IT SECURITY POLICY
2020-21 SY UPDATES

INTRODUCTION

This policy ensures that all staff and students follow basic rules about internet and general IT use. It aims to prevent students or staff from coming to harm as a result of others accessing intolerant, extremist, or hateful websites while also protecting students and staff from cyberbullying.

This policy applies to all members of staff, including temporary workers, other contractors, volunteers, interns, governors, and any and all third parties authorised to use the IT systems. All staff members are required to familiarise themselves with its contents and comply with the provisions contained in it.

The person responsible for reviewing and implementing this policy is:
Leonardo Amulfi, Principal/CEO, Kindergarten SRL direzione@kindergarten.it

GENERAL PRINCIPLES

Information Security can be defined as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. KINDERGARTEN takes the issue of security seriously and it is dedicated to ensuring the highest standards of information security. **The school is committed to informing and educating the school community (staff, teachers, students) about the positive use of IT facilities**.

RESPONSIBILITIES OF THE IT CONSULTANT AND SCHOOL RESPONSIBLE FOR SAFETY POLICIES

The IT Consultant, appointed by the Principal and in conjunction with the school management, is responsible for the following:

- ensuring that IT Security standards within the School are effectively implemented and regularly reviewed, working in consultation with the School's management, and reporting the outcome of such reviews to the School's management;
- monitoring all IT security within the School and taking all necessary action to implement this policy and any changes made to this policy in the future;
- ensuring that regular backups are taken of all data stored within the IT Systems at regular intervals and that such backups are stored at a suitable location offsite.

The school responsible for safety policies oversees:

- ensuring that all staff members are kept aware of this policy, assisting all staff members in understanding and complying with this policy;

Learn, discover, share

Sedi scuola
Sede centrale: Via S.Gallo 105/Viale Lavagnini 11 - FI
Sede succursale: Viale Matteotti 52 - FI
Sede succursale: Via Lupi 8 - FI

kiwa certified — Certificazione del Sistema di Gestione per la salute e la sicurezza sui luoghi di lavoro secondo la norma OHSAS 18001 (Kiwa Cermet S.p.A. PIANO DI CERTIFICAZIONE N. 11178)

Cambridge Assessment International Education
Cambridge International School

RESPONSIBILITIES – STAFF MEMBERS

The School carries out regular checks of the buildings and storage systems to ensure they are maintained at a high standard. Staff must immediately inform the school management of:

- any security concerns relating to the IT Systems which could or has led to a data breach.
- other technical problems (including, but not limited to, hardware failures and software errors, viruses) which may occur on the IT Systems.

Staff is not entitled to install any software of your own without the approval of the School management.

All staff members are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone else other than those in accordance with this policy.

Only authorized persons may remotely access the Kindergarten IT network.

HOME WORKING

Staff should not take confidential or any other information home without prior permission of the Principal, and only if appropriate technical and practical measures are in place within their home to maintain the security and confidentiality of that information.

USE OF THE INTERNET

The school provides Internet access to staff, teachers, and students for the primary purpose of study, legitimate research, e-mail access, and general internet access.

Kindergarten has put in place firewalls and parental controls in order to prevent access to unsuitable websites.

The use of the Internet to access and/or distribute any kind of offensive material, or material that is not work or study-related, leaves individuals (staff and students) liable to disciplinary action or dismissal.

Internet and IT provision may not be used for:

- transmitting, retrieving, or storing any communications of a discriminatory or harassing nature;
- transmitting, retrieving, or storing any communications which are derogatory to any individual or group;
- obtaining material that would be offensive on the grounds of race, colour, religion, political beliefs, ethnic origin, sexual orientation, gender, age, disability, nationality, marital status;
- engaging in ANY form of cyberbullying;
- searching for obscene, offensive, sexually explicit, or pornographic material;
- obtaining any material to be used in the harassment of another person;
- establishing communications that are defamatory or threatening;

Learn, discover, share

Sedi scuola
Sede centrale: Via S.Gallo 105/Viale Lavagnini 11 - FI
Sede succursale: Viale Matteotti 52 - FI
Sede succursale: Via Lupi 8 - FI

Certificazione del Sistema di Gestione per la salute e la sicurezza sui luoghi di lavoro secondo la norma OHSAS 18001 (Kiwa Cermet S.p.A. PIANO DI CERTIFICAZIONE N. 11178)

Cambridge Assessment
International Education
Cambridge International School

- obtaining material that is unlawful or that infringes on another person's legal rights (e.g. illegal downloads);
- conducting internet searches and looking at websites that can in any way be regarded as extremist, intolerant of other's faiths and beliefs, or that challenge the rule of law and the right to individual liberty.

