LA SCUOLA ITALIANA A LONDRA

CODE OF PRACTICE FOR E-SAFETY

Last reviewed May 2018

INTRODUCTION

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing.

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings.

This Code of Practice is drawn up to protect all parties: the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements. It also highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.
It has been discussed with staff, agreed by the senior management and approved by Governors. It will be reviewed annually.

This Code of Practice is summarised in the Parents' Handbook and in the Staff Handbook and is available in the School Office, on our website: www.scuolaitalianalondra.org and on the Staff Drive.

The school's e-safety Code of Practice should operate in conjunction with other policies including those for Safeguarding and Child Protection, School Behaviour and Discipline, Privacy Policy, Data protection Policy and Bullying and Curriculum.

Created by:
Ines Saltalamacchia (Designated Safeguarding Lead (DSL) and ICT coordinator)

AIMS

- To set out the key principles expected of all members of the school community at SIAL with respect to the use of ICT-based technologies.
- To safeguard and protect the children and staff of SIAL.
- To fulfil the responsibilities imposed by UK and EU laws and regulations in respect to data protection and privacy.
- To assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- To set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- To ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- To minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

SCOPE

- This code of practice applies to the whole school community including SIAL's Senior Leadership Team, school board directors, all staff employed directly or indirectly by the school and all pupils.
- SIAL's Senior Leadership Team and school directors will ensure that any relevant or new legislation that may impact upon the provision for eSafeguarding within school will be reflected within this code of practice.
- The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of students or pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other eSafeguarding-related incidents covered by this code of practice, which may take place out of school, but is linked to membership of the school.

- SIAL will clearly detail its management of incidents within this code of practice, associated behaviour and anti- bullying policies and will, where known, inform parents and carers of incidents of inappropriate eSafeguarding behaviour that takes place out of school.

CONTEXT AND BACKGROUND

The technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New internet and online technologies are enhancing communication and the sharing of information.

Current and emerging Internet and online technologies used in school and, more importantly in many cases, used outside school by children and staff include:

- The Internet – World Wide Web
- e-mail
- Instant messaging (often using simple web cams, e.g. Instant Messenger)
- Web based voice and video calling (e.g. Skype)
- Online chat rooms
- Online discussion forums
- Social networking sites (e.g. Facebook)
- Blogs and Micro-blogs (e.g. Twitter)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Video broadcasting sites (e.g. You Tube)
- Music and video downloading (e.g. iTunes)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, messaging and internet access
- CCTV Recordings

Our whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities
- e-Safety teaching is embedded into the school curriculum and schemes of work

ROLES AND RESPONSABILITIES

e-Safety is recognised as an essential aspect of strategic leadership in this school and the SLT, with the support of Governors, aims to embed safe practices into the culture of the school.

Governors

The School Governing body is responsible for overseeing and reviewing all school policies, including the e-Safety Policy.

Leadership team

- The SLT is ultimately responsible for ensuring the safety (including e-safety) of members of the school community.
- All safeguarding issues will be dealt with following the procedures within this code of practice and the Child Protection and Safeguarding Procedures. (See Safeguarding and Child Protection code of

Practice). The DSLs (*Designated Safeguarding Leads)* are the first point of contact in School, for all safeguarding matters. The DSL is Ines Saltalamacchia, the Deputy DSL is Benjamin Mearhart.

- The SLT ensures that this code of practice is implemented across the school via the usual school monitoring procedures.
- The SLT is responsible for ensuring that all relevant staff receive suitable training to enable them to carry out their eSafeguarding roles.
- The SLT should be aware of procedures to be followed in the event of a serious eSafeguarding incident.

e-Safety Co-ordinator

Our school DSLs (*Designated Safeguarding Leads) are also* e-Safety Co-ordinators. The DSL is Ines Saltalamacchia, the Deputy DSL is Benjamin Mearhart.
The role of the e-Safety Co-ordinator includes:

- To promote an awareness and commitment to eSafeguarding throughout the school
- To take day-to-day responsibility for eSafeguarding within school and to have a leading role in establishing and reviewing the school eSafeguarding policies and procedures
- To ensure all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- To provide training and advice for staff
- To liaise with the Local Authority
- To receive reports of e-safety incidents and creates a log of incidents to inform future e- safety developments
- To ensure that eSafeguarding education is embedded across the curriculum
- The e-Safety Co-ordinator is also responsible for:
- Supporting the school in providing a safe technical infrastructure to support learning and teaching
- Ensuring that users may only access the networks and devices through a properly enforced password protection policy
- Ensuring that provision exists for misuse detection and malicious attack
- Taking responsibility for the security of the school ICT system
- Ensuring that access controls exist to protect personal and sensitive information held on school-owned devices
- Ensuring that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school
- Ensuring that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

