Whole School E-Safety Policy

03.018

Standardized Cover Page of Internal policy

Author/ *Autor*: Iain Murray
Superiors name / *Jméno nadřízeného*: Tim Roberts
Approval date / *Datum schválení*: 29th May 2015
Policy/ *Vnitřní předpis je*: Public/Veřejná
Archive number / *Archivační číslo*: 150529_03.018

Whole School E-Safety Policy

Content:

Policy Statement

For clarity, the E-Safety Policy uses the following terms unless otherwise stated:

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

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, school trips etc.

Wider school community – students, all staff and school board.

Safeguarding is a serious matter; at PBS 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.

Policy Governance (Roles & Responsibilities)

School Board

The school board is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- 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.

- The E-Safety officer will:
  - Keep the board up to date with emerging risks and threats through technology use.
  - Keep the board updated with regards to training, identified risks and any incidents.

Heads

Reporting to the school board, the Heads have overall responsibility for E-Safety within our schools. The day-to-day management of this will be delegated to a member of staff, the E-Safety Officer (or more than one), as indicated below.

The Heads 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 school board, parents.
- The designated E-Safety Officer(s) has had appropriate CPD in order to undertake the day to day duties.
- All E-Safety incidents are dealt with promptly and appropriately.

E-Safety Officer (ESO)

The E-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarise 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 Heads.
- Advise the Heads, school board 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 IT department and other agencies as required.
- Retain responsibility for the E-Safety incident log (located in the 3Sys MIS); ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical E-Safety measures in school (e.g. Internet filtering and monitoring software, behavior management software) are fit for purpose through liaison with IT department.

- Make him/herself aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Heads and responsible board member to decide on what reports may be appropriate for viewing.
- Chair the E-Safety Committee and reports to the Board regularly.

IT Department 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; that categories of use are discussed and agreed with the e-safety officer and Heads.
  - Passwords are applied correctly to all users regardless of age. Passwords for all must conform to the network minimum.

All Staff

Staff are to ensure that:

- All details within this policy are understood. The boundaries of use of ICT equipment and services in this school are given in the Staff E-Safety guidelines below If anything is not understood it should be brought to the attention of their Head or line manager.
- 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 relevant Head or line manager. If you are unsure the matter is to be raised with the E-Safety Officer or the Head or line manager to make a decision.
- The reporting flowcharts contained within this e-safety policy are fully understood.

All Students

The boundaries of use of ICT equipment and services in this school are given in the Students E-Safety guidelines below; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behavior policy.

E-Safety is embedded into 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.

Parents and 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 parents evenings, school newsletters and the VLE 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 that the school needs to have rules in place to ensure that their child can be properly safeguarded.

E-Safety Committee

Chaired by the E-Safety Officer, the E-Safety Committee is responsible:

- to advise on changes to the E-Safety Policy.
- to establish the effectiveness (or not) of E-Safety training and awareness in the school.
- to recommend further initiatives for E-Safety training and awareness at the school.

Established from the E-Safety Officer, Data Manager, ICT manager, Kamyk Primary ICT coordinator, Vlastina Primary ICT coordinator, Child protection officer and others as required, the E-Safety Committee will meet on a termly basis and its sessions will have written minutes.

Technology

School uses a range of devices including PC's, laptops, Apple Macs, Notebooks, IPads, and Tablets. In order to safeguard the student and in order to prevent loss of personal data we are entitled to employ the following assistive technology:

Internet Filtering – school is entitled to use appropriate software that prevents unauthorised 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 Coordinators, E-Safety Officer, E-Safety Liaisons and IT Manager are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Heads and Line Managers.

Email Filtering – the school is entitled to use appropriate software 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.

Passwords – school is entitled to use appropriate security systems to prevent all users to access any device without a unique username and password.

Anti-Virus – All capable devices will have anti-virus software. This software is automatically updated as new virus definitions become available. IT Support will be responsible for ensuring this task is carried out, and will report to the Heads if there are any concerns.

