Perrott Hill

BRITISH SCHOOL · PRAGUE

Personal Device Policy

Smartphones / Watches / Tablets / Computers

Personal Device Policy

Table of Contents

Personal Device Policy

1. Rationale

Perrott Hill British School [PHBS] is aware that *personal devices* and *mobile phones* are an important part of today's world, particularly for young people. They are important for personal reasons, whilst we also understand that they comprise an important part of day-to-day individual safety. Surveying the opinion of parents, guardians, and students, the school leadership and our teaching faculty know that students carry phones so that they can contact their families if necessary, whether it be before, after, or even during school/lesson time. Young people today feel a heightened connection to their mobile devices and we acknowledge the integral part they play in the social life of our students. Further, [PHBS] also recognises that moder day teaching and pedagogical methodologies increasingly demand the integration of technology into the classroom as well as wider school-life.

The positives of personal devices & mobile phones are reasoned above. The negatives, however are increasingly noticetable not just to the education practioners in [PHBS] but to global pedagogical leadership. As stated by the Department of Education (UK): "mobile phones can be immensely distracting in the classroom for both pupils and their teachers". Away from learning, mobile phone/personal device use increasingly plays a factor in safeguarding & child protection concerns.

Smart phones, such as those powered by Apple OS (iPhone), Android (Google devices, Samsung, HTC, Nexus, Huawei), Windows, and more, now have numerous additional functions. Used wisely, they can be fun and enriching; used poorly, they can be pernicious, damaging and cruel. Whether it be through integrated cameras on smart phones, video recording capabilities, or messaging systems, [PHBS] is alarmed by the damaging possibilities personal devices can have upon the well-being of our students. Easy access to the internet also allows students to connect to the internet whenever and wherever they ara, allowing access to web-applications, downloadable apps and, most worryingly, social networking, e.g. Facebook, Twitter, TickTock, WhatsApp, SnapChat, and more.

As educators, we have encountered many problems with smart phones and personal devices in school. These include: bullying (in-school and online); disruption to lessons; taking pictures and images without consent; videoing without consent; recording audio without consent; plagiarism of school-work; spreading false information; and also the dissemination of extremist views which are contrary to our school's philosophy and proud international, as well as multicultural, character.

Being a British School Overseas in the Czech Republic, the above dangers are contrary to the UK's Department of Education's (i) "Keeping Children Safe in Education" (2022) & (ii) the "Prevent Duty" (2015) policies, as well as the Czech Republic's Ministry of Education, Youth & Sports (iii) "Methodological Recommendations for the Primary Prevention of Risky Behaviou Youth" (2016) and (iv) guidance from the "Centre for Prevention of Risky Virtual (Faculty of Education / Palacký University Olomouc).

    (i)   https://tinyurl.com/yckan362
    (ii)   https://tinyurl.com/2mam8dvw
    (iii)   https://tinyurl.com/47xeup75
    (iv)   https://www.prvok.upol.cz

A proud social and family-orientated school, our policy exists to encourage social interaction amongst our students. Our wish is for our students to bond during school-time, to make and foster perserving friendships. Social interaction and communication is so important for young people and creates a more enriching learning atmosphere. During the breaks/lunchtime, we encourage these positive beheaviours and, because of this, we introduce this policy to encourage positive student welfare.

Our central rules:

Smart/mobile phone use is strictly prohibited during short breaks and lunch-break

Short Break #1	09:10 - 09:20
Short Break #2	11:00 - 11:10
Lunch Break	11:50 - 12:20
Short Break #3	13:00 - 13:10
Short Break #4	13:50 - 14:00

Devices may be used before school, long-break and after-school

Before School	08:00 - 08:30
Long Break	10:00 - 10:20
After School	14:40 - *onwards*

1.1 Purpose of the Policy

The purpose of the policy is to clearly clarify our epxectations of students whilst they are on the school grounds/premises. It intends to outline the rules of the school, pertaining to personal device usage, as well as the behavioural procedure when the guideliens are not followed. At this point, [PHBS] wishes to make it clear that any device a student brings into school is their personal responsibility. [PHBS] is not responsible for the loss, damage, or theft, of any personal device, even when it is confiscared in accordance to the rules of this policy.

