ISTITUTO MARANGONI LONDON

ICT POLICY

September 2023

Version Control Statement

Version	3.0		
Document title	Istituto Marangoni London ICT Policy		
Document approved by	Prevent Working Group London School Board		
Approval date	7 September 2021		
Date for review	September 2023		
Amendments since approval	Detail of revision	Date of revision	Revision approved by
	Changed Section 1.2, 3.5, 4.2, 8.1	12/08/2021	London School Board
	Changed section 5.8	24/07/2023	

0. TABLE OF CONTENT

1. About This Policy & Definitions

1.1 Istituto Marangoni London ICT and communications systems are intended to promote effective communication and working practices within the organisation. This policy outlines the standards you must observe when using these systems, the circumstances in which the School will monitor your use, and the action the School will take in respect of breaches of these standards.

1.2 This policy covers Employees & Faculty, Visitors and anyone who has access to the School's IT and communication systems.

1.3 Misuse of IT and communications systems can damage the business and the reputation. Breach of this policy may be dealt with under the Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

1.4 This policy does not form part of any employee's contract of employment and it may be amended at any time.

1.5 Definitions used within this policy are the following:

I(C)T: Information (Communication) Technology

Data: Any and all information relating to the business, employees and customers

System(s): Any and all software or database (e.g email, phone, file sharing or file storage)

The School: Istituto Marangoni Limited

2. Personnel Responsible for the Policy

2.1 The ICT Department, Communications Department and HR Department all have overall joint responsibility for the effective operation of this policy and for ensuring compliance with the relevant statutory framework. Day-to-day responsibility for operating the policy and ensuring its maintenance and review has been delegated to the ICT Department.

2.1 Managers have a specific responsibility to ensure the fair application of this policy and all members of staff are responsible for supporting colleagues and ensuring its success.

2.2 The ICT Department will deal with requests for permission or assistance under any provisions of this policy and may specify certain standards of equipment or procedures to ensure security and compatibility.

3. Equipment Security And Passwords

3.1 You are responsible for the security of the equipment and accounts allocated to or used by you and must not allow it to be used by anyone other than yourself in accordance with this policy.

3.2 You are responsible for the security of any computer terminal used by you. You should lock your terminal or log off when leaving it unattended or on leaving the office, to prevent unauthorised users accessing the system in your absence. Anyone who is not authorised to access the School's network should only be allowed to use terminals under supervision.

3.3 Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting the ICT Department.

3.4 You should use passwords on all ICT equipment, particularly items that you take out of the office. You must keep your passwords confidential and change them regularly. You must not use another person's username and password or make available or allow anyone else to log on using your username and password. On the termination of employment (for any reason) you must return any equipment, key fobs or access cards to the ICT Department.

3.5 You must not use another person's username and password or make available or allow anyone else to log on using your username and password unless authorised by your line manager.

3.6 If you have been issued with a laptop, tablet computer, smartphone or other mobile device, you must ensure that it is kept secure at all times, especially when travelling. You should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport.

4. Systems And Data Security

4.1 You should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of your duties).

4.2 You must not download or install software from external sources without written or verbal authorization from the ICT Department. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files.

4.3 You must not attach any device or equipment to our systems without authorization from the ICT Department. This includes any USB flash drive, tablet, smartphone or other similar device, whether connected via wired or wireless connection.

4.4 The School monitors all emails passing through the system for viruses. You should exercise particular caution when opening unsolicited emails from unknown sources or an email which appears suspicious (for example, if it contains a file whose name ends in .exe .dmg or .pkg Or it is sent by an unknown sender as well as senders with a similar spelling of a company name). Inform the ICT Department immediately if you suspect your computer may have a virus. The School reserves the right to delete or block access to emails or attachments in the interests of security.

4.5 You should not attempt to gain access to restricted areas of the network, or to any password-protected information, except as authorised in the proper performance of your duties.

5. Email

5.1 Although email is a vital business tool, you should always consider if it is the appropriate method for a particular communication. Correspondence with third parties by email should be written as professionally as a letter. Messages should be concise and directed only to relevant individuals. Our standard disclaimer should always be included.

5.2 You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, or otherwise inappropriate emails. Anyone who feels that they have been harassed or bullied, or are offended by material received from a colleague via email should inform their line manager or the Human Resources Department.

5.3 You should take care with the content of email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Remember that you have no control over where your email may be forwarded by the recipient. Avoid saying anything which would cause offence or embarrassment if it was forwarded to colleagues or third parties or found its way into the public domain.