Safe Use Guidelines and restrictions

Internet– Use of the Internet in school is a privilege, not a right and is subject to the rules content in this policy

Email– 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. Students are permitted to use the school email system, and as such will be given their own email address.

Photos and videos– The word 'image' is used here to include photographs, digital photographs, webcam images, film and video recordings. The Prague British School believes that the responsible use of children's images can make a valuable contribution to the life and morale of the school. The use of photographs in school publicity materials can increase pupil motivation and help parents and the local community identify and celebrate the school's achievements. We only use images that the School Heads consider suitable and which appropriately represent the range of activities the school provides and the values it adheres to. No images will be used which could be considered to put any child at increased risk. We will only use images of children in suitable dress. The School Heads decide if images of some activities – such as sports or arts – are suitable without presenting risk of potential misuse. Any evidence of use of inappropriate images, or the misuse of images, should be reported to the School Head / E-Safety Officer immediately. Full names of individual pupils will not be published online in conjunction with their image.

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).

Social Networking– there are many social networking services available; PBS 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 list of social media services which are permitted for use within PBS and have been appropriately risk assessed is regularly updated by ESO and published

Uploading software –It is strictly forbidden to upload any type of software without prior permission of the IT Department.

Notice and take down policy – should it come to the schools 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.

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. The E-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

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, PBS 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.
E-Safety lessons plans can be found in the following location

W:\ac_kamyk\Teachers\All\E-safety

Pupils will receive education relating to E-Safety from their class teachers in the Primary schools, with the material covered tailored to the age of the pupils.
Pupils in the Secondary schools will receive e-safety lessons from the specialist ICT teachers during the course of the year.

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 and responsible Board member 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 for further CPD.

The E-Safety Training Programme can be found in the following location

W:\ac_kamyk\Teachers\All\E-safety

Staff E-Safety guidelines

Note: All Internet and email activity is subject to monitoring

You must read this policy in conjunction with the E-Safety Policy.

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 allowed in school in accordance with the E-Safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become "friends" with pupils on personal social networks

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 school ICT equipment for personal use unless specific permission has been given from the Head or Line Manager 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 or Line Manager. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by IT Department and the E-Safety Officer.

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

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.

Student's E-Safety guidelines

Our Charter of Good Online Behaviour

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 other people's work or pictures without permission to do so.

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.

E-Safety Incident Log

Child's Name		**Year Group and Class**	
Child's DOB		**Class Teacher**	
Male /Female	**Nationality:**	**Student's address (if known)**	
Student No:	**Reported By:** *(name of staff member)*	**Reported To:** *(e.g. Head, E-Safety Officer)*	
	When:	**When:**	
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)			
Signature (Teacher)		**Date**	
Review Date:			
Result of Review:			
Signature (Head)		**Date:**	
Signature (Board member)		**Date:**	

Risk Log

(with a couple of examples)

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 Headteacher and School Board.**
Final decision rests with Headteacher and School Board