The policy aims to:

- Clearly state and highlight the school's personal device / smart phone policy

- Ensure that students, parents, as well as school staff, fully understand the policy and understand the reasons for the policy

- Work with the school's Positive Behavioural Policy and Safeguarding Policy to ensure that [PHBS] is a safe and character enriching environment for our students

- Reduce possible anti-social behaviours associated with personal device and smart phone use, such as (but not restricted to): bulling; online bullying; non-consenual photography; and minimising disruption to the classroom and learning

Personal Device Policy

2. Unacceptable Use of Smart/Mobile Phones, Watches, Tablets & Computers

Every member of [PHBS] should understand what constitutes as an unacceprtable use of a personal device. Clear misuse of a personal device is defined as the following under specific catergories:

2.1 Personal Device Responsibility

- Any personal device brought into [PHBS] is the sole responsibility of the owner

- As above, any personal device taken on a [PHBS] excursion, trip, or external school event, remains the sole responsibility of the student

- Ownership includes a device given to a student by a parent, guardian, friend, or any non-[PHBS] member, for which they have personal responsibility

- We recommend that all personal devices are labelled for clear identification of ownership (in the event of a lost or stolen device)

2.2 Safe Storage of Personal Devices

- Mobile phones & smart phones must be locked in the correct storage box at all times (by 08:30 and the first bell)

- Larger personal devices such as laptop computers, tablets, headphones (including earbuds), must be safely stored in the student's locker or kept in the student's backpack/suitcase/satchel

2.3 Interfereing with Education / Lessons

- Using a mobile/smart telephone or personal device during a classroom lesson without the express permission of a teacher, member of staff or present adult

- Using a smart watch during a lesson for any purpose without a clear direction from a teacher, member of staff or present adult

- Disturbance caused by a sound emitting from any personal device (those previously stated throughout this policy)

- Entering a classroom whilst using a personal device, including: headphones & earbuds, mobile/smart phone, tablet device, personal gaming system, and personal computer

- Recording (whether video or audio) a teacher and lesson content without the direct permission of the instructor

2.4 Safeguarding, Child Protection & Positive Behaviour

- Bullying by text, image, social media, messaging, or emailing (this includes any of these conducted toward a [PHBS] member even outside of school hours (08:00 - 15:30)

- Using a personal device for *sexting* personal images (images of themselves)

- Using a personal device for *sexting* images of others

- Sexting can include but is not restricted to the following: the electronic distribution/spread of text messages, one's own photographs or own videos containing sexual content, including naked imagery and imagery of 'near-naked' poses including underwear, lingerie, exposing sensitive areas of the body, including what can be considered 'non acceptable' dress as identificied in the school's dress- code

- Encouraging others to take or send *sexts* is also forbidden

- Sending inapprpraite imagery to others, including: racist imagery, violent imagery, imagery which mocks a person's gender or sexuality,

- The deliberate engineering of situations where people's reactions (including students, teachers, members of [PHBS] administration and general staff) are filmed or photographed in order to humiliate, embaress and intimidate by publishing to a wider audience (for example, any social media platform)

- Students posting material on social network sites with no thought to the risks to their personal reputation and sometimes with deliberate intention of causing harm to others

- Using personal devices to make rude, menacing and hurtful comments, lying about events/actions or making false-accusations about other students or teachers

- Photographing or filming other students, teachers or staff members without their knowledge or permission

- Photographing or filming in toilets, changing rooms and similar areas

- Outside of school: even though it is not school hours, using a personal device to harm or intimidate a member of [PHBS] is still an actionable matter; breaking any of the previously stated guidelines, outside of school, is considered to be as unacceptable as if in school

Personal Device Policy

3.   Acceptable Use of Smart/Mobile Phones, Watches, Tablets & Computers

Acceptable use of personal devices means that students operate their smart/mobile phones, smart watches, tablets, according to the following guidelines. The policy is not designed to restrict or be unfair to students, but to enable them to better focus on effective learning and to develop healthy, normal, communicative relationshisp with other students in-and-around the school. Breaking or infringing upon these guidelines will result in consequences outlines in the Positive Behaviour Policy and in Section 4 of this document.

- Smart/mobile phones must be turned off during school hours and placed in the student's own personal device storage box
- "School hours" are defined on Page 5 of this policy document
- Placing a phone on "silent" and keeping it in one's bag/locker is not permitted
- Personal devices must not be used anywhere on the school premises during 'school hours', including outside (the changing room area, the sport's field, the car-park and behind the school classrooms)
- Personal devices may be used in a lesson only with the express permission of a teacher
    - o Students will be informed ahead about this and teachers have the responsibility to log when a lesson will use a personal device
- During the hours when use of a mobile/smart phone are acceptable (see Page 5), students are to strictly adhere to the guideliene displayed in Section 2 of this policy (Unacceptable Use)
    - o Morning: all phones must be placed in their storage box by the first bell (08:28)
    - o Long break: all phones must be placed in their storage box by the first bell (10:18)

Personal Device Policy

4. Offence Procedure

The following procedures are designed to enforce the school policy. Our chief priority is the welfare and we believe, based on our own experience and increasing literature on the subject, that a high level of personal device use in schools is increasingly hazardous to education as well as a student's development.

4.1 Offence Procedure

- Students may use their mobile phones before the start of the school day (before 08:28), during long-break (to communicate any important information to their parents), and at the end of the school day (14:40).
  - Any student found using their mobile phone outside of the above hours will have their device confiscated. <u>Phones must not be seen or heard</u>. This includes the use of "smart" watches - the use of these is not allowed as they are effectively mobile phones and will be treated as such.
- Serious misuse will lead to the confiscation of a student's mobile phone or personal device. Communication with parent will be immediate and the following steps, outlined below and depending on the severity of the offence, will be implemented. If there offense is serious (for example the sharing of sexual, discriminatory, racist or material which can constitute as bullying) then other external authorities can be contacted.

