Meridian International School s.r.o.

– E-Safety Policy –

KINDERGARTEN & PRE-SCHOOL
(YEAR ONE)

Review Date: 1st September (2017)

Next Review Date: 20th August (2018)

Approved by: Mr. Ahmet Gursoy (School Director)

Signature: _____

Important E-Safety & Incident Contact Information

Name	Responsibility	Contact
Mr. Ahmet Gursoy (School Director)	Safeguarding Lead	**Telephone:** +420 775 137 777 **Email:** ahmet.gursoy@meridianedu.cz
Mr. Michal Hajek (Head of School – All Sections)	Safeguarding Lead	**Telephone:** +420 777 633 474 **Email:** mhajek@meridianedu.cz
Mr. Daniel Flynn (I.T. Teacher: Secondary/High School)	E-Safety Officer	**Telephone:** +420 773 774 076 **Email:** daniel.flynn@meridianedu.cz
Mr. Erdal Ozyurt (I.T. Teacher: Pre-School/Primary School)	Deputy E-Safety Officer & I.T. Technical Support	**Telephone:** +420 777 146 056 Email: erdal.oyzurt@meridianedu.cz
Mr. Richard Jackson (Deputy Head of School – All Sections)	Deputy Safeguarding Lead	**Telephone:** +420 774 507 577 **Email:** richard.jackson@meridianedu.cz

PLEASE REFER TO PAGE 13 FOR THE E-SAFETY INCIDENT LOG. THIS IS THE APPROPRAITE FORM TO COMPLETE IF ANYONE – STAFF, PARENT OR GUARDIAN – HAS A CONCERN ABOUT AN INDIVIUAL CHILD IN REGARD TO E-SAFETY. THE FORM MUST BE COMPLETED AND RETURNED TO THE APPROPRAITE INDIVIDUAL.

Important Child & General Safety Contact Information

Name	Contact Number
Police Department	158
Fire Department	150
Ambulance	155
International Aid Communication in Foreign Languages	112
Prague City Police	156
Department of Social and Legal Protection of Children	+ 420 222 805 244
Educational Psychologist (Prague 8)	+ 420 286 882 368
Canadian Medical Centre Child Psychiatrist	+420 235 360 133

Contents: E-Safety Policy

Meridian International School

− KINDERGARTEN & PRE-SCHOOL (YEAR 1) −

1. Policy Statement

For clarity, the e-safety policy uses the following terms unless otherwise stated:

Users - refers to staff, School Director, school volunteers, students and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, boarding house, school trips etc.

Wider school community – students, all staff, School Director, parents.

Safeguarding is a serious matter; at Meridian International School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the Meridian International School, Prague, website. Upon review, all members of staff will sign as read and understood both the e-safety policy and the Staff Acceptable Use Policy. A copy of this policy and the Students Acceptable Use Policy will be sent home with students at the beginning of each school year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet.

2. Policy Governance (Roles & Responsibilities)

2.1 Administration

The Meridian International School administration is responsible and accountable for ensuring that our school has effective policies and procedures in place; as such they will:

1) Review this policy at least annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e- safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

2) Designate the overall responsibility for the governance of e-safety at the school who will:

- Keep up to date with emerging risks and threats through technology use.

- Receive regular updates from the Head of School in regards to training, identified risks and any incidents.

- Chair the e-Safety Committee.

2.2   Head of School

The Head of School has overall responsibility for e-safety within Meridian International School. The day-to-day management of this will be delegated to a member of staff, the e-Safety officers (Mr. Daniel Flynn), as indicated below.

The Head of School will ensure that:

- E-Safety training throughout the school is planned and up-to-date and appropriate to the recipient, i.e. students, all staff, senior leadership team and administration, parents.

- The designated e-Safety Officer has had appropriate professional training to undertake the day-to-day duties.

- All e-safety incidents are dealt with promptly and appropriately.

2.3   E-Safety Officer

The day-to-day duty of e-Safety Officer is devolved to Mr. Daniel Flynn.

The e-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarize him/herself with the latest research and available resources for school and home use.

- Review this policy regularly and bring any matters to the attention of the Head of School.

- Advise the Head of School, School Director on all e-safety matters.

- Engage with parents and the school community on e-safety matters at school and/or at home.

- Liaise with the local authority, IT technical support and other agencies as required.

- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.

- Ensure any technical e-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.

- Make him/herself aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Head of School and responsible governor to decide on what reports may be appropriate for viewing.

2.3   ICT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:

  - Anti-virus is fit-for-purpose, up to date and applied to all capable devices. Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.

