

## **Rationale**

At the Midlands Academy of Dance & Drama (M.A.D.D) we believe ICT to be one of the core components of the learning experience and that it facilitates the journey and enhances learning by providing access to the wealth of information, often freely available.

The internet is an essential element of modern education, business and social interaction. ICT skills and knowledge are vital for life-long learning and employment opportunities. ICT is now seen as a functional, essential life-skill along with language and numeracy. Curriculums require pupils to learn how to locate, retrieve and exchange information using technology including the internet. All learners are given the opportunity to learn to use the internet safely and efficiently to develop a responsible and mature approach to accessing, interpreting and disseminating information. Internet access is provided on the understanding that agreement is given to follow the guidelines contained within this document.

## **Benefits to Education**

- Access to educational resources including performance archives, music, museums and art galleries world-wide.
- Cultural, vocational, social and leisure utilisation.
- Access to experts and their published information in many fields, for both students and staff.
- Staff continuous professional development (CPD) through access to national development platforms, educational materials and good curriculum practice resources.
- Communication with support services, professional associations and colleagues.
- Improved access to technical support including remote management of networks.
- Exchange of curriculum and administration data with the Local Authority and the DfES.

## **Benefits to Learning**

- The organisation provides limited internet access for student use.
- Students will be taught what internet use is acceptable and what is not, and given clear objectives for its use.
- Internet access will be used to enrich and extend learning activities.
- Staff will guide students through on-line activities that will support the anticipated learning outcomes.
- Students will be educated in the effective use of the internet for research purposes, including the skills of knowledge location, referencing, retrieval and evaluation to ensure the content is suitable and fit for purpose.

Our conditions of use reflect the strong emphasis we place on promoting and recognising good behaviour and working patterns as well as the legal implications of copyright, data protection, and the creation or publication of offensive material.

## **The Policy**

At M.A.D.D the ICT facilities may only be used for legal activities consistent with the aims of the Academy and the behaviour policy. The computer network and internet facilities are provided for the purpose of curriculum related activities and recognised academy work. Failure to comply with the terms and conditions of the ICT User Policy will result in a temporary or permanent ban from the network and its associated services. Additional action may be taken in line with the disciplinary

procedures. Where applicable, police or local authorities may also be notified if required or deemed appropriate.

All computer and internet users should be aware that any material accessed or transmitted may be viewed by the system administrator at any time and may be monitored.

It is considered a serious breach of the ICT User Policy and Behaviour Policy to make use of the internet or email in such a manner to bring the name of the Academy into disrepute. All users of the computer systems and internet services must follow the same principles of acceptable behaviour, as stated in the Staff/Student Handbooks. This includes, but is not exclusive to, such potential issues as racist, sexist, homophobic, extremist, violent or abusive language, content or images.

M.A.D.D uses the Clean Browsing content filtering system and has in-place email scanning and virus protection to ensure that potentially harmful, unsafe or inappropriate material is restricted from accessing the network.

As far as is reasonably possible, students will be directed to information sources that have been reviewed and evaluated prior to use. However, students may pursue electronic research independently of staff supervision and we are aware that students might find ways to access unsuitable material. Our view is that parents or guardians of students are ultimately responsible for setting and conveying standards that their children should follow when using media and information.

## **E-Safety**

A large proportion of the material on the internet is published for an adult audience and some will be unsuitable for students. In addition, there is information on weapons, crime and racism that would be considered inappropriate and restricted elsewhere. In-line with our policies to protect students from other dangers, M.A.D.D takes every precaution to provide students with as safe an internet environment as possible and instructs students to be aware of, and respond responsibly to any risk that presents itself.

## **Policies & Procedures**

The organisation:

- Supervises students' use as far as is reasonable.
- Uses the Clean Browsing content filtering system to restrict websites that fall into categories previously stated in the policy.
- Is vigilant when conducting 'raw' image searches with students e.g. Google or other platform image searches.
- Informs users that their internet use is filtered and monitored.
- Informs staff and students that they must report any failure of the filtering systems directly to a member of staff or IT Manager immediately.
- Requires staff and students to be made aware of the acceptable use agreement, which is fully explained and used as part of the teaching programme. This includes agreed consent to use the internet under supervision in the learning environment.
- Makes clear all users know and understand what the '*rules of appropriate use*' mean and what sanctions result from misuse through staff meetings and the teaching programme.
- Records of any breach of the acceptable use policy are kept on file permanently.
- Immediately refers any material we suspect is illegal to the appropriate authorities, police and the local authority.
- When logging on to any computer or device in the Academy, all users agree to the following rules and regulations.

## **The Academy does not permit the following activities:**

- Sending or displaying offensive messages or images.
  - Accessing undesirable material e.g. pornography, extremist content.
  - Contacting members of staff through any social networking platform.
  - Accessing social networking sites/chat rooms during lessons.
  - Posting undesirable, abusive or derogatory comments on websites.
  - Using racist, sexist, homophobic, violent or abusive language through email or messaging platforms and other internet platforms.
  - Knowingly introducing viruses to the organisations network.
  - Accessing another students files, folders and documents.
  - Intentionally wasting resources used for printing.
  - Interfering with the functioning of the network or any other network that can be accessed via the internet.
- 
- Any breach of security that results in information being made available or displayed to others, either publicly or privately.
  - Any attempt to corrupt or destroy data, violate site privacy or deny service by overloading the network or an individual's email box.
  - Any attempt to create, transmit, publish or receive any material likely to cause offence, inconvenience or needless anxiety.
  - Any attempt to install personal or home software (including games) onto the network or the computer systems.