4.2 Personal Device Misuse - FIRST OFFENCE

- (Step #1) Phones taken from students will be taken to the office of the Head of School. If the Head of School is unavailable it will be taken to the School Secretary. The phone will be kept secure and safe in these private office spaces. Students will be asked to fully turn off their devices before handing them to the member of staff.
- (Step #2) This first misuse will be logged and recorded in accordance to the Positive Behavioural Policy.
- On the first confiscation, students will be allowed to collect their phone at the end of the school date from the Head of School. They will be required to sign that their phone has been returned and that they understand that this is the first step in the policy

4.3 Personal Device Misuse - SECOND OFFENCE

- If the phone is taken again, the same procedure as above will occur (steps 1 and 2).

- Parents will be contacted to collect the mobile phone or personal device from school.

- If a parent does not come to school to collect the device, it will be kept protected in the school safe until they do so. The length of time the phone remains in the care of the school is dependent on the judgement of the parent (this applies to all the stages that follow).

- The student will receive a long-break and lunch-time detention, the date of which to be decided by the school's Behavioural Coordiantor.

- The second misuse will be logged and recorded in accordance to the school behavioural rules.

4.4 Personal Device Misuse - THIRD OFFENCE

- Parents will be contacted to collect the mobile phone device from the school Parents

- will be required to have a meeting with the appropriate Class Teacher

- The above meeting constitutes as "STAGE 2" found in the "Positive Behaviour Policy"

- As the student is now attached to the "Positive Behaviour Policy", the misuse of personal devices is now considered to be a deeper offence than previous. This means that personal device misuse is considered to no longer be a 'minor misdemeanor'.

4.5 Personal Device Misuse - FOURTH OFFENCE

- Parents will be contacted to collect personal device from school Parents

- will be required to have a meeting with the Head of School

- The above meeting constitutes as "STAGE 3" found in the "Positive Behaviour Policy"

- As the student is now on Stage 3, any future personal device misuse may result in being sent home early from school and, also, possible suspension for 1-day

4.5 Personal Device Misuse - FIFTH OFFENCE

- Parents will be contacted to collect the personal device from school

- The fifth offence will constitute as "STAGE 4" found in the "Positive Behaviour Policy"; therefore a behavioural committee will be convened

- The behavioural committee will be comprised of the Head of School, the School Director and one/two members of staff who do not teach the student

- The fifth offence will likely lead to student suspension, the number of days determined by the behavioural committee

4.6   Personal Device Misuse - ONGOING OFFENCES

If the student continues to break the guidelines of the Personal Device Policy, the following protocol will be implemented:

- At this point, the student will be completely banned from bringing personal devices into school

- The offending student will be sent home from school

- Parents will be notified of this ahead of time and their cooperation will be sought in regard to the safe travel of the student

- The behavioural committee will reconvene to discuss further days of suspension including, possibly, expulsion depending on the extremity of the offence

Personal Device Policy

5. Examination of Personal Device Content

The examination, similar to actions such as bag searches, are conducted reluctantly by Perrott Hill British School. The school and its employees respect the right to student privacy and will only cross this line when absolutely necessary. As an institution with an active Childprotction & Safeguarding Policy, the safety our students trumps all other concerns. Due to this, when it is deemed absolutely necessary, a trained and designated member of staff will examine personal device content.

In accordance with Czech law, the examination will be conducted infront of the owner of the device. Additionally, the parent and/or guardian of the student will be conducted and informed of the search. Further, the examination will be recorded, logged and performed infront of a second staff member. All actions will be recorded responsibly and methodically, in case any digital content discoveries become evidence of criminal activity.

Parents/guardians will be informed of every occurance, step and discovery.

Personal Device Policy

6. Appendix

Preamble: As a British School Overseas (BSO) in the Czech Republic, the policies of Perrott Hill British School are guided chiefly by (1) the laws, stipulations and governance of local laws in the Czech Republic and (2) recommendations and influence from the Deaprtment of Education found in the United Kingdom of Great Britain and Northern Ireland. At Perrott Hill British School we respect and act within the confines of local laws and customs yet, as a proud BSO institution, we will always apply UK policy as much as we can.