5.4 Email messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable, either from the main server or using specialist software.

5.5 In general, you should not:

5.5.1 send or forward private emails at work which you would not want a third party to read;

5.5.2 send or forward chain mail, junk mail, cartoons, jokes or gossip;

5.5 contribute to system congestion by sending trivial messages, copying or forwarding emails to those who do not have a real need to receive them, or using "reply all" unnecessarily on an email with a large distribution list;

5.5.4 sell or advertise using our communication systems or broadcast messages about lost property, sponsorship or charitable appeals;

5.5.5 download or email text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this;

5.5.6 send messages from another person's email address (unless authorised) or under an assumed name;

5.5.7 send confidential messages via email or the internet, or by other means of external communication which are known not to be secure;

5.6 If you receive an email in error you should inform the sender by directly replying to them and do not cc everyone else.

5.7 Do not use your own personal email account to send or receive email for the purposes of the School business. Only use the email account(s) the School has provided for you.

5.8 In the event that the employee has to leave the school, the mailbox should be deactivated by setting up an automatic responder that provides the sender with the contact details of another recipient who can guarantee business continuity.

The competent IT staff will delete the former employee's mailbox within a maximum of 30 working days.

6. Internet Usage

6.1 Internet access is provided primarily for business purposes. Occasional personal use may be permitted as set out in paragraph 7.

6.2 When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is of a kind described in paragraph 9.1, such a marker could be a source of embarrassment to the visitor and the School, especially if inappropriate material has been accessed, downloaded, stored or forwarded from the website. Such actions may also, in certain circumstances, amount to a criminal offence if, for example, the material is pornographic in nature.

6.3 You should not access any web page or download any image, document or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral. Even web content which is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

7. Personal Use Of School Systems

7.1 The School permits the use of the internet, email and telephone systems to send personal email, browse the internet and make personal telephone calls subject to certain conditions set out below. Personal use is a privilege and not a right. It must not be overused or abused. We may withdraw permission for it at any time or restrict access at our discretion.

7.2 Personal use must meet the following conditions:

7.2.1 use must be minimal

7.2.2 use must not interfere with business or office commitments;

7.2.3 use must not commit us to any marginal costs; and

7.2.4 use must comply with this policy (see in particular paragraph 5 and paragraph 6) and the School’s other policies including the Equal Opportunities Policy, Anti-harassment Policy, Privacy Standard and Disciplinary Rules.

7.3 You should be aware that personal use of the School’s systems may be monitored (see paragraph 8) and, where breaches of this policy are found, action may be taken under the disciplinary procedure (see paragraph 9). The School reserves the right to restrict or prevent access to certain telephone numbers or internet sites if the School considers personal use to be excessive.

8. Monitoring

8.1 The School systems monitor email and internet use and contents for antivirus and internet safety reasons, and in order to carry out legal obligations in the role as an employer. Monitoring is only carried out by computers and automated systems.

8.2 Audio recordings of Phone calls and contents of text messages (including SMS, WhatsApp or Other) are never monitored or recorded.

8.3 We reserve the right to manually retrieve the contents of email messages or check internet usage in the interests of the business, for the following purposes (this list is not exhaustive):

8.3.1 to assist in the investigation of alleged wrongdoing; or

8.3.2 to comply with any legal obligation.

9. Prohibited Use Of The School’s Systems

9.1 Misuse of the telephone or email system or inappropriate internet use will be dealt with under our Disciplinary Procedure. Misuse of the internet can in some circumstances be a criminal offence. In particular, it will usually amount to gross misconduct to misuse the systems by participating in online gambling, forwarding chain letters, or by creating, viewing, accessing, transmitting any of the following material (this list is not exhaustive):

9.1.1 pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

9.1.2 offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our clients;

9.1.3 a false and defamatory statement about any person or organisation;

9.1.4 material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equal Opportunities Policy or our Anti-harassment and Bullying Policy);

9.1.5 confidential information about the School or any staff or clients (except as authorised in the proper performance of your duties);

9.1.6 any other statement which is likely to create any criminal or civil liability (for you or us); or

Any such action will be treated very seriously and is likely to result in summary dismissal.

9.2 Where evidence of misuse is found the School may undertake a more detailed investigation in accordance with the Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the Disciplinary Procedure. If necessary, such information may be handed to the police in connection with a criminal investigation.