  - Any e-safety technical solutions such as Internet filtering are operating correctly. Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer and Head of School.

  - Passwords are applied correctly to all users regardless of age - 1 yearly password change per year. Passwords for staff will be a minimum of 8 characters. We consider age-appropriate passwords for students.

  - The IT System Administrator password is to be changed on a monthly (30 day) basis.

2.4   All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Head of School.

- Any e-safety incident is reported to the e-Safety Officer (and an e-Safety Incident report is made), or in his/her absence to the Head of School. If you are unsure the matter is to be raised with the e-Safety Officer or the Head of School to make a decision.

- The reporting flowcharts contained within this e-safety policy are fully understood.

2.5   All Students

The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

E-Safety is embedded in our curriculum; students will be given the appropriate advice and guidance by staff. Similarly, all students will be fully aware how they can report areas of concern whilst at school or outside of school.

2.5   Parents & Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parent's evenings, school newsletters the school will keep parents up to date with new and emerging e-safety risks and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student Acceptable Use Policy before any access can be granted to school ICT equipment or services.

2.6   E-Safety Committee

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parent's evenings, school newsletters the school will keep parents up to date with new and emerging e-safety risks and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student Acceptable Use Policy before any access can be granted to school ICT equipment or services.

3.   Technology

Meridian International School uses a range of devices including PCs and laptops, as well as the student's own personal devices (Apple Macs, tablets & mobile smart-phones). In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

3.1   Internet Filtering

At Meridian International School we use **Smooth Wall** software that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The ICT Coordinator, e-Safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Head of School.

3.2   Email Filtering

We use **1 and 1 Premium Filtering Solution** that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

3.3   Encryption

All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted using **AES Crypt**. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB key drives) is to be brought to the attention of the Head of School immediately. The Head of School will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.

3.4   Passwords

All staff and students will be unable to access any device without a unique username and password. Staff and student passwords will change on a termly basis or if there has been a compromise, whichever is sooner. The ICT Coordinator and IT Support will be responsible for ensuring that passwords are changed. School tablets are password free however have controlled apps and settings to prevent misuse of the device and its Internet connection is filtered via the school Internet Filtering System.

3.5   Anti-Virus

All capable devices will have anti-virus software called **AVG and AVAST**. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out and will report to the Head of School if there are any concerns. All USB peripherals such as key drives (if you allow them) are to be scanned for viruses before use.

4.   Safe Use

4.1   Internet

Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this e-safety and the staff Acceptable Use Policy; students upon signing and returning their acceptance of the Acceptable Use Policy.

4.2 E-Mail

All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

4.3 Photos and Videos

Digital media such as photos and videos are covered in this policy. All parents must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance.

4.4 Social Networking

There are many social networking services available; Meridian International School is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within Meridian International School and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the e-Safety Officer who will advise the Head of School for a decision to be made. Any new service will be risk assessed before use is permitted.

- Blogging – if used by staff and students in school.
- Twitter – if used by the school as a broadcast service (see below).
- Facebook – if used by the school as a broadcast service (see below).

A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be "followed" or "friended" on these services and as such no two-way communication will take place.

In addition, the following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a license which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

4.5   Incidents

Any e-safety incident is to be brought to the immediate attention of the e-Safety Officer, or in his/her absence the Head of School. The e-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

4.6   Training and Curriculum

It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Meridian International School will have an annual programme of training which is suitable to the audience.

E-Safety for students is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

The e-Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Head of School and responsible Teacher for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Head of School for further CPD.

5. Acceptable Use Policy (Staff)

Note: All Internet and email activity is subject to monitoring

You must read this policy in conjunction with the e-Safety Policy. Once you have read and understood both you must sign this policy sheet.

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-safety incident, reported to the e-safety officer and an incident sheet completed.

Social networking – is not allowed in school in accordance with the e-safety policy. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become "friends" with parents or pupils on personal social networks. Only authorized staff will have access to social networking for the sole purpose of school communication with the local community.

Use of Email – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or student, or IT support.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that your device (laptop, USB pen drive etc.) is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Head of School who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of Personal ICT - use of personal ICT equipment is at the discretion of the Head of School. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by IT support and the e-Safety Officer.

Viruses and other malware - any virus outbreaks are to be reported to the e-safety officer as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

e-Safety – like health and safety, e-safety is the responsibility of everyone to everyone. As such you will promote positive e-safety messages in all use of ICT whether you are with other members of staff or with students.