6.1 Statutory Guidance (Czech Republic)

Č.j.: MSMT− 32550/2017−1

<table>
<tr><td colspan="2">WHAT TO DO WHEN – TEACHER INTERVENTION
Risky behavior in the school environment - framework concept
Appendix No. 7
Title: Cyberbullying and other forms of cyber aggression
Author: Kamil Kopecký, René Szotkowski (Centre PRVoK PdF UP Olomouc)</td></tr>
<tr><td>Type of risky behavior</td><td>Cyberbullying is a form of aggression that is used against an individual or a group of people using information and communication technologies (computers, tablets, mobile phones and other modern communication tools), and which occurs repeatedly, whether by the original aggressor or other people - so-called .secondary attackers (e.g. repeated sharing of the recording, repeated commenting, etc.).
Although cyberbullying is usually defined as intentional activity, it can also occur unintentionally – for example, as an inappropriate joke that gets out of control in an online environment.
Cyberbullying is often confused with online harassment. The term online harassment refers to one-off attacks, the impact of which is only temporary. In particular, "real" cyberbullying must meet the criteria of repetition, it must be long-term and it must be perceived as hurtful. The victim is then unable to effectively defend himself against the attacks, there is a power imbalance.</td></tr>
<tr><td>Starting points</td><td>A. Differences between traditional bullying and cyberbullying

Cyberbullying has its own specifics that distinguish it from traditional psychological or physical bullying.

<i>Cyberbullying reach and audience size</i>
Compared to forms of classic bullying that takes place "face to face", cyberbullying by its very nature has a much greater reach, which worsens the experience of the victim. If the victim is being bullied in class, at most a few dozen people witness the gossip, swearing, mocking and embarrassment. In the Internet environment, there are probably several tens of thousands of people who are witnesses (as well as attackers). All of them can become involved in cyberbullying and become aggressors, or even participate in the spread of cyberbullying among other Internet users.

<i>The place of attack</i>
While in traditional bullying you can predict when and where the attack will take place (eg at school, on the playground, on the way home from school), in the case of cyberbullying, the aggressor can carry out the attack anytime and anywhere. In principle, therefore, the presence of the aggressor and the victim in the same place is not necessary (Krejčí, 2010; Ministry of Education, 2009).

<i>Anonymity</i>
The perpetrator of cyberbullying can be anonymous, hidden behind a nickname or other vague identifier, so the victim is often unable to identify the aggressor. Although identifying the anonymous perpetrator</td></tr>
</table>

of cyberbullying is quite difficult, research by the Minimization of Bullying Project has shown that in 78% of cyberbullying cases the identity of the attacker was established - 51% of the aggressors were from the same class as the victim, 27% of the perpetrators were from the same school as the victim, only from a different class (Krejčí, 2010; Udatná, 2008).

In some cases, the perpetrators are not anonymous, especially if the cyberbullying first takes place in a closed group in a social network environment - there is no need to mask the identity, the perpetrators appear under real names and surnames. At this stage, the victim may not be aware of the initial cyberbullying, only becoming aware of it when the number of discussants increases significantly or when the group becomes public. In the case of an anonymous or non-anonymous attack, the perpetrator often does not perceive the impact of his actions, does not see the victim's direct reaction to the attack, and is unable to evaluate the intensity of the attack. His attack then has a greater impact than he originally expected. An anonymous attack is essentially depersonalized – it is accompanied by a disinhibition effect (Kovářová & Kopecký, 2012; Suler, 2004; Udris, 2014), which contributes to cyberbullying.

Time

As such, cyberbullying can take place all the time. The actual attack on the victim can be carried out at any time - during school hours, during breaks, outside of school hours, on the weekend, at any time of the day or night. The preparation of cyberbullying itself is not limited either, the perpetrator has any amount of time at his disposal and can think about his attack (e.g. create a defamatory, offensive collage from a photo, which he will further distribute among online users).

Because cyberbullying takes place mainly in the Internet environment, the attack spreads much faster than with regular bullying. Within minutes defamatory material can be spread among hundreds or thousands of users and can reach the limit of viral distribution. If offensive material (e.g. a photo) goes viral, it cannot in principle be removed from the Internet – it spreads through the Internet like a virus (hence the term viral spread). In many cases, there is also a time lag between the creation of defamatory content
and the moment when the victim himself becomes aware of the cyberbullying. Pupils, for example, set up a public discussion group about their classmate, in which they defame, insult, slander, share their photos or videos, etc. The victim finds out about the discussion group over time - for example, after several days or weeks. At that time, a large number of users can already be involved in cyberbullying.

The transformation of aggressor and victim

The anonymity of the virtual environment erases differences between people - whether it is age, gender, social status, physical disposition, numerical superiority or, for example, the courage to attack. And as evidenced by the results of cyberbullying research from recent years, the

perpetrators of cyberbullying are often the victims themselves who, for example, react disproportionately to the hardships they have experienced (Kopecký, Szotkowski, & Krejčí, 2015). An offender who wants to carry out cyberbullying may only have basic IT literacy skills (most services are intuitive enough that advanced knowledge is not necessary).

Different ways to deal with cyberbullying and bullying
When dealing with cyberbullying, a number of situations arise that are more difficult to resolve than with traditional forms of bullying.

