MIHSG
ICT Acceptable Use Policy
Updated October 2017

Why have an Acceptable Use Policy?

Help us to help you keep safe.

An Acceptable Use Policy is about ensuring that you, as a student at MIHSG can use the internet, email and other technologies available at the school in a safe and secure way. The policy also extends to out of school facilities e.g. equipment; printers and consumables; Internet and email; virtual learning environments and websites.

An Acceptable Use Policy also seeks to ensure that you are not knowingly subject to **identity theft** and therefore fraud. In addition, that you **avoid cyber-bullying** and just as importantly, you **do not become a victim of abuse**. We have also banned certain proxy sites as well as anonymous proxy sites, because they put the school network at risk.

MIHSG recognises the importance of ICT in education and the needs of students to access the computing facilities available within the School. The School aims to make the ICT facilities it has available for students to use for their studies both in and out of lesson times. To allow for this MIHSG requires all students to sign a copy of the Acceptable Usage Policy before they receive their username and password.

Listed below are the terms of this agreement. All students at MIHSG are expected to use the ICT facilities in accordance with these terms. Violation of the terms outlined in this document may lead to loss of access and/or disciplinary action, which will be taken in accordance with the Behaviour Policy of the School.

Please read this document carefully, and sign and date it to indicate your acceptance of the Policy. Access to the School's ICT facilities will only take place once this document has been signed by **BOTH** the **student** and **parent/carer**

1. Equipment

1.1 Vandalism

Vandalism is defined as **any action** that harms or damages any equipment or data that is part of the School's ICT facilities. 1990 (see Glossary). This includes, but is not limited to:

- Deliberate damage to computer hardware such as monitors, base units, printers, keyboards, mice or other hardware
- Change or remove of software
- Unauthorised configuration changes
- Create or upload computer viruses
- Deliberate deletion of files

Such actions reduce the availability and reliability of computer equipment; and puts other users' data at risk. In addition, these actions lead to an increase in repairs of the ICT facilities, which impacts upon every student's ability to use the ICT facilities. The other result of vandalism is that it incurs costs, which reduce the funds available to improve the ICT facilities the School has. Parents/carers will be billed for any vandalised equipment.

1.2 Use of removable Storage Media

MIHSG accepts the fact that you may wish to transfer school work done at home to school using a flash memory device or a CD disk. However MIHSG cannot guarantee that your work will be able to be transferred properly using these.

1.3 Printers and Consumables

Printers are provided in the library for use by students. You must use the printers sparingly and for educational purposes only. Take the time to check the layout and proof read your work using the 'Print Preview' facility before printing.

All printer use is recorded and monitored and therefore if you deliberately use the printer for non-education or offensive material you will be subject to the behaviour management measures of the School which includes the following:

- A warning
- Email and/or Internet facilities removed
- Letter home to parents
- Loss of access to the print facilities available within the School
- Report to the Trustees
- Report to appropriate external agencies like the Police

1.4 Data Security and Retention

All data stored on the MIHSG network is backed up daily and backups are stored for up to at least two weeks. If you should accidentally delete a files or files in your folder or shared area please inform the ICT department immediately so that it can be recovered by the ICT manager. Generally, it is not possible to recover files that were deleted more than 10 days previously.

2. Internet Email

2.1 Content Filtering

Through our Internet service provider, MIHSG provides internet filtering, designed to remove controversial, offensive or illegal content. However, it is impossible to guarantee that all controversial material is filtered. If you come across any inappropriate website or content whilst using the ICT equipment, **you must report it to a member of the ICT department immediately.**

2.2 Acceptable use of the Internet

All Internet access is logged and actively monitored and they are stored for up to at least 2 months and usage reports can and will be provided to any member of staff upon request.

Use of the Internet should be in accordance with the following guidelines:

- Only access suitable material – the Internet is not be used to download, send, print, display or transmit material that would cause offence or break the law.
- Do not access Internet Chat sites. Remember you could be placing yourself at risk.
- Never give or enter your personal information on a website, especially your home address, your mobile number or passwords.
- Do not access online gaming sites. Remember that your use of the Internet is for educational purposes only.
- Do not download or install software from the Internet, as it is considered to be vandalism of the School's ICT facilities.
- Do not use the Internet to order goods or services from on-line, e-commerce or auction sites.
- Do not subscribe to any newsletter, catalogue or other form of correspondence via the Internet.
- Do not print pages directly from a website. Web pages are often not properly formatted for printing and this may cause a lot of waste. If you wish to use content from websites, consider using the copy and paste facility to move it into another application, copyright permitting.