NAME: _____

SIGNATURE: _____   **DATE:** _____

6. Acceptable Use Policy (Students)

Note: All Internet and email activity is subject to monitoring

I Promise – to only use the school ICT for schoolwork that the teacher has asked me to do.

I Promise – not to look for or show other people things that may be upsetting.

I Promise – to show respect for the work that other people have done.

I will not – use a tablet/digital device for non-educational purposes.

I will not – use other people's work or pictures without permission to do so.

I will not – use the Internet to play games, search or visit inappropriate sites.

I will not – damage the ICT equipment, if I accidentally damage something I will tell my teacher.

I will not – share my password with anybody. If I forget my password I will let my teacher know.

I will not – use other people's usernames or passwords.

I will not – share personal information online with anyone.

I will not – download anything from the Internet unless my teacher has asked me to.

I will – let my teacher know if anybody asks me for personal information.

I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will – be respectful to everybody online; I will treat everybody the way that I want to be treated.

I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.

I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

Parent Name:_____

Signed (Parent):   _____

Student Name: _____

Signed (Student):   _____

Date: _____

7. E-Safety Incident Log

Date:	Reported By:	Reported To:
	When:	Where:

Incident Description: (Describe what happened, involving which children and/or staff, and what actions was taken)		

Review Date:	

Result of Review:	

Signature (Head of School)	Date:

Signature (E-Safety Officer)	Date:

8. Risk Log

Below are some examples of possible risks, likelihood and impact of score of a given risk.

No.	Activity	Risk	Likelihood	Impact	Score	Owner
1	Internet browsing	Access to inappropriate/illegal content – staff	1	3	3	E- Safety Officer IT Support
1	Internet browsing	Access to inappropriate/illegal content – students	2	3	6	
2	Blogging	Inappropriate comments	2	1	2	
2	Blogging	Using copyright material	2	2	4	
3	Student laptops	Students taking laptops home – access to inappropriate/illegal content at home	3	3	9	

Likelihood: How likely is it that the risk could happen (foreseeability).

Impact: What would be the impact to the school (e.g. this could be in terms of legality, reputation, complaints from parents, reporting in press etc.).

Likelihood and Impact are between 1 and 3, 1 being the lowest.

Multiply Likelihood and Impact to achieve score.

LEGEND/SCORE:

1 – 3 = Low Risk

4 – 6 = Medium Risk

7 – 9 = High Risk

Owner: The person who will action the risk assessment and recommend the mitigation to Head of School and School Director. Final decision rests with Head of School and School Director.

9.   Risk Assessment

Risk No.	Risk
3	In certain circumstances, students will be able to borrow school-owned laptops to study at home. Parents may not have internet filtering applied through ISP. Even if they do there is no way of checking the effectiveness of this filtering; students will potentially have unrestricted access to inappropriate/illegal websites/services.
Likelihood 3	The inquisitive nature of children and young people is that they may actively seek out unsavoury online content, or come across such content accidentally. Therefore, the likelihood is assessed as 3.
Impact 3	The impact to the school reputation would be high. Furthermore, the school may be held vicariously liable if a student accesses illegal material using school-owned equipment. From a safeguarding perspective, there is a potentially damaging aspect to the student.
Risk Assessment	HIGH (9)
Risk Owner/s	e-Safety Officer and IT Support
Mitigation	This risk should be actioned from both a technical and educational aspect: Technical: Laptop is to be locked down using Smooth Wall software. This will mean that any Internet activity will be directed through the school Internet filter (using the home connection) rather than straight out to the Internet. The outcome is that the student will receive the same level of Internet filtering at home as he/she gets whilst in school. Education: The e-Safety Policy and Acceptable Use Policy will be updated to reflect the technical mitigation. Both the student and the parent will be spoken to directly about the appropriate use of the Internet. Parents will be made aware that the laptop is for the use of his/her child only, and for school work only. The current school e- safety education programme has already covered the safe and appropriate use of technology, students are up to date and aware of the risks.

10.   Inappropriate & Illegal Activity Flowchart

A Concern is Raised

Who is Involved?

Member of Staff

Pupil

Child Protection Issue?

Child Protection Issue?

NO

YES

NO

YES

Report to:

Head of School

Report to:

School Director & Safeguarding Lead

Consider:

Inform parents
Risk Assess
Counselling
Discipline
Referral

Report to:

School Director and Safeguarding Lead

Consider:

Risk Assess
Counselling
Discipline
Referral

Report to:

Police - 158

Praha 8 Social Workers -

+ 420 222 805 244

Report to:

Police - 158

Praha 8 Social Workers -

+ 420 222 805 244