Cyberbullying makes it difficult to:
A.   ensure quick protection of the victim (e.g. remove the discussion group or profile in which the cyberbullying occurs, ensure the removal of defamatory materials from the Internet and thus stop the further spread of cyberbullying, etc.),

B.   ensure a sufficient number of witnesses (cyberbullying often lacks witnesses, the audience is largely anonymous and it is impossible to identify who has information about cyberbullying),

C.   trace the attacker (with traditional bullying, we know the attacker, but with cyberbullying, the attacker often appears only under a nickname, uses fake profiles, etc.),

D.   recognize when it is cyberbullying and when it is not (students often do not recognize the boundaries of cyberbullying and do not know how to deal with it, who to contact, how to proceed, what steps to take).

A. Basic forms of cyberbullying and related phenomena

Cyberbullying often begins as traditional bullying (psychological or physical), or is an accompanying phenomenon. However, it can exist completely independently of traditional bullying.

The basic forms of cyberbullying from the point of view of the connection between attackers and victims include:

1. Direct cyberbullying

In direct cyberbullying, the aggressor attacks the victim directly, for example, begins to defame the victim, creates a fake profile about him, publishes his photo or video, etc.

2. Indirect cyberbullying (cyberbullying-by-proxy)

In indirect cyberbullying, the aggressor uses another person for the attack, who often does not know that he has become an instrument of the attack - e.g. revenge. A typical example is a situation where an attacker penetrates the victim's account (e.g. an account on a social network), through this account he begins to defame other users, who begin to react

and take revenge for online insults to the owner of the account from which the defamatory messages were sent. The account owner only learns about this after a time delay.

In the case of both forms of cyberbullying, the perpetrator can use both their own identities and fake identities.
Cyberbullying can be further divided by whether the audience is actively involved or whether it takes place in private without an audience present.

Thus, the basic forms include:
1.   Cyberbullying with an audience (public)
It is cyberbullying, the essence of which is to spread information about the victim among a large number of users. This category includes the publication of humiliating recordings of the victim, identity theft, verbal forms of cyberbullying (defamation, insults, provoking), etc. The presence of an audience is a basic and mandatory part of cyberbullying. Communication takes place through public communication channels.

2.   Cyberbullying without an audience (private)
It is cyberbullying, in which usually only the perpetrator and the victim communicate, while their communication is private, without the presence of an audience. As part of this form of cyberbullying, there is often an exchange of intimate material - either voluntarily or under duress. Cyberbullying in the form of blackmail or threats can be included in this category. Communication takes place via private communication channels – private chat within social networks, instant messengers and VoIP communicators (Skype), or via SMS/MMS. Manifestations of cyberbullying (e.g. defamation, provocation, threats, blackmail in an online environment, etc.) can occur in the form of a one-off attack (so-called fake cyberbullying, cyber-harassment, cyber-aggression, etc.) or a long-term attack with increasing intensity (so-called true cyberbullying). The most well-known manifestations/forms of cyberbullying (Kopecký, Szotkowski, & Krejčí, 2014a; Krejčí, 2010; Willard, 2007b) mainly include attacks using photos, video recordings, audio recordings, but also common verbal forms of attacks.

Cyberbullying includes manifestations of traditional psychological bullying enhanced by the use of ICT, for example:
Defamation (humiliation, cursing, insulting) in the online environment.
Threats and intimidation in the online environment.
Blackmail in an online environment.
Defamation (slander) in the online environment.

Typical forms of cyberbullying also include:
Posting humiliating videos, audios or photos
Denigration

	Identity theft (impersonation) and its misuse
	Embarrassment with fake profiles
	Provoking and attacking users in online communication (flaming/bashing)
	Disclosure of other people's secrets with the aim of harming the victim (trickery/outing)
	Exclusion from the virtual community (exclusion)
	Harassment
	Specific forms of cyberbullying associated with playing online games
	Happy slapping
	Cyberstalking (stalking in connection with the use of information and communication technologies)
	Webcam trolling (abuse of webcams to manipulate Internet users through fake video recordings)
Risk and protective factors	**Risk factors** In the field of cyberbullying prevention, a modified classification of risk factors according to Offord and Bennett (2002) can be used: **1. Individual factors** (e.g. gender, temperament, thrill-seeking, emotional disorders, impulsivity (impulsive posting of electronic content without thinking of consequences), anxiety, depression (a combination of cyberbullying and depression can lead to self-harm or suicidal behavior), deficits in social skills, hostility and aggression, violence, low self-esteem and self-esteem (people with low self-esteem may use online environments more), negative life events and traumatic experiences, failure in school (may be related to teacher cyberbullying as a revenge motive), problems with the law). **2. Family factors** (e.g. dysfunction in the family, strength of bond or bond between parent and adolescent, lack of parental supervision, weak parental support, insufficient parental interest and control (e.g. lack of rules for the use of IT tools in the family), inconsistent upbringing (unhealthy support for child behavior and in situations where the child is the aggressor in the context of cyberbullying), poverty and unemployment in the family, rudeness and conflicts in the family (transferring inappropriate patterns of behavior to communication with the environment)). **3. Peer relationships** (e.g. bullying, dysfunctional relationships with peers, peer pressure (group pressure can accelerate unwanted behavior in cyberspace), membership in a group with risky behavior or positive attitudes towards it (e.g. in hate groups in an online environment targeted at various targets groups), rejection and exclusion from the peer group). **4. School factors** (e.g. not always effective school programs focused on primary prevention, unhealthy school climate, low expectations of educators, focus on performance). **5. Community, fellowship, neighborly relations** (e.g. low quality of youth organizations, loss of economic and educational opportunities, insufficient offer of leisure activities). (Offord & Bennett, 2002; NIDA, 2003; EMCDDA, 2009; Miovský et al., 2012).

