RAMBERT SCHOOL

RAMBERT SCHOOL
INFORMATION TECHNOLOGY POLICY: ACCEPTABLE USE
September 2023-

Contents

RAMBERT SCHOOL
INFORMATION TECHNOLOGY POLICY: ACCEPTABLE USE
September 2023-

1. Introduction and Scope of the Policy

This is a universal policy that applies to all Users and all Systems of Rambert School, including but not limited to students and staff. For some Users and/or some Systems a more specific policy exists (such as for our students): in such cases the more specific policy has precedence in areas where they conflict, but otherwise both policies apply on all other points.

This policy covers only internal use of Rambert Schools systems, and does not cover use of our products or services by third parties. This policy is intended to provide a framework for the use of Rambert School's IT resources. It applies to all computing, telecommunication and networking facilities provided by Rambert School to its staff and students, and any other user authorised by an Officer of Rambert School in their professional capacity to access these facilities (eg a Trustee; guest lecturer etc).

This policy applies to all IT facilities provided by Rambert School (including computers and other hardware), and extends to the use of such facilities to connect to external IT facilities, as well as the use of personal equipment if used on School business or to transmit information via Rambert School IT facilities.

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 Higher Education Provider registered with the Office for Students, 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 Rambert School's 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.

2. Policy

Rambert School has internet facilities, including email and Microsoft Teams communications systems. Members of staff are provided with access to the internet and online communications systems for business use, and students are granted access to a limited facility.

All Staff and Students are expected to utilise both systems in a responsible manner. Under no circumstances should staff members allow anyone to know their password.

The following policy governs all members' use of the internet, and email. It is not intended to inhibit, but is to be used as a guide asking staff and students to exercise common sense and discretion. Rambert School undertakes to treat all staff and students fairly at all times, and this extends to any action exercised under this Policy.

Any concerns, complaints or queries regarding this policy may be raised with the Academic Registrar & Head of Compliance in the first instance.

Allied Policies

The following policies and documents are allied to this policy:

- Emergency Powers of Exclusion & Suspension
- IT Security Policy
- Non-Academic Misconduct Policy & Procedures
- Policy on Sexual Misconduct, Harassment & Related Behaviours
- PREVENT Strategy
- PREVENT Policy
- Staff Disciplinary Procedure
- Staff Grievance Procedure
- Student Complaints Procedure
- Student Terms & Conditions
- Support Through Studies Policy & Procedures

3. Acceptable Use

Rambert School has a duty of care to all students and staff and this policy is intended to support this duty of care, as well as providing clarity for our community on what the School considers to be unacceptable use of its IT systems and internet resources.

Access to the internet is strictly limited to persons granted access by an authorising Officer of Rambert School (such as the Head of Facilities, Office Management/HR staff, or a member of the School Senior Management Team; other staff may be delegated to grant authorisation by the Chief Executive, Principal & Artistic Director and/or Chief Finance Officer as and when required).

Personal use

Use of Rambert School IT facilities for personal activities is permitted, provided that it does not infringe the law or any School policies, does not interfere with the valid use of these facilities by other members of our community, and for staff, is not done inappropriately during their working hours.

The use of Rambert School emails or other services for outside bodies that is being undertaken on a personal basis, solely for personal gain and not through Rambert School channels, requires explicit permission from the Chief Executive, Principal & Artistic Director.

PREVENT

In ensuring that Rambert School is fulfilling its obligations with regard to PREVENT and is taking the necessary and appropriate steps to prevent terrorism and reduce the risk of radicalisation, our rules on unacceptable use (set out below) take account of this duty.

Rules on unacceptable use

The following constitute unacceptable use of Rambert's IT systems and facilities:

- Accessing, creating, downloading, sharing or transmitting illegal, indecent, offensive or obscene materials (eg pornographic/extremist/terrorist-related materials)
- Downloading or accessing materials that infringe personal liberties or promote extreme political views or radicalisation
- Creating websites (including webpages, vlog and blog posts) that are obscene, defamatory, infringe copyright, infringe personal liberties or promote extremist political views, terrorism or radicalisation
- Accessing websites which support academic misconduct (ie 'essay mills' or 'academic cheat sites')

4. Procedures

IT Support and Management

The School's computer system is managed and monitored by ClickOnIT London Ltd. In case of any computer problem during office hours, staff and students should advise the Facilities Manager or ClickOnIT directly, in their absence.

Access to institutional documents

Staff have access to shared files through the network with documents being stored on a cloud-based system.

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.