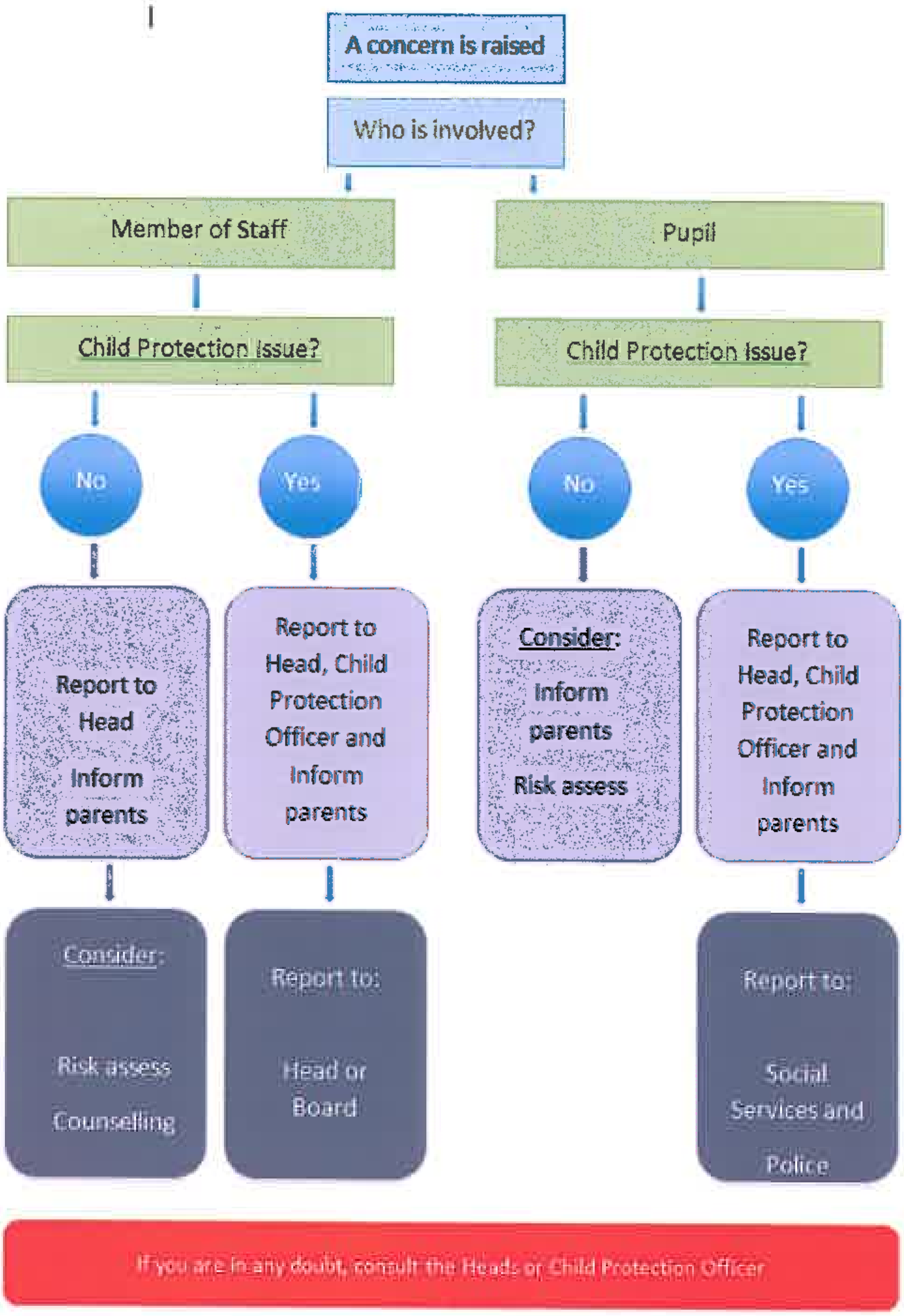
Risk Assessment (Examples)

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. As the laptops are owned by the school, and the school requires the student to undertake this work at home, the school has a common law duty of care to ensure, as much as is reasonably possible, the safe and wellbeing of the child.
Likelihood 3	The inquisitive nature of children and young people is that they may actively seek out unsavory 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 IT Support
Mitigation	This risk should be actioned from both a technical and educational aspect: Technical: Laptop is to be locked down using XXXXXXXX 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.

Approved / Not Approved (circle as appropriate) **Date:**

Signed (Headteacher) : **Signed (Board Member) :**

Inappropriate Activity Flowchart



A concern is raised

Who is involved?

Member of Staff

Child Protection Issue?

No

Report to Head

Inform parents

Consider:

Risk assess

Counselling

Yes

Report to Head, Child Protection Officer and Inform parents

Report to:

Head or Board

Pupil

Child Protection Issue?