	Protective factors In the field of cyberbullying prevention, a modified classification of protective factors according to Fergus and Zimmerman (2005) can be used: **1. Individual factors** (e.g. good coping strategies, social skills, emotional stability, positive self-relation, school performance, resistance to stress, flexibility, conscientiousness, agreeableness, resistance to group pressure). **2. Family factors** (parental support, parental cohesion, parental supervision, healthy lifestyle of parents, control, intolerance to risky behavior, clearly defined rules of behavior and possible sanctions for transgressions, positive bond between parents and child, emotional support, clear rules and boundaries, parental control and consistency). **3. Peer factors** (good peer group with appropriate interests and activities, good interpersonal communication, enough friends, mutual support). **4. School factors** (healthy school environment, good relations with teachers, understandable rules, timely systematic and effective specific primary prevention, participation of pupils and parents). **5. Community, fellowship, neighborly relations** (e.g. organizations that support positive youth development, social and economic opportunities, activities based on spiritual development). (Offord & Bennett, 2002; NIDA, 2003; EMCDDA, 2009; Miovský et al., 2012).
Network of partners, cooperation in the community, region	Within the school, it ensures the cooperation of all activities related to the consulting activities of the school management. The principal of the school usually entrusts the counseling activity to the school's prevention methodologist, or educational counselor, who then cooperates with other pedagogical staff. The school prevention methodologist also cooperates with the school psychologist (if he works at the school), the class teacher, and the school counseling facility. Each school should have an overview of institutions, such as a pedagogical and psychological counseling center, non-profit organizations, a crisis center, a special pedagogic center, an educational care center, a body for the social and legal protection of children, the Police of the Czech Republic, medical facilities, etc., located in region, to whom he can turn in case of any problems. It is advisable to publicly present the list of contacts of all regional partners, e.g. on the school's website, so that teachers, pupils or parents can also use them.
Legislative framework (regional plans, strategies)	**Legislative framework (state level):** **At the state level, the prevention of risky behavior** – in our case, cyberbullying or bullying – is generally managed by a number of strategic documents, from which sub-documents are based. **Strategic documents related to the prevention of cyberbullying include in particular:** Act No. 561/2004 Coll., on preschool, elementary, secondary, higher vocational and other education (Education Act), as amended,

Č.j.: MSMT−
32550/2017−1

Act No. 563/2004 Coll., on teaching staff and on the amendment of certain laws, as amended,

Methodological recommendations for the primary prevention of risky behavior in children and youth ID no.: 21291/2010-28,

Methodical instruction of the Minister of Education, Youth and Sports on the prevention and solution of bullying in schools and school facilities, reference no. MSMT-21149/2016,

Crime Prevention Strategy 2016–2020 (defined in multi-year cycles by Resolution of the Government of the Czech Republic),

National strategy for the primary prevention of risky behavior of children and youth for the period 2013–2018 (Ministry of Education of the Czech Republic, 2013).

Legislative framework (school level):
Schools are obliged to ensure the safety and health of their pupils and at the same time create conditions for preventing the emergence of socially pathological phenomena. This obligation is given by the Education Act (Act 561/2004 Coll., 2012), specifically § 29, which focuses on safety and health in schools. Schools mean schools and school facilities.

The school's strategic documents related to the prevention of risky behavior:
1. Internal rules of the school facility, school rules
2. School preventive strategy
3. School preventive program (formerly Minimum preventive program)
4. Emergency plans

Other documents that are closely connected with primary prevention at primary school may include, for example:

School Counseling Program – this includes the description of activities, the division of roles and the definition of responsibilities of school counseling workers, the creation of a time space for the services provided, methods of communication and cooperation within the counseling workplace and outside with specialized counseling workplaces in education (pedagogical-psychological counseling center, special pedagogic center, educational center care) and with relevant organizations outside education.

Plan for further education of pedagogues – includes the training of pedagogues and, to an increased extent, the worker in charge of dealing with bullying (usually the school's prevention methodology) and classroom teachers (especially in the prevention of bullying, in the area of communication, conflict resolution, effective preventive strategies in school practice, interaction between teacher and pupil).