Heads of Department are responsible for ensuring that their departmental files are suitably accessible to authorised personnel, and that in the event of a staff member leaving this does not pose any limitations for the department that may affect the business of the institution.

New User Accounts

Requests for new user accounts must be made through the Facilities Manager, Chief Finance Officer or Head of Administration. Any changes to current user accounts must be authorised by the Facilities Manager, Chief Finance Officer, Head of Administration, or a nominee of the Chief Finance Officer or Head of Administration.

Passwords

Passwords must be kept private and not disclosed to any other person.

New software

Any requirements to add new software to the system must be authorised by the Facilities Manager and Chief Finance Officer. Only authorised personnel should be granted access to the School IT Server; please contact the Facilities Manager with any queries about the Server.

Personal use of Rambert School Internet

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 good practice to ensure that it is clear these are your own views. 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".*

Notwithstanding the above, it is also important to remember that as a student or staff member of Rambert School, in all circumstances you are an ambassador for, and representative of, the School. Please see the **Social Media Policy** for additional guidelines on social media use as a member 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 Facilities Manager or ClickOnIT directly.
- Some of these factors are a crime under the Computer Misuse Act 1990 (see further on in this policy for more details about this Act).

Legal Issues

- **Never send an email or electronic communication that you wouldn't be happy to have read out in court.**

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 placed on 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.

Staff and students 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.

5. Breaches of this Policy

Misuse of computers is a serious disciplinary offence and may constitute gross/serious misconduct. 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 inappropriately 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 copyrighted information without authorisation.
- Posting confidential information about Rambert School, its community, or its customers or suppliers

Students

Students alleged or suspected to have committed a potential breach of this policy will normally be referred into the procedures under the Non-Academic Misconduct Policy & Procedures to determine whether or not an alleged breach has occurred.

In certain circumstances an alleged breach may necessitate the use of Emergency Powers of Exclusion and Suspension, or Precautionary Measures under the Policy on Sexual Misconduct, Harassment and Related Behaviours. Where such emergency measures are taken, these will be without prejudice and have no bearing on, nor constitute any indication of any School finding with regard to an alleged breach of this policy.

Where on the balance of probabilities the School establishes that a breach has occurred, the School will take into account whether the breach is minor or major and the nature of the breach, in determining any action, including the level of any sanction/penalty.

Any queries regarding the above should be addressed to the Academic Registrar & Head of Compliance.

Staff

Staff alleged or suspected to have committed a potential breach of this policy will normally be referred to HR, to determine whether there is a need to refer the matter into staff disciplinary procedures. Where necessary, staff may be suspended without prejudice pending an investigation.

Where on the balance of probabilities the School establishes that a breach has occurred, the School will take into account whether the breach is minor or major and the nature of the breach, in determining any action, including the level of any sanction/penalty.

Any queries regarding the above should be addressed to the Head of Administration.

Criminal investigations

Where a staff member or student is alleged to have committed a criminal offence that may also constitute a breach of this policy, the School may take action under relevant policies (see above) to suspend or exclude that staff member or student without prejudice pending conclusion of the criminal investigation. In determining what action should be taken, the School will use a risk-based approach to assess the most appropriate course of action, subject to the nature and severity of the alleged criminal offence and taking account of the duty of care to its community.

Alleged IT misuse/breach of this policy involving suspected extremist/radicalisation materials (PREVENT)

Where a student or staff member is alleged to have or suspected of having accessed, created, downloaded, shared or transmitted materials which are extremist/terrorist-related and/or which may present a risk of radicalising an individual or a group of individuals, this should be **immediately** reported to the PREVENT Single Point of Contact (SPOC), who is the Academic Registrar & Head of Compliance. In the event that the PREVENT SPOC is not available, the Chief Executive, Principal and Artistic Director or the Head of Admissions, Student Support and Registry, should be contacted.

6. 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 student messages, including email and TEAMS or other messaging platforms.
- 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 Principal will decide whether to involve the police.
- Any member of staff who suspects that a fellow employee or student is abusing the computer system may speak in confidence to the Principal. Please see Section 5 'Breaches of this Policy' for further information about breaches of this Policy and what action may be taken.

7. 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, the UK Data Protection Act 2018, 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, but are not limited to:

- Abused drugs
- bot nets, cheating (academic)
- confirmed spam sources
- cult and occult
- gambling
- hate speech/acts, including but not limited to racism, transphobia, anti-Semitism, religious intolerance or other targeted hate
- illegal malware sites
- marijuana
- spyware and adware
- violence (including weapons)