or harassing, speak to your line manager (harassing internal e-mail will be dealt with under the school's guidelines).
- You should be aware that, in the event of the school being involved in legal proceedings, any relevant e-mails (including internal e-mail) may have to be disclosed, on the same basis as is the case for written documents.
- Email should be accessed via school ICT equipment only, if you wish to use a personal device to download school emails, you must ensure that your device is secured by a password at all times, that this password is not shared with any other person and that all reasonable care is taken to prevent unauthorised access to confidential information. You must have security measures to protect the privacy of the content of your device in the event that it is stolen or lost.
- School email must not be used to sign up to non-school related organisations.

3. Social Networking Sites/Messaging Software/Apps

Social media applies to blogs, microblogs like Facebook, X, Bebo, LinkedIn, videos, MySpace, social networks, discussion forums, wikis, and other personal webspace. The Governing Body at this school permits the use of internet, social media and messaging software on work premises, outside of work time, but only where it meets the following guidelines. This is usually outside normal working hours and must not interfere with your or others' day-to-day duties. Personal access, whether accessed via school or personally owned devices, should not be in view of any pupils, and you are reminded to log out or 'lock' the screen immediately upon leaving your mobile phone or PC, even if only for a short while. There may be occasions where you require the use of your mobile phone to authenticate on applications such as Office 365 or CPOMS. Under these circumstances it is considered acceptable to use your mobile phone to grant these requests.

- Do not "speak" for the school unless you have express permission to do so, this covers all comments relating to the school. You must be mindful of any posts you like, share and/or re-post
- Protect yourself from identity theft
- If you can be linked to the school, act appropriately. This includes photos and status updates
- Remember that colleagues, prospective employers, parents and children may see your online information
- School policy is that you are not allowed to be 'friends' with students until they have left us by three years, unless there are exceptional circumstances, eg child, sibling etc
- Please choose your 'friends' carefully, especially in light of the last above. Ensure your settings are on private and only you and YOUR friends can see them.
- If in doubt, please seek advice in school.

4. Office 365 and One Drive

O365 allows access to email, office and files to support teaching and learning. Professional values must be followed when using the software at all time. Below are the key points for the use O365 and One Drive.

- Ensure that adequate measures are taken to protect sensitive data as covered in the ICT Policy
- Office can be downloaded on up to 5 devices but cannot be shared with family and friends or any other 3rd party
- Use of the software is only permitted whilst an employee at MHHS

4.1. Cyber Security

Everyone has a responsibility to ensure the security of the network. This includes using 2 Factor Authentication to access e-mails and remote access.

Signing up to any websites or services that are not school related will be a breach of this policy and can put the network and yourself at risk of a data breach.

4.2. Bring Your Own Device (BYOD)

Bring your own device or BYOD defines acceptable use by school users whilst using 'their own' devices, systems and applications, for accessing, viewing, modifying and deleting of school held data and accessing its systems. This will also include accessing the school's cloud-based management information system (Bromcom). Typically, this will apply when connecting to the school's wireless services or for working from home.

If you wish to BYO to access school systems, data and information you may do so, provided that you follow the provisions of this policy and the advice and guidance provided through the IT Helpdesk. It is the school's intention to place as few technical and policy restrictions as possible on BYOD subject to the school meeting its legal and duty of care obligations.

The School, as the Data Controller, remains in control of the data regardless of the ownership of the device. As a user, you are required to keep school information and data securely. This applies to information held on your device, as well as on school systems. You are required to assist and support the school in carrying out its legal and

operational obligations, including co-operating with IT Services or the Data Protection Officer (DPO) should it be necessary to access or inspect school data stored on your personal device. The school reserves the right to refuse, prevent or withdraw access to users and/or particular devices or software where it considers that they are unacceptable in terms of security, or other risks, to its staff, students, business, reputation, systems, or infrastructure.

The school takes Information and Systems Security very seriously and invests significant resources to protect data and information in its care. The use of your own device MUST adhere to this policy and the school's Data Protection Policy. When you use your own device as a work tool, you MUST maintain the security of the school's information that you handle (which includes but is not limited to viewing, accessing, storing, sharing, deleting and/or otherwise processing). It is your responsibility to familiarise yourself with the device sufficiently to keep data secure.

5. Disciplinary Action

Disciplinary action may be taken against employees who contravene these guidelines, in accordance with the school's disciplinary procedures.

5.1. Advice

If you require any advice on the use of these guidelines, please speak to Rob Pilkington (Director of ICT) or your Line Manager.

5.2. Standards for live and recorded lessons

- Expectations are high – the 7 basics of the MHHS lesson should be employed/adapted in this virtual setting.
- All lessons should have objectives.
- Lessons should be pitched appropriately – adapt shared resources/SOW to ensure all learners can make progress.
- Use success criteria to provide support and challenge.
- Recap and review prior learning.
- Recap and review learning at appropriate intervals throughout the lesson.
- Pause the recording to enable responses – offer possible examples to support non-attenders or address misconceptions.
- Adapt your lesson from the contributions of your attendees.
- Visual aids can stimulate ideas and support understanding.
- Use scaffolds to support independent learning.
- Use this opportunity to provide WAGOLs and explore why these are effective models.
- Opportunities for 'walk and talk' mock-style activities.
- Make vocabulary teaching explicit and support Literacy needs.
- Find opportunities to be creative – could assignments be completed in a more engaging format online?
- Use of quizzes to engage and assess understanding.
- Use of GCSEpod to support independent learning – make links to pods clear so that students can utilise these to secure their understanding/recap learning.

5.3. Teaching from home is different to teaching in the classroom

Teachers should:

- When broadcasting a lesson or making a recording, consider what will be in the background e.g. sit against a neutral background.
- Avoid recording in your bedroom.
- Students should not be in their bedroom.
- Wear professional dress (as per our policy in our staff handbook).
- Use professional language.
- Double check that any other tabs you have open in your browser are appropriate, if you're sharing your screen.
- Ask pupils to turn off your cameras and only unmute if they wish to ask a question or contribute to a discussion etc.
- Ask parents/carers who'll also be there to be mindful that other children might hear them in the background.
- Make a recording of live sessions to support students further and to assist non-attenders.

6. Communicating with parents, carers and pupils

Where education is now having to take place remotely, it's important for schools, teachers and pupils to maintain professional practice as much as possible. When communicating online or by phone with parents, carers and pupils, schools should:

Communicate within school hours as much as possible (or hours agreed with the school to suit the needs of staff) We have expectations with parents/carers already about contacting staff and when they'll get replies, politely remind them about these.

Communicate through the school channels approved by the senior leadership team. As always, staff shouldn't communicate with parents, carers or pupils outside school channels (e.g., they shouldn't talk to parents/carers using their personal Facebook accounts or contact pupils using their personal email addresses or phone numbers).

- Use school email accounts (not personal ones).
- Use school devices over personal devices wherever possible.
- Do not share your personal information.
- Contact through parents'/carers' phones only (unless this itself poses a safeguarding risk).
- Make sure someone else at school is aware/ keep a record of the date and time of each call.
- When speaking to a child, request their parent or carer to be there at the child's end, and have the phone on speaker phone.
- Try to find a quiet or private room or area to talk to pupils, parents or carers.