Preventive and counseling services are provided in the school environment mainly through so-called school counseling workplaces, which are defined by Decree Decree No. 72/2005 Coll., on the provision

	of counseling services in schools and school counseling facilities, as amended. Counseling services at school are usually provided by an educational counselor, a school prevention methodologist, or a school psychologist/school special pedagogue and their consulting team composed of selected pedagogues (Ciklová, 2014). The goal of school counseling centers is mainly counseling support for pupils, parents and teachers.

Prevention - non-specific and specific (general, indicated, selective)	**How to prevent cyberbullying:**
	Cyberbullying can be classified among the basic areas of risky behavior, specifically between bullying and extreme manifestations of aggression (Miovský, 2010), according to the National Strategy for the Primary Prevention of Risky Behavior of Children and Youth 2013-2018, it is classified as interpersonal aggressive behavior (MŠMT, 2013).
	The basic way to prevent cyberbullying or minimize its impact is general primary prevention. The goal of primary prevention is to prevent risky behavior. Prevention focused on the area of cyberbullying and other forms of cyber aggression can be implemented in both specific and non-specific forms. Specific primary prevention can be divided into 3 levels, on:
	    a) lying: General prevention (it affects the entire class, school, etc. without distinction). Activities such as long-term prevention programs, interactive discussions, project days, etc. can be included here. At the same time, the topics of primary prevention can be included in the teaching, linked with cross-cutting topics and key competences of the pupil.
	    b) Selective prevention (interferes with persons with increased risk factors for the emergence and development of various forms of risky behavior, e.g. children from excluded locations, children with behavioral disorders, etc.).
	    c) Indicated prevention (targeted at situations where cyberbullying has already occurred in the classroom/school).
	
	Non-specific prevention is then focused on developing a healthy climate in the classroom and school, strengthening good relationships between children, etc.
	
	How to prevent cyberbullying at the school level:
	● Include in the school rules the rules for the use of ICT, the intranet and mobile phones (during lessons, during breaks, on the school premises).
	● Inform pupils about netiquette and the "bill of rights on the Internet". Parents of underage pupils should also be informed about this list, e.g. by posting it on school websites.
	● Install and use software that enables the teacher in the classroom to find out via his computer what the student is doing on his desktop. (Inform pupils about this measure and do not abuse the system!)
	● Be a role model for the appropriate use of modern technology.

<table>
<tr><td></td><td>

- Work on raising pupils' awareness of risky behavior on the Internet.
- Define competences within the school and at events organized by the school outside the place where education takes place).
- Incorporate topics related to risky behavior on the Internet into teaching.
- Educate teachers.
- Encourage the positive use of technology.

How to prevent cyberbullying at the level of individual educators:
- Strengthen empathy between pupils.
- Work on the classroom, school climate.
- Lead to respect for other people.
- Give positive feedback to students.
- Create good relationships between pupils and colleagues.
- Consistently take action against noticeable individual manifestations of aggression.
</td></tr>
</table>

Recommended procedures from the point of view of the teacher - the school	**Strategie řešení kyberšikany** *A. Addressing cyberbullying from the victim's perspective* There is no 100% protection against cyberattacks - whether in the form of one-off cyberaggression or advanced cyberbullying, even if the victim stops using Internet or mobile services, the cyberattack will not stop - the victim only "does not yet know" that he is being defamed in the Internet environment. It is only a matter of time before he becomes aware of the existing situation. According to the findings of Parrisová (Varjas et al., 2010), who conducted research focused on high school students, strategies for coping with cyberbullying from the victim's point of view can be divided into two basic groups, namely reactive and preventive strategies (Černá et al., 2013; Varjas et al., 2010). Reactive strategies for coping with cyberbullying include avoidance (deleting messages, account, blocking phone numbers, ignoring the situation), acceptance (cyberbullying is seen as a part of life), justification (finding reasons why it is not important to deal with cyberbullying, "putting down the aggressor" – is stupid, not worth it, etc.) and searching for support in the neighborhood (confiding in someone, involving other people). According to the students from Parrisova's research (Varjas et al., 2010), preventive strategies included personal communication (trying to prevent misunderstandings caused by the online environment), security and raising awareness of the issue (improving account security, limiting published information, etc.), however, other findings of the research also included the students' opinion that prevention of cyberbullying is not possible - according to them, the Internet provides such a high degree of anonymity that the aggressor records that it is impossible to completely avoid cyberbullying. **Appropriate action for a victim of cyberbullying:**

The individual points do not have to follow each other exactly, e.g. a child can report an attack to an adult already in the initial stages.