No

Consider:

Inform parents

Risk assess

Yes

Report to Head, Child Protection Officer and Inform parents

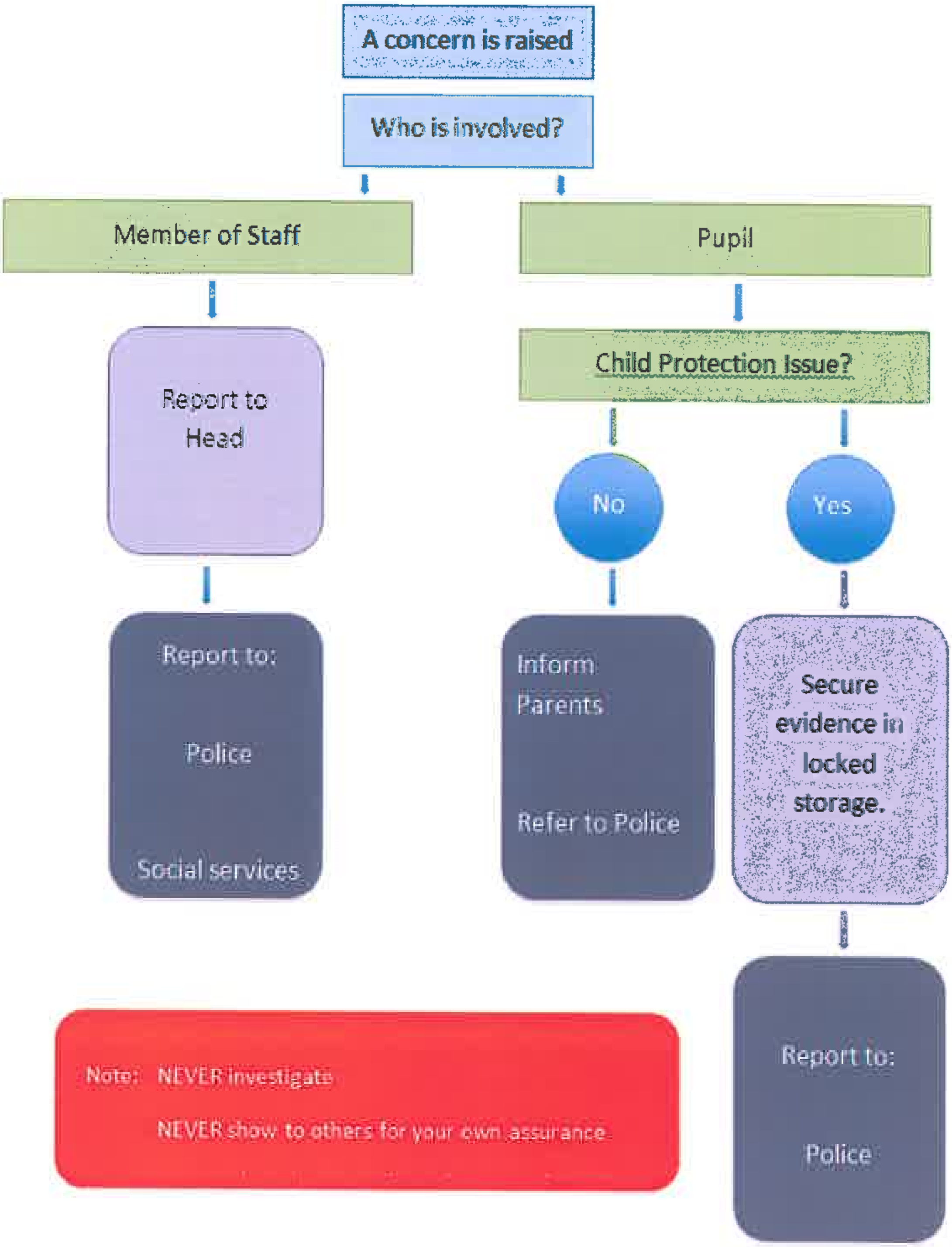
Report to:

Social Services and

Police

If you are in any doubt, consult the Heads or Child Protection Officer

Illegal Activity Flowchart



A concern is raised

Who is involved?