School Staff

The role of the school staff includes:

- To have an up to date awareness of e-safety matters and of the current school e-safety code of practice and procedures
- To adhere to the SIAL data protection and privacy policies.
- To read, understand and adhere to the Staff Acceptable Use Agreement
- To report any suspected misuse or problem to the DSL / e-Safety Co-ordinator for investigation / action / sanction
- To model safe and responsible behaviours in their own use of technology
- To ensure that all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- To embed e-safety issues in all aspects of the curriculum and other activities
- To supervise and guide pupils carefully when engaged in learning activities involving technology
- To ensure that pupils understand and follow the e-safety and acceptable use policies

- To ensure that pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- To monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current codes of practice with regard to these devices
- To ensure that in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- To understand and be aware of incident-reporting mechanisms that exist within the school

Pupils

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-Safety code of practice covers their actions out of school, if related to their membership of the school

Parents/Carers

- Parents/Carers are given information about the school's e-safety code of practice
- They are given copies of the School-Pupil Internet Use agreement, and asked to support these rules with their children.

COMMUNICATION

Staff

- The eSafety Code of Practice is provided to and discussed with all members of staff formally
- All amendments will be updated on the system and awareness sessions will be held for all members of the school community
- All members of staff are asked to read and sign the school's Staff Acceptable Use Agreement
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential
- The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

Pupils

- Pupils are asked to read, understand and adhere to the Pupil Acceptable Use Agreement
- e-Safety rules or copies of the Pupil Acceptable Use Agreement are posted in all rooms with Internet access
- An e–Safety module is included in the PSHE and/or ICT programmes covering both safe school and home use
- Pertinent points from the school eSafeguarding code of practice are reinforced across the curriculum and across all subject areas when using ICT equipment within school

- All staff endeavour to embed eSafeguarding messages across the curriculum whenever the internet or related technologies are used
- eSafety is introduced to the pupils during an assembly at least once a year
- Pupils are informed that network and Internet use could be monitored.

Parents/Carers

- Parents/Carers' attention is drawn to the school e–Safety Policy in the Parents' Handbook, school's newsletters and on the school website
- A partnership approach to e-Safety at home and at school with parents/carers is encouraged
- Written permission is obtained from parents/carers to give children access to ICT facilities and equipment and the Internet.
- Parents/Carers are requested to read and sign the Pupil Acceptable Use Agreement and discuss its implications with their children
- Information and guidance for parents/carers on e–Safety is made available to interested parents/carers
- Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet is made available to interested parents/carers

TRAINING

- SLT members and Key-stage Co-ordinators receive e-Safety training on a regular basis (a minimum of two or three years).
- All staff receive regular information and training on eSafeguarding issues in the form of insets and staff meetings.
- As part of the induction process all new staff receive information and guidance on the e-Safeguarding policy and the school's Staff Acceptable Use Agreement.
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of eSafeguarding and know what to do in the event of misuse of technology by any member of the school community.

LEARNING AND TEACHING

Internet use is part of the statutory curriculum and is a necessary tool for learning.
The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
Internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we have a duty to help prepare them to safely benefit from the opportunities the internet brings.
We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education.

Internet access at school

- Internet access is carefully controlled by teachers according to the age and experience of the pupils, and the learning objectives being addressed.
- Pupils are always actively supervised by an adult when using the Internet, and computers with Internet access are carefully located.

Using the Internet for learning

- Teachers carefully plan all Internet-based teaching to ensure that pupils are focussed and using appropriate and relevant materials.
- Pupils are taught how to use a range of age-appropriate online tools in a safe and effective way.
- They are taught how to use search engines and how to evaluate Internet-based information as part of the ICT curriculum, and in other curriculum areas where necessary.

- They are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- They are taught in an age-appropriate way about copyright in relation to online resources and will be taught to understand about ownership and the importance of respecting and acknowledging copyright of materials found on the Internet.