3.0 Privacy and Data Protection

3.1 Passwords

- **Never** share your password with anyone else or ask others for their password.
- When choosing a password, choose a word or phrase that you can easily remember, but not something which can be used to identify you, such as your name or address. Generally, longer passwords are better than short passwords, although you should not exceed 10 characters.
- If you forget your password, inform the ICT department immediately.
- **If you believe that someone else may have discovered your password then inform the ICT department who will request the ICT Manager to provide you with a new one.**

3.2 Security

- **Never** attempt to access files or programs to which you have not been granted access to. Attempting to bypass security barriers may breach data protection regulations and such attempts will be considered as hack attacks and will be subject to disciplinary action.
- You should report any security concerns immediately to a member of staff
- If you are identified as a security risk to the School's ICT facilities you will be denied access to the systems and be subject to disciplinary action.

3.3 Storage and Safe Transfer of Personal Data

- MIHSG holds information on all students and in doing so, we must follow the requirements or the Data Protection Act 1998 (see Glossary). This means that data held about students can only be used for specific purposes and therefore all data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- MIHSG will seek to ensure that personal data sent over the internet will be encrypted or otherwise secured.

4.0 Service

Whilst every effort is made to ensure that the systems, both hardware and software are working correctly, the school will not be responsible for any damages or loss incurred as a result of system faults, malfunctions or routine maintenance. These damages include loss of data as a result of delay, non-deliveries, mis-deliveries or service interruptions caused by the system or elements of the system, or your errors or omissions. Use of any information obtained via the School's ICT system is at your own risk. MIHSG specifically denies any responsibility for the accuracy of information obtained whilst using the ICT systems.

5.0 Network monitoring

For reasons of safeguarding and wellbeing MIHSG uses monitoring software across the computer networks. This software checks all computer activity and searches for keywords and phrases that could be used for grooming or other activity that may put children at risk. This software checks all document types that are opened within school.

Student internet safety curriculum

The school has a clear internet safety education programme delivered primarily as part of the ICT curriculum but referenced in all areas of school life. It covers a range of skills and behaviours appropriate to students' ages and experience, including:

- Digital literacy.
- Acceptable online behaviour.
- Understanding of online risks.
- Privacy and security.
- Reporting concerns.

The school will:

- Plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Remind students through assemblies and the tutor programme about their responsibilities using the Acceptable Use Policy signed by every student.
- Ensure that staff model safe and responsible behaviour in their own use of technology during lessons.
- Ensure that staff and students understand issues around plagiarism and copyright/intellectual property rights, and understand how to critically assess the validity of the websites they use.
- Include E Safety for students as part of safeguarding and code of conduct training for staff

Glossary

Computer Misuse Act

The Computer Misuse Act makes it an offence for anyone to have:-

- Unauthorised access to computer material e.g. if you find or guess a fellow student's password and use it.
- Unauthorised access to deliberately commit an unlawful act e.g. if you guess and fellow student's password and access their learning account without permission
- Unauthorised changes to computer material e.g. if you change the desk-top set up on your computer or introduce a virus deliberately to the school's network system.

Data Protection Act 1998

The Data Protection Act ensures that information held about you is used for specific purposes only. These rules apply to everyone in the school, including teaching staff, support staff, volunteers and governors.

The Act covers the collection, storing, editing, retrieving, disclosure, archiving and destruction of data held about individuals in the school. The Act not only applies to paper files it also applies to electronic files.

The Principles of the Act state that data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Kept no longer than necessary
- Processed in accordance with data subject's rights
- Secure
- Not transferred to other countries without adequate provision.

RIPA – Regulation of Investigatory Powers Act 2002

If a request for authorised access is made to the school they will provide the appropriate access to your ICT records and files. The Act legislates for using methods of surveillance and information gathering to help the prevention of crime, including terrorism. RIPA makes provision for:

- the interception of communications
- the acquisition and disclosure of data relating to communications
- the carrying out of surveillance
- the use of covert human intelligence sources
- access to electronic data protected by encryption or passwords

(MM/KF)

REQUIRED SIGNATURES

STUDENT

I understand and agree to the provisions and conditions of this agreement. I understand that any disobedience to the above provisions may result in disciplinary action and the removal of my privileges to access ICT facilities. I also agree to report any misuse of the system to a staff member and I understand that misuse may come in many forms but may be viewed as any messages sent or received that indicate or suggest pornography, unethical or illegal activities, racism, sexism inappropriate language, any act likely to cause offence.

NAME: _____ FORM: _____

SIGNATURE: _____ DATE: _____

PARENTS / GUARDIANS

As the parent or Guardian of _____

I have read this agreement and understand that access to electronic information services is designed for educational purposes. I understand that, whilst the Internet service provider operates a filtered service, it is impossible for MIHSG to restrict access to all controversial materials and will not hold the school responsible for materials acquired on the network. I also agree to report any misuse of the system to the school. I hereby give my permission to MIHSG to permit my daughter access to electronic information services and I certify that the information given on this form is correct.

NAME: _____

SIGNATURE: _____ DATE: _____