Member of Staff

Pupil

Report to Head

Report to:

Police

Social services

Child Protection Issue?

No

Yes

Inform Parents

Refer to Police

Secure evidence in locked storage.

Report to:

Police

Note: NEVER investigate

NEVER show to others for your own assurance

Essential Contacts in the Czech Republic

Name	Telephone	Websites, Note
Police	158	
Emergency	155, 112 (English)	
Social Care (OSPOD)	Prague 12: 261 397 327 Prague 6: 220 189 611	
Helpline (Dětské krizové centrum)	241484 149 nonstop	www.dkc.cz
Helpline (Linka bezpeči)	116 I11 for children 840 111 234 for parents and adults	www.link:abe eci.cz (also in English)
Nadace Naše dítě	266 727 933	www.nasedite.cz (also in English) Helping children in difficult situation e.g. abused, exploited, abandoned
Helpline DONA	251 511 313 nonstop	www.donalinka.cz (also in English) for domestic violence victims
FOD, Klokánek shelter ul. Láskova 1803, Praha 4	271 912 500	www.klokanek-laskova.cz shelter for mothers and children
Office for International Legal Protection of children Úfad pro mezinárodněprávní ochranu dětí Šilingerovo nám.3/4 60200Brno	542 215 522 731 654 879 - only for emergency calls	www.umpod.cz (also in English)
Drop-In Karoliny Světlé 18, Praha I		The first place of contact for those in need of help connected with problems concerning non-alcoholic drugs.
Poradenská linka pro pedagogy Helpline for teachers	841 220 220 777 711 439	

Whole School E-Safety Policy
03.018

Standardized Acknowledgment list of Internal Policy by the Board
Standardizované prohlášení o Vnitřním předpisu „ Boardem "

Author/ *Autor*: Iain Murray
Superiors name/ *Jméno nadřízeného*: Tim Roberts
Approval date/ *Datum schválení*: 29th May 2015
Policy is/ *Vnitřní předpis je*: PUBLIC/ VEŘEJNÝ
Archive number/ *Archivační číslo*: 150529_03.018

Standardized Acknowledgment list of Internal Policy by the Board of Directors

Standardizované prohlášení o Vnitřním předpisu „Boardem“

The member of the Board of Directors accepts and by signature acknowledges enactment of Internal Policy name: **Whole School E-Safety Policy**
Number: **03.018**

I, a member of the Board of Directors declare that I am familiar with the Internal Policy, and I will inform managers and employees in my line of management about its existence and /or update.

Členové „Boardu“ PŘIJÍMAJÍ a svým podpisem STVRZUJÍ platnost vnitřního předpisu.
Název: **Whole School E-Safety Policy**
Číslo: **03.018**

Zároveň PROHLAŠUJI, jako člen „Boardu“, že jsem se s vnitřním předpisem seznámil/a, a budu o jeho vzniku a/nebo aktualizaci informovat jednotlivé manažery a zaměstnance, kteří jsou v mé kompetenci a zodpovědnosti.

School/Department **Škola / Oddělení**	**Name and Surname** **Jméno a Příjmení**	**Signature/ Podpis**	**Date /Datum**
Finance, ICT, HR	*Michal Bočan*		10/6/2015
Head of Primary Schools	*John Bagust*		10/6/2015
Head of Senior School	*Tim Roberts*		10/6/2015
Marketing, Admission	*Fraser Litster*		10/6/2015
Sourcing and Services, Office	*Lenka Bizdrová*		10/6/2015

Ing. Michal Bočan
Managing Director_Executive head
Výkonný ředitel/Jednatel

Date/Datum: 10/6/2015

Lenka Bizdrová
Executive head CBZS
Jednatelka ČBZŠ