Teaching safe use of the Internet and ICT

We think it is crucial to teach pupils how to use the Internet safely, both at school and at home

- We will provide a series of specific eSafeguarding-related lessons in every year group as part of the PSHE and/or ICT curriculum.
- We will celebrate and promote eSafeguarding through a planned programme of assemblies and whole- school activities.
- We will discuss, remind or raise relevant eSafeguarding messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- We will remind pupils about their responsibilities through a Pupil Acceptable Use Agreement which every pupil will sign
- All pupils will be reminded of what to do if they come across unsuitable content
- Pupils will be taught about the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as the CEOP report abuse button

We use theKidsmart safety code to support our teaching in this area:
Kidsmart has been developed by the Childnet charity, and is endorsed by the DfES
http://www.kidsmart.org.uk
The main aspects of this approach include the following five SMART tips:

- Safe - Staying safe involves being careful and not giving out your name, address, mobile phone no., school name or password to people online...
- Meeting someone you meet in cyberspace can be dangerous. Only do so with your parents'/carers' permission and then when they are present...
- Accepting e-mails or opening files from people you don't really know or trust can get you into trouble - they may contain viruses or nasty messages...
- Remember someone online may be lying and not be who they say they are. If you feel uncomfortable when chatting or messaging end the conversation...
- Tell your parent or carer if someone or something makes you feel uncomfortable or worried...

Suitable material

We encourage pupils to see the Internet as a rich and challenging resource, but we also recognise that it can be difficult to navigate and find useful and appropriate material. Where possible, and particularly with younger children, we provide pupils with suggestions for suitable sites across the curriculum and staff always check the suitability of websites before suggesting them to children, or using them in teaching.

Non-Education materials

We believe it is better to support children in finding their way around the Internet with guidance and positive role modelling rather than restrict Internet use to strict curriculum based research. As well as Internet material directly related to the curriculum, we encourage children to visit appropriate entertainment and child-oriented activity sites that have interesting and relevant activities, games and information.

Unsuitable material

Despite the best efforts of the school staff, occasionally pupils may come cross something on the Internet that they find offensive, unpleasant or distressing. Pupils are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken. The action will include:

1. Making a note of the website and any other websites linked to it.
2. Informing the e-Safety Co-ordinator
3. Logging the incident
4. Discussion with the pupil about the incident, and how to avoid similar experiences in future

MANAGING ICT SYSTEMS AND ACCESS

- SIAL will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible. To this effect all staff is required to use strong authentication process, which will be updated once a term.
- Virus protection is installed on all appropriate hardware, and will be kept active and up to date.
- The use of user logins and passwords to access the school network will be enforced by 2- steps verification.
- Files held on the school's network will be regularly checked.
- Staff are allowed to use their own portable media storage (USB Keys etc.) provided that it does not contain any kind of personal data. If use of such a device result in an anti-virus message they should remove the device and immediately report to the e-Safety Co-ordinator.
- Unapproved software will not be allowed in work areas or attached to email.

FILTERING INTERNET ACCESS

- The Internet is a valuable tool for teaching and learning. Unfortunately, not all content that is available on the Internet is suitable for schools, so provision has to be made to ensure that a suitable, fit-for-purpose Internet filtering solution is deployed.
- The e-Safety Co-ordinator will ensure that regular checks are made to ensure that the filtering methods selected are effective.

EMERGING TECHNOLOGIES

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The acceptable use of any new or emerging technologies in use within school will be reflected within the school's eSafeguarding and Acceptable Use Agreements.
- Prior to deploying any new technologies within school, staff and pupils will have appropriate awareness training regarding safe usage and any associated risks.

MANAGING DIGITAL CONTENT

Thought needs to be given whenever images, video and sound, including the use of school-generated assets and those found on the internet, are used in school. In order to ensure compliance with GDPRS regulations and to respect privacy, we need to be careful when sharing these images, videos and sounds online. In addition, pupils should be taught to think about how they share images, video and sound online in their personal lives.

- Written permission from parents or carers will be obtained for the following locations before photographs of pupils are published. Parents and carers may withdraw permission, in writing, at any time.
    - On the school website

- In the school prospectus and other printed promotional material
- In display material that may be used around the school
- Recorded or transmitted on a video or via webcam in an educational conference

- We will remind pupils of safe and responsible behaviour when creating, using and storing digital images, video and sound.
- We will remind pupils of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.
- Pupils and staff will only use school equipment to create digital images, video and sound. In exceptional circumstances, personal equipment may be used with permission from the senior management team provided that any media is transferred solely to a school device and deleted from any personal devices.
- In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file name or in accompanying text online; such resources will not be published online without the permission of the staff and pupils involved.
- If pupils are involved, relevant parental permission will also be sought before resources are published online.
- Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites.
- When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

Storage of images

- Any images, videos or sound clips of pupils must be stored on the school server protected by appropriate passwords and never transferred to personally owned equipment.
- Pupils and staff are not permitted to use personal portable media for storage of any images, videos or sound clips of pupils.

