RAMBERT SCHOOL
INFORMATION TECHNOLOGY POLICY ~ acceptable use

Scope

This is a universal policy that applies to all Users and all Systems. This policy covers only internal use of Rambert Schools systems, and does not cover use of our products or services by third parties.
Some aspects of this policy affect areas governed by local legislation in certain countries (e.g., employee privacy laws): in such cases the need for local legal compliance has clear precedence over this policy within the bounds of that jurisdiction. In such cases local teams should develop and issue users with a clarification of how the policy applies locally.
As a school of the Conservatoire for Dance and Drama, Rambert School has a statutory duty, under the Counter Terrorism and Security Act 2015, which is termed Prevent. The purpose of this duty is to aid the process of preventing people being drawn into terrorism. This Prevent duty informs its policy on the acceptable use of IT systems. Staff members at Rambert School who monitor and enforce compliance with this policy are responsible for ensuring that they remain compliant with relevant local legislation at all times. Links to local laws and legislation relating to this document are provided at the end of this document (if you are reading this in an electronic format) or copies can be obtained from the IT department.

Policy

Rambert has both internet and email facilities. Access to both is granted to Administration, Artistic and Academic Staff and a limited facility is available to Students. All Staff and Students are expected to utilise both systems in a responsible manner. Under no circumstances should staff or student members allow anyone to know their password.

As a staff member or student, you are provided with access to the internet and email for business and educational use. The following policy governs your use of the internet, and email. It is not intended to inhibit, but is to be used as a guide asking you to exercise common sense and discretion.

Access to the internet is strictly limited, where access is given the following restrictions will apply:

- Staff and students are banned from using the internet for private or freelance business,

- Staff and Students are banned from visiting pornographic sites or conducting political activities.

- Browsing and surfing should not be carried out in the School's time.

- All Users are forbidden to access, create and transmit offensive, obscene and indecent material on the internet

Procedures

The School's computer system is managed and monitored by ClickOn IT London Ltd. In case of any computer problem during office hours, staff and students should advise Jonathan Aloia in the Administration Office or any other member of the Administration Department in his absence.

Staff have access to shared files through the network with documents being stored on the S Drive.

No documents should be kept on a computer's hard drive, for instance on the desktop, as such documents will not be backed up in case of system loss.
Any changes to current user accounts must be authorised by Jonathan Aloia.

Passwords must be kept private and not disclosed to any other person. The system will prompt every user to change their password the first time they log in and thereafter twice a year. The system will remember the last three passwords used and will not allow them to be repeated. Passwords must be at least eight characters in length and include a Capital letter and one number/symbol.

Any requirements to add new software to the system must be authorised by Jonathan Aloia.

The server is located in the Downstairs Wardrobe. Access to the server is limited to the Administration department. Back ups are taken every evening and stored remotely.

Limited personal use of the Internet for sending or receiving personal e-mail is acceptable as long as it does not interfere with your work and providing you exercise good judgment. If you use your School email account for personal statements, it is recommended you use the following:

"The statements and opinions expressed here are my own and do not necessarily represent those of Rambert School".

Viruses

- The School uses a comprehensive software programme to monitor email attachments for viruses. However, this is not a 100% effective method and viruses can still be transmitted. Therefore, care should be exercised and email attachments should only be opened if the recipient is known, or the email is expected. Email attachments are a potential source of a virus infection and may contribute to excessive network traffic.
- Phishing emails may be received from unscrupulous companies. These are emails apparently from established companies requesting School information, such as bank details. The companies the School deals with will never ask for this information by email and these emails should always

be considered a hoax and deleted without replying. If you are in any doubt, you should ask the Finance Assistant or Finance Director.

Some of these factors are a crime under the Computer Misuse Act 1990.

Legal Issues

- Be warned…email messages do not disappear; they are permanently recorded and available to be reassembled at a later date and consequently can be libellous. Retrieval is possible even when they have apparently been deleted from computers. In law, internal emails and paper memos are not distinguished between. Broadly speaking an untrue statement of fact which damages the reputation of a person or company by causing people to think worse of the victim, will be libellous.
- Copyright infringement can occur when downloading files from the internet with no express or implied permission to do so and includes graphics, sound effects and text that is copied into or attached to an email message. Additionally, the new material may not be licensed.
- Emails have to be disclosed if requested for court cases. Messages about an employee that could be relevant in future litigation must be printed and placed in the employee's personnel file.
- Email messages can be legally binding. Contracts can be set up via email.
- Police are entitled to intercept email messages and read them without obtaining warrants.

Computer Misuse Act 1990

The following activities are offences under the Computer Misuse Act 1990.

- **Password Offences and Hacking -** A person is guilty of an offence if they cause a computer to perform any function with the intent of securing access to any programme or data, knowing that the intended access is unauthorised.
- **Computer modifications** – A person is guilty of an offence if they perform modifications such as adding or deleting data, knowing that they are not authorised to do so.
- **Viruses** – A person is guilty of an offence if they introduce a virus, even if they do not know where or what the effect will be.
- **Data Protection** – A person is guilty of an offence if they fail to exercise appropriate security measures to protect data covered by the Data Protection Act.

Employees should be aware that penalties under the Act vary from fines to a maximum of 5 years imprisonment in relation to offences involving the use of the computer to commit an arrestable offence.

Security & Monitoring

- To ensure the School gains the maximum benefit from computers and to prevent legal cases the School may monitor the use of the systems (email and internet). From time to time the School may monitor staff and students messages.
- All breaches of computer security will be referred to the Principal. Where a criminal offence may have been committed, the line manager in conjunction with the Director will decide whether to involve the police.
- Any staff member or student who suspects that a fellow employee or student is abusing the computer system may speak in confidence to the Principal. Staff or students who breach the company policy may be

dealt with by the School's disciplinary procedure. The level of sanction will be dependant on the severity of the breach.

- Misuse of computers is a serious disciplinary offence and may result in summary dismissal. This is not an exhaustive list, but the following are some examples of misuse:-

  - Fraud and theft
  - System sabotage
  - Introduction of viruses and time bombs
  - Using unauthorised software
  - Obtaining unauthorised access
  - Using the system for non business use
  - Sending flame mail or mail that is harassing by nature
  - Hacking
  - Breach of company security procedures
  - Taking part in electronic chain letters
  - Accessing pornography
  - Engaging in on-line gambling
  - Downloading or distributing copyright information.
  - Posting confidential information about Rambert or its customers or suppliers

Monitoring and Filtering

All data that is created and stored on School computers is the property of the School and there is no official provision for individual data privacy, however wherever possible the School will avoid opening personal emails.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy.

The School has the right (under certain conditions) to monitor activity on its systems, including internet, email and social media use, in order to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with audited, controlled internal processes, GDPR, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

The School employs filtering of web content. Examples of content filtered include: Abused drugs, bot nets, cheating (academic), confirmed spam sources, cult and occult, gambling, hate and racism, illegal, malware sites, marijuana, peer to peer, spyware and adware, violence, weapons, religion.

RAMBERT SCHOOL

Sept 2019