COMPUTER AND INTERACTIVE WHITEBOARD PASSWORDS

Staff should avoid writing down passwords to remember them. If necessary, staff may write down passwords provided that they store them in a secure manner (e.g. in a locked drawer or in a secure password database). Passwords should never be left on display for others or students to see. Computers and other electronic devices with displays and user input devices (e.g. mouse, keyboard, touchscreen, etc.) shall be protected with a screen lock that will activate after a period of inactivity. Teachers are not allowed to alter the set time period or disable the lock.

MONITORING STUDENTS' USE OF COMPUTER SYSTEMS

The school periodically monitors electronic information created and/or communicated by students using Kindergarten IT systems and networks, including e-mail messages and usage of the Internet.

SOCIAL NETWORKING SITES

Social networking sites can be a great way to connect with friends. But there are some social networking safety tips that students should always keep in mind. Teachers help the students to improve their safety access to social networks.

- DO use the computers for school/study use or to connect with other students in a positive manner.
- DO NOT search for illegal and inappropriate sites or material.
- DO NOT bully anyone through blogs, e-mails, chatrooms, or any other form of internet use
- DO NOT download anything illegally.
- DO NOT upload anything (ex. video, photos, audio recordings, etc.) without explicit permission.
- DO NOT use the internet to give opinions that are extremist, intolerant of other's faiths and beliefs, or that challenge the rule of law and the right to individual liberty.

Any work-related issue or material that could adversely affect KINDERGARTEN, its staff, or its students must not be placed on a social networking site at any time and via any medium.

E-MAIL

Learn, discover, share

Sedi scuola
Sede centrale: Via S.Gallo 105/Viale Lavagnini 11 - FI
Sede succursale: Viale Matteotti 52 - FI
Sede succursale: Via Lupi 8 - FI

Certificazione del Sistema di Gestione per la salute e la sicurezza sui luoghi di lavoro secondo la norma OHSAS 18001 (Kiwa Cermet S.p.A. PIANO DI CERTIFICAZIONE N. 11178)

Cambridge Assessment International Education
Cambridge International School

The use of e-mail is encouraged because, when used appropriately, it facilitates efficient communication. Inappropriate use, however, causes many problems including distractions, time-wasting, and legal claims.

E-mail is available for communication and matters directly concerned with the legitimate business of KINDERGARTEN. Employees using e-mail should give particular attention to the following:

- All e-mails comply with school communication standards;
- E-mail should not be used as a substitute for face-to-face communication or telephone contact. Inflammatory e-mails (i.e. e-mails that are abusive) must not be sent. Hasty messages sent without proper consideration can cause upset, concern, or misunderstanding;
- if an e-mail is considered confidential the user must ensure that the necessary steps are taken to protect confidentiality.
- at KINDERGARTEN, offers or contracts transmitted by e-mail are considered as legally binding as those sent on paper.

KINDERGARTEN will not tolerate the use of e-mail for unofficial or inappropriate purposes, including:

- any messages that could constitute bullying, harassment or other detriments, gambling and pornography;
- personal use (e.g. social invitations, personal messages, jokes, cartoons, chain letters, or other private matters);

PENALTY FOR SECURITY VIOLATION

KINDERGARTEN takes the issue of security seriously. Those who use the technology and information resources of KINDERGARTEN must be aware that they can be disciplined if they violate this policy. Upon violation of this policy, an employee may be subject to discipline up to and including discharge.

Learn, discover, share

Sedi scuola
Sede centrale: Via S.Gallo 105/Viale Lavagnini 11 - FI
Sede succursale: Viale Matteotti 52 - FI
Sede succursale: Via Lupi 8 - FI

Certificazione del Sistema di Gestione per la salute e la sicurezza sui luoghi di lavoro secondo la norma OHSAS 18001 (Kiwa Cermet S.p.A. PIANO DI CERTIFICAZIONE N. 11178)

Cambridge Assessment
International Education
Cambridge International School