DATA PROTECTION

Personal data will be recorded, processed, stored, transferred and made available according to the General Data Protection Regulation and our Data protection and Privacy Code of Practice.

E-MAIL

E-Mail is a valuable and stimulating method however there are responsibilities involved in using the e-mail facilities of communication that plays an important role in many aspects of our lives today. By activating a school account, users are agreeing to fulfil the responsibilities imposed by the school regulations and recognising that they are subject to UK, EU and other relevant laws.

This document explains more fully how these considerations govern the use of e-mail.

Pupils

- We believe it is important that our pupils understand the role of e-mail, and how to use it appropriately and effectively
- We teach the use of e-mail as part of our ICT curriculum, including:
  - dangers of revealing personal information within email conversations.
  - not revealing personal details of themselves or others in email communications. Pupils should get prior permission from an adult if they arrange to meet with anyone through an email conversation.

- dangers of opening email from an unknown sender or source or viewing and opening attachments.
- dangers of opening attachments from an untrusted source

- Pupils are not allowed to access personal e-mail using school Internet facilities

Staff (including Governors)

- Staff members will be given a school e-mail address and we ask staff to use it for all professional communication with colleagues, organisations, companies and other groups. Staff should bear in mind that e-mail messages can be very easily read by those for whom they were not intended and they should recognise particularly that e-mails can be:
  - intercepted by third parties (legally or otherwise)
  - accessed by any individuals mentioned in the e-mails, under data protection legislation
  - wrongly addressed
  - forwarded accidentally
  - forwarded by initial recipients to third parties against your wishes
  - viewed accidentally on recipients' computer screens
- Staff should not forward e-mails relating to SIAL business to personal non-SIAL e-mail accounts (such as gmail or hotmail) particularly where these communications include personal data relating to others.
- Sensitive personal data should not be communicated by e-mail unless the express permission of the subject has been obtained or unless adequate encryption facilities have been employed.
- Staff should never use a false identity in e-mails.
- The SIAL's e-mail system must not be used to create or distribute unsolicited, offensive, or unwanted e-mail, including the dissemination of chain letters. The sending of unsolicited marketing messages is a criminal offence.
- Staff should exercise caution when downloading material from the internet and opening e-mail attachments if there is any suspicion of it including a virus. If they have any suspicions, they should not open an attachment and contact the ICT Coordinator immediately.
- Staff are encouraged to familiarise themselves with advice on phishing provided by the school.
- Staff are reminded that using this e-mail address means that they are representing the school, and all communications must reflect this.
- E-mail accounts provided by the school may sometimes need to be accessed, although personal privacy will be respected.
- Any inappropriate use of the school email system or receipt of any inappropriate messages from another user should be reported immediately.
- Staff e-mail addresses are to be used primarily for the conduct of SIAL business. Use of the SIAL e-mail accounts for personal purposes is acceptable provided that it does not interfere with work and is fully compliant with these guidelines and other relevant SIAL regulations.

Staff e-mails and data protection

As a member SIAL staff are subject to General Data Protection Regulation 2018. These prescribe a number of further rights and responsibilities in using e-mail:

- Personal data is subject to this legislation. Under its terms, personal data includes any information about a living identifiable individual, including their name, address, phone number, and e-mail address. If such information is included in an e-mail or an attachment to an e-mail, staff would be deemed to be "processing" personal data and must abide by the legislation. Personal information also includes any expression of opinion.
- Staff should be cautious about putting personal information in an e-mail. In particular, staff should not collect such information without the individual knowing they propose to do this; they may not disclose or amend such information except in accordance with the purpose for which the information was collected; and they should ensure the information is accurate and up to date.

They should not use e-mail for any purpose that is not permitted under SIALs Data Protection Policy.

- SIAL has, by law, to provide any personal information held about any data subject who requests it under data protection legislation. This includes information on individual computers in departments, and staff have a responsibility to comply with any instruction to release such data made by SIAL data protection officer. Emails which contain personal information and are held in live, archive or back-up systems or have been "deleted" from the live systems, but are still capable of recovery, may be accessible by data subjects.
- The law also imposes rules on staff in retaining personal data. Such data should be kept only for as long as it is needed for the purpose for which it was collected. SIAL retain deleted e-mails (for thirty days) to allow for accidental loss or any other later requirement by the user for it to be retrieved.
- Staff should take care when sending e-mails containing personal information to countries outside the European Economic Area, especially if those countries do not have equivalent levels of protection for personal data.