M.A.D.D will challenge and apply sanctions (in line with the Disciplinary Policy, including denial of access to the ICT systems) against any perpetrator(s) who are found in breach of the organisations ICT Policy. This may, in some instances, lead to criminal prosecution.

## **E-mail**

- Sending malicious or threatening e-mails and other messages is a criminal offence under the Protection from Harassment Act (1997), the Malicious Communications Act (1988) and Section 43 of the Telecommunications Act (1984).
- Students must immediately inform a member of staff if they receive inappropriate or offensive e-mail.
- The forwarding of anonymous messages and chain letters is not permitted.
- The use of obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language is not permitted, and may be subject to the organisations disciplinary procedures.

## **Education & Training**

The organisation:

- Fosters a 'no blame' environment that encourages students to tell a responsible adult immediately if they encounter any material that makes them feel uncomfortable.
- Ensures students and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to a member of staff or IT Manager.
- Ensures all students know how to report abuse.
- Ensures that when using material from the internet, staff and pupils understand issues around plagiarism, how to check copyright and also know that they must observe and

respect copyright / intellectual property rights. For further information learners and staff should refer to [www.cla.co.uk](http://www.cla.co.uk).

- Students should not copy or use material from the internet without acknowledging the source. Failure to acknowledge the source, thereby gaining unfair advantage (plagiarism), may lead to disqualification by examination boards.

## Technology & Infrastructure

The organisation:

- Ensures network functionality through appropriate anti-virus software and network set-up so staff and pupils are at a reduced risk of encountering malicious programs.
- Ensures the IT manager confirms that the filtering methods are in place and that they restrict access to websites considered inappropriate.
- Never allows pupils access to internet logs.
- Never sends personal data over the internet unless it is encrypted or otherwise secured.
- Never allows personal level data off-site unless it is on an encrypted device.

## The Website

- The point of contact on the website is the organisations address, e-mail and telephone number. Staff or students personal information will not be published unless authorisation is received.
- The Principal will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The copyright of all material must be held by M.A.D.D, or be attributed to the owner, where permission has been obtained. **Inappropriate Websites and Material**
- In common with other media such as magazines, books and video, some material available via the internet is unsuitable for students. M.A.D.D will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on all computer systems. The organisation cannot accept liability for information accessed, or any consequences as a result of internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed periodically.
- Students will not knowingly search for profane, harmful or obscene material, that advocates illegal acts, or that advocates violence or discrimination towards others.
- If staff or students discover unsuitable sites, the URL (website address) and content must be reported to a senior member of staff.

## Policy Awareness

- Staff should be aware that internet traffic may be monitored, with discretion and professional conduct being expected at all times.
- **Students** will be informed that all internet use is monitored and exercises its right to audit the use of the computer systems, including the interception and monitoring of e-mail. Files

will be subject to deletion if unauthorised use of the Academy's computer system taking place.

- **Parents / Carers** attention will be drawn to the Academy ICT User Policy in newsletters, during enrolment and is contained in the prospectus.

## **NETWORK**

### **Network Security**

- The ICT systems will be reviewed periodically with regard to security.
- Students will immediately inform a member of staff or IT Manager if they identify a potential security issue.
- Virus protection will be installed.
- Use of portable media such as memory sticks will be subject to a virus check when used on the network.
- Files held on the network will be regularly checked for viruses and malicious software.

### **It is not permitted to:**

- Attempt to download, store or install software on the organisations computers.
- Attempt to introduce a virus or malicious code to the network.
- Attempt to bypass network or system security.
- Attempt to use any form of hacking software, system or practice.
- Access, download, create, store or transmit material that is indecent or obscene material that could cause annoyance, offence or anxiety to other users, or material that infringes copyright or is unlawful.

## **NEW TECHNOLOGIES**

New and emerging technologies will be examined for educational benefit, reliability and whether they provide any benefit to the learner and represent value for money.

### **Mobile Devices**

- Mobile phones will not be used during lessons or formal lesson time, unless otherwise directed by a staff.
- The sending of abusive, sexual or inappropriate text messages is forbidden; all incidents will be investigated and may be subject to the Academy's disciplinary procedure
- Students must not use camera phones to take or distribute photographs of other students or staff without their knowledge or consent. Any student who is concerned that they have been photographed without their consent or that someone is misusing their camera phone should immediately report their concerns to a member of staff.
- It is an offence to send obscene, indecent or menacing images.
- Technology that can be used to store, transmit or manipulate data, such as media rich phones, MP3 players, personal digital assistants (PDAs), USB media or tablet computers should be used responsibly and in accordance with the ICT User Policy, even when not used with M.A.D.D equipment.

### **Staff use of mobile phones**

Tutors mobile phone should not be on during classes.

In keeping with the organisations non-fraternisation rule of employment, staff members must not interact with pupils or students on social networking sites. Staff are not permitted to hold pupil or student phone numbers in their devices and should not give out their personal phone number to pupils or students. Staff should take an organisation mobile phone for any off-site activities and trips. This phone should be used as a contact point for students.

The only exception to the above will apply to rehearsal periods when out of hours contact is occasionally essential.

### **The taking of photographs of Pupils and Students by adults**

It is not permitted for staff, parents or other adults to take still or moving images of pupils or students whilst in Academy or in productions without the express permission of the Academy. This is printed in all Academy's show programmes.

#### **POLICY VIOLATION**

- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any complaint about staff misuse will be referred to the Principal.
- Students and parents will be informed of the complaints procedure at this juncture.
- Sanctions include:
  - Interview/counselling.
  - Informing Parent/Carer.
  - Temporary or permanent ban of internet use.
  - Where appropriate, police or local authorities may be involved.

**Reviewed:** September 2025  
**Next review due:** September 2026