MOBILE PHONES AND PERSONAL DEVICES

More and more young people have access to sophisticated new internet-enabled devices such as SMART mobile phones, tablets and music players.

It is important that whilst the school recognises the potential advantages these devices can offer, there are clear and enforceable rules for their use in school, particularly when they give access to the Internet, and allow pictures and information to be remotely posted to a website or weblog.

Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

<u>No images or videos should be taken on mobile phones or personal devices.</u>

Pupils' use

- Pupils are not allowed to have personal mobile phones or other similar devices in school. Parents may request that such devices are kept at the School Office for pupils who may need them on their journey to and from school.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office, to only be released to the pupil's parent or carer.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone

Staff use

- Mobile phones and personal devices will not be used during lessons or formal school time, unless in emergency circumstances.
- Personal mobile phones or devices are permitted only during school trips as emergency contact.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff are not to permit children to use their mobile phone as part of an educational activity.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use school provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

CHAT, DISCUSSION AND SOCIAL NEWORKING SITES

These forms of electronic communication are used more and more, and can also contribute to learning across a range of curriculum areas.

Online chat rooms, discussion forums and social networking sites present a range of personal safety and privacy issues for young people.

- Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the site's terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the e-Safety co-ordinator before using Social Media tools in the classroom. Individual pupil names or identifying information will never be used.
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupils will be encouraged to approve and invite only known friends on social networking sites and to deny access to others by making profiles private.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Agreement.

DELIBERATE MISUSE OF THE INTERNET FACILITIES

SIAL has to act within the law, which means it has, in turn, to ensure that its pupils and its staff are doing so, by enforcing the Rules and Regulations as explained in this Policy. Therefore, any breach of these Rules will be treated by SIAL as a serious disciplinary matter. If the breach or misuse results in a data breach SIAL commits to reporting any such breach to the ICO (Information Commissioners Office) and notifying appropriately data subject and data controllers without undue delay.

Pupils
All pupils have discussed the rules for using the Internet safely and appropriately. These rules should be displayed in each classroom.

Where a pupil is found to be using the Internet inappropriately, for example to download games, or search for unsuitable images, then sanctions will be applied according to the nature of the misuse, and any previous misuse.

Sanctions will include:

Unsuitable material (e.g. online games, celebrity pictures, music downloads, sport websites etc)
- Initial warning from class teacher
- Report to SLT
- Letter to parent/carer

Offensive material (e.g. pornographic images, racist, sexist or hate website or images etc)
- Incident logged and reported to the SLT

- Initial letter to parent/carer
- Meeting with Parent/Carer to re-sign Internet use agreement
- Subsequent incidents will be treated very seriously by the SLT, and may result in exclusion and/or police involvement.

HOW WILL COMPLAINTS REGARDING E-SAFETY BE HANDLED?

The school will take all reasonable precautions to ensure that users access only appropriate material.
Methods to identify, assess and minimise risks will be reviewed regularly.
However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer.
Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions.
Sanctions available include:

- All incidents will be recorded
- Interview/counselling by class teacher, e-Safety Coordinator, SLT
- Informing parents or carers
- Removal of Internet or computer access for a period
- Referral to LA / Police.

Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Heads.

CYBERBULLYING - Online bullying and harassment

By cyber-bullying, we mean bullying by electronic media. It is an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend him/herself.

Cyberbullying is insidious; it can be conducted 24 hours a day, seven days a week, following children into their private space and outside school hours. It can be anonymous. The audience is large and can be reached rapidly. Unlike other forms of bullying, a single incident can be experienced as a multiple attack – a video posted to a website can be copied to many different sites. Bystanders can become accessories by passing on a humiliating message. Messages on social networking sites remain there to damage social life and friendships.

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated.

SIAL educates its pupils both in the proper use of telecommunications and about the serious consequences of cyber-bullying through PSHE and in ICT lessons and assemblies.

We encourage pupils to discuss any concerns or worries they have about online bullying and harassment with staff.

- Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy.
- Complaints related to child protection are dealt with in accordance with school child protection procedures.

e-SAFETY – STAFF ACCEPTABLE USE AGREEMENT FORM

Introduction

The use of the latest technology is actively encouraged at SIAL. With this comes a responsibility to protect users and the school from abuse of the system.
This document has been developed to ensure that all staff within our school are aware of their professional responsibilities when using ICT equipment and systems. All staff should follow the guidelines at all times. You are responsible for your behaviour and actions when carrying out any activity, which involves using ICT equipment and information systems, either within school, or at other locations, such as home.
The following guidelines are general in nature as not every possible scenario can be thoroughly described or known at this point in time.

When using the school's ICT equipment, I have understood and will comply with the following statements:

- I will obtain the appropriate log on details and passwords from the e-Safety Co-ordinator.
- I will seek consent from the e-Safety Co-ordinator prior to the use of any new technologies (hardware, software, cloud-based services) within school.
- I will not allow unauthorised individuals to access school ICT systems or resources
- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Heads and Governing Body
- I will not search for, download, upload or forward any content that is illegal or that could be considered an offence by another user. If I encounter any such material I will report it immediately to the e-Safety Co-ordinator.
- I will take a professional and proactive approach to assessing the effectiveness of the Internet content-filtering platform in relation to the educational content that can be viewed by the pupils in my care. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the e-Safety Co-ordinator.
- I understand my personal responsibilities in relation to data protection and privacy and disclosure of personal and sensitive confidential information.
- I will take reasonable precautions to ensure that any devices (laptops, tablets, cameras, removable media or phones) are turned off and stored in a secure manner at the end of the day (lockable cupboard or staff room)
- I will secure any equipment taken off site for school trips.
- I will ensure that I will not take off site and store on personal devices any personal or sensitive data.
- I will not download or install any software from the Internet or from any other media, which may compromise the school network or information situated on it without prior authorisation from the e-Safety Co-ordinator.
- I understand that the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be

reported to the appropriate authorities.

- I understand that my files, communications and internet activity may be monitored and checked at all times to protect my own and others' safety, and action may be taken if deemed necessary to safeguard me or others.
- I understand that if I do not follow all statements in this e-Safety Agreement and in other school policies relating to the use of ICT equipment I may be subject to disciplinary action in line with the schools established disciplinary procedures.

Social Media

The Internet provides a range of social media tools that allow us to interact with one another.
We understand that everyone has the right to a private life and SIAL respects this provided we follow the guidelines set out in our policies.
SIAL expects staff to maintain reasonable standards in their own behaviour, such that enables them to maintain an effective learning environment and also to uphold public trust and confidence in them and their profession.
Employees should avoid any conduct which is likely to bring the school into disrepute.

I have understood and will comply with the following statements:

- I must not talk about my professional role in any capacity when using personal social media such as Facebook, Twitter and YouTube or any other online publishing websites.
- I must not use social media tools to communicate with current or former pupils under the age of 18.
- I will not use any social media tools to communicate with parents unless approved in writing by the SLT.
- I will set and maintain my profile on social networking sites to maximum privacy and give access to known friends only.
- I must not access social networking sites for personal use during school hours.
- If I experience any derogatory or slanderous comments relating to the school, colleagues or my professional status, I will take screenshots for evidence and escalate to SLT.

Managing Digital Content

One has to be careful whenever images, video and sound are used in school. In order to protect our pupils, we need to think about how we will share images, video and sound online, e.g. on the school website. In addition, pupils should be taught to think about how they share images, video and sound online in their personal lives.
To protect ourselves, we need to think about how we will take, use and store these digital resources.

I have understood and will comply with the following statements:

- I will demonstrate professional, safe and responsible behaviour when creating, using and storing digital images, video and sound within school.
- I will only use school equipment to create digital images, video and sound. Digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress. No resources will be published online without the permission of the staff and pupils involved as detailed in the eSafeguarding code of practice / e-Safety Agreement (or any other relevant policy).
- Under no circumstances will I use any personally owned equipment for video, sound or images without prior consent from the designated member of staff (member of SLT).
- I will ensure that any images, videos or sound clips of pupils are stored on school-owned pcs/devices and never transferred to personally owned equipment.

- I will ensure that any images taken on school-owned devices will be transferred to the school pcs and immediately deleted from the memory card.
- I will model safe and responsible behaviour in the creation and publishing of online content within the school learning platform and any other websites. In addition to this I will encourage colleagues and pupils to adopt similar safe behaviour in their personal use of blogs, wikis and online publishing sites.

Learning and Teaching

I have understood and will comply with the following statements:

- I will support and promote the school eSafeguarding policy at all times. I will model safe and responsible behaviour in pupils when using ICT to support learning and teaching.
- I will ensure that I am aware of my individual responsibilities relating to the safeguarding of children within the context of eSafeguarding and know what to do in the event of misuse of technology by any member of the school community.
- I understand the importance of respecting and acknowledging copyright of materials found on the internet and will model best practice in the creation of my own resources at all times.

Email

Email is an essential communication mechanism for both staff and pupils in today's digitally-connected world. The use of email can bring significant educational benefits for any school, both for its staff and pupils. However, email use for staff and pupils needs to be thought through and appropriate safety measures put in place. The unregulated use of email could potentially lead to a safeguarding incident as the more traditional, non-technical access controls can be bypassed with ease.
School email should in no way be considered private and its use should be for all school-related communication.
A school email account is provided for staff to communicate with other teaching professionals, or any school-related third party only for official school business.

I have understood and will comply with the following statements:

- I will use only my school email address for all correspondence with staff or other agencies and I understand that any use of the school email system will be monitored and checked.
- I will not share neither my school email address nor my personal email address with any pupil in the school.
- I understand that all communication between staff and members of the wider school community should be professional and related to school matters only.
- I will ensure that any posts made on websites or via electronic communication, by either myself or the pupils in my care, will not damage the reputation of my school.
- I will take care in opening any attachments sent by email. I will only open emails and associated attachments from trusted senders.
- I understand that emails sent to external organisations will be written carefully before sending to protect myself. As and when I feel it necessary, I will carbon copy (cc) a member of the SLT or another suitable member of staff into the email.
- I will ensure that I manage my email account, delete unwanted emails and file those I need to keep in folders.
- I will access my school email account on a regular basis to ensure that I respond in a timely manner to communications that require my attention.
- I will not forward e-mails relating to SIAL business to personal non-SIAL e-mail accounts (such as gmail or hotmail) particularly where these communications include personal data relating to others.

- I will not share sensitive personal data by e-mail unless the express permission of the subject has been obtained or unless adequate encryption facilities have been employed.
- I will never use a false identity in e-mails.

Mobile Phones and Devices

In today's digital world, communications and content are available almost anywhere at any time.
As mobile phones have increased in sophistication, with the functionality being almost parallel to that of school-based desktop and laptop computers, more care has to be taken with the usage of mobile smart type devices within school.
Mobile phones with integrated cameras could lead to child protection, bullying and data protection issues with regards to inappropriate capture, use or distribution of images of pupils or staff.

I have understood and will comply with the following statements:

- I will ensure that my mobile phone and any other personally owned device is switched off or switched to 'silent' mode during school hours.
- I will ensure that my Bluetooth communication is 'hidden' or switched off and my mobile phone or device will not be used during teaching periods unless a member of the SLT in emergency circumstances has granted permission.
- I will not contact any parents or pupils on my personally owned device.
- I will not use any personally owned mobile device to take images, video or sound recordings.

Data protection and information security

Schools hold lots of information and data on pupils, families and on staff. The amount of information which schools hold is increasing all the time and, while this data can be very useful in improving the service which a school provides, the school has a duty of care for how it handles and controls access to the sensitive and personal information and data which it holds.
The handling of secured data is everyone's responsibility, whether they are an employee, volunteer, technical support or third party provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even provoke legal action.

I have understood and will comply with the following statements:

- I will abide by the school Data Protection and Privacy Code of Practice.
- I will not leave personal and sensitive printed documents on printers within public areas of the school.
- All access to personal or sensitive information owned by the school will be controlled appropriately through technical and non-technical access controls.
- I will log off any computers that I have used to access sensitive information.
- I will be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.
- I will only access information systems via a suitably complex password.

I have read and understood the implications and my personal responsibilities in relation to the use of ICT equipment, which is detailed within this code of practice.

Staff name _____

Signed _____

Date _____

e-SAFETY – PUPIL ACCEPTABLE USE AGREEMENT FORM

Introduction

This document has been developed to help you understand the rules of using computers in school. You should always follow the rules set out in this document because these rules will help keep you and your classmates safe.

When using the school's ICT equipment, I have understood and will comply with the following statements:

- I will ask permission before using any ICT equipment (e.g. computers, digital cameras, etc.) and only use it when a teacher or another adult is with me.
- I will only use the user name and password provided by the school to access the school network.
- I will only use the school's computers for schoolwork or homework.
- I will not deliberately waste resources, particularly printer paper and toner.
- I will make sure I take care of any school-owned ICT equipment that I use.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I see anything like this I will tell my teacher immediately.
- I will only delete my own files, and I will not look at other people's files without their permission.
- I will only use memory sticks with permission from my teacher.
- I will not upgrade or install any software on school computers.
- I will return any school-owned ICT equipment to my teacher when I have finished using it.
- I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my safety.
- I will not damage any school-owned ICT equipment.
- I will not eat or drink while using school-owned ICT equipment.

Using the Internet

- I will ask permission before using the Internet, and only use it when a member of staff is present.
- I will only use the user name and password provided by the school to access the internet.
- I will not try to access any websites that the school has blocked access to.
- I will not download anything (files, images, etc.) from the Internet unless given permission
- I will not play games, visit chat rooms, access social networking sites or watch entertaining videos during the school day, unless associated with a class and I have permission from my teacher.
- I will not use the Internet to view, download, send or print materials which are unlawful, obscene or abusive.
- I will always respect the work and ownership rights of people inside and outside of the school. This includes abiding by copyright laws on music, videos, software and intellectual materials.
- If I see anything that makes me uncomfortable, I will immediately tell my teacher.

Social Media

- I know that some websites and social networks have age restrictions and I should not use them

unless I am old enough.

- I will not say nasty or hurtful things about any one online.
- I will not give away any of my personal details (full name, age, date of birth, sex, address etc.) or the personal details of other users in school, over the Internet. This includes photographs or video images of me, other pupils or members of staff.
- I will never arrange to meet anyone I have only met online unless a trusted adult is with me.
- If I see any hurtful comments I will report it to my teacher.

Digital Content

- I will only use school-owned equipment to create pictures, video and sound. Pictures, video and sound will not be taken without asking permission first.
- I will not publish anything online, e.g. images or pictures, without asking my teacher.

Email

- I will only use approved email account provided for me by the school to send email as part of my learning. I will not use personal email accounts at school.
- I will only send email to contact people I know or those agreed by my teacher or parent/carer.
- I will take care in opening any attachments sent by email. I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- When sending emails I will make sure that they are polite and sensible.
- If I receive a message I do not like, I will not respond to it but I will immediately tell my teacher.
- Mobile Phones and Devices
- I will only bring my mobile phone or other devices to school with permission from my parent and will always hand it in at School Office.
- I will never use mobile phones and mobile devices (e.g. Nintendo DS) during the school day.
- I will only take pictures at school using school-owned cameras.
- I will not store any picture or videos on my personal device.

Agreement

I have read and discussed this agreement with my parents.
I have read and know what the rules in this document mean to me and I agree to follow these rules. I know that if I break any of these rules my parent/carer may be told and I may be banned from using computers in school for a period of time.

Pupil name _____

Pupil signature _____

Parent/Carer's signature_____

Date _____

LA SCUOLA ITALIANA A LONDRA
Bilingual Italian and English School with Nursery
154-156 Holland Park Avenue LONDON W11 4UH tel.02076035353

CONSENT FORM for ICT - PHOTOS/VIDEOS

Child's full name: ……

Internet and ICT:

As the parent or legal guardian of the pupil(s) named above, I grant permission for the school to give my child access to:

- the Internet at school
- the school's chosen email system
- ICT facilities and equipment at the school. ☐

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. ☐

I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there are concerns about my child's e-safety or e-behaviour they will contact me. ☐

I will not share online, photographs of other children (or staff) at school events without permission. ☐

Use of digital images, photography and video:

I understand the school has a clear policy on "The use of digital images and video" and I support this. ☐

I understand that the school will necessarily use photographs of my child or include them in video material to support learning activities. ☐

I accept that the school may use photographs / video that include my child in the school prospectus and other printed promotional material that promotes the work of the school ☐

I accept that the school may use photographs / video that include my child on the school website ☐

I accept that the school may use photographs / video that include my child recorded or transmitted on a video or via webcam in an educational conference ☐

I will not take and then share online, photographs of other children (or staff) at school events without permission. ☐

Social networking and media sites:

I understand that the school has a clear policy on "The use of social networking and media sites" and I support this. ☐

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour. ☐

I will support the school by promoting safe use of the Internet and digital technology at home. I will inform the school if I have any concerns. ☐

NAME IN FULL ……

SIGNATURE …… DATE ……