1. Keep calm - do not act hastily.
2. Keep evidence - keep and trace all evidence of cyberbullying (SMS messages, e-mail messages, chat messages, save web pages, etc.). Based on this evidence, an investigation can be initiated against the attacker or attackers. (see the attachment for the procedure).
3. End communication with the offender - do not communicate with the attacker, do not try to discourage him from his actions in any way, do not threaten, do not take revenge. The attacker's goal is to elicit a reaction from the victim, whatever it may be.
4. Block the perpetrator and block the content he spreads - try to prevent the attacker from accessing the victim's account or phone number and, if possible in the given situation, to the tool or service he uses to carry out his attacks (contact the service provider).
5. Identify the perpetrator (if this does not endanger the victim)
6. Report the attack to adults (teacher, parent) - confide in a close person. To preserve evidence, contact someone with higher IT literacy. Contact the school and specialized institutions (PPP, Police, SVP, intervention services specializing in dealing with cyberbullying, psychologists, etc.).
7. Do not be afraid to seek help from specialists - contact specialized organizations, counseling centers or the Police of the Czech Republic.
8. *Ask for a final verdict (in case the school resolves the situation) - after investigating the entire case, insist on the final opinion of all interested institutions.*

B. Addressing cyberbullying from a school perspective

Since cyberbullying is closely related to traditional forms of bullying that normally take place in school, cyberbullying is also addressed in the school environment. However, before the solution itself, the school often decides whether it should, can or must be involved in the solution of cyberbullying.

Among the most common arguments against the solution of cyberbullying by the school are the following (Krejčí, 2010):

1. If cyberbullying takes place outside the school building (or outside a school event), it is not the school's problem.
2. Solving cyberbullying in the school will cause negative publicity and discourage potential clients - parents of newly admitted/enrolled pupils.
3. The school does not have the tools to deal with cyberbullying.
4. The tools used by the school are not working (e.g. the attacker's parents are not cooperating).
5. Cyberbullying will go away on its own, so it makes no sense to deal with it in the school environment.

Among the most common arguments for addressing cyberbullying by schools are the following (Krejčí, 2010)

1. Cyberbullying is often accompanied by other types of bullying that take place in the school environment. The school must take care of its climate, it must ensure the rights of both children and employees (e.g. the right to education, the right to working conditions, etc.).
2. According to the number of victims of cyberbullying or related forms of cyber aggression, almost all schools have a problem with it. A school that solves the problems that occur in its environment does the right thing and thus ensures good publicity.
3. The school can proceed in the same way as when dealing with traditional bullying - cyberbullying is related to traditional bullying and is often closely connected with it.
4. If the tools for dealing with cyberbullying do not work, it is necessary to consult the problem, for example, with the departments of social and legal protection of children, the Police of the Czech Republic, specialized counseling centers and solve it in cooperation with them.
5. If we do not deal with cyberbullying, we give a signal to pupils who know about cyberbullying that they can also commit cyberbullying and will not be punished for it. In this way, we build harmful patterns of behavior in them, which they can then pass on.

Although we can discuss the above arguments, the position of the Ministry of Education, Youth and Sports of the Czech Republic, defined in methodological instructions and recommendations for solving risky communication phenomena at school and their prevention, says clearly:

The school should deal with cyberbullying whenever it becomes aware of it (Ministry of Education, 2009).

The basic task must then be to map a specific case, which will help us decide on the correct solution procedure.

When dealing with cases of cyberbullying, the Scenario for ordinary initial bullying can be used (Kolář, 2011), however, due to the specifics of cyberbullying, its individual phases cannot always be implemented (e.g. the perpetrator may be anonymous, there are no witnesses). Although cyberbullying and bullying are usually closely connected - for example, a child who is a victim of traditional bullying also becomes a victim of cyberbullying - the procedure for dealing with cyberbullying is specific and corresponds to the differences between traditional bullying and cyberbullying. The perpetrator can be, for example, anonymous, cyberbullying can take place in a closed environment, cyberbullying also takes place outside of school and the victim needs to be protected outside of school hours, etc. Below we offer basic procedures that can be used when dealing with cyberbullying (Jurková, 2010; Kopecký et al. , 2015; Krejčí, 2010; Ministry of Education).

What the school can do:

1. Support the victim and ensure his safety
The first steps include calming down the victim (he is often upset, his reactions can be exaggerated, in some cases even suicidal) and offering support. At the same time, it is necessary to ensure that cyberbullying does not continue, i.e. remove objectionable content from the Internet - e.g. delete videos that humiliate the victim, delete objectionable photos, block the offender's profile, etc. This can be done in cooperation with an IT expert, the provider of the given online service , service administrators, etc.

2. Secure as much evidence as possible
However, before deleting the materials itself, it is necessary to provide sufficient evidence - take snapshots with evidence, download the given website to the local computer, ensure a list of pupils who have become the audience of cyberbullying (e.g. within a discussion group on a social network) - ideally with links to their profiles, try to identify the aggressor (e.g. through his friends).

With public newsgroups, obtaining evidence is relatively easy because everyone has access to the group, however, there are a large number of cases where attackers have set up a closed newsgroup to which they have invited pre-selected classmates. Within this closed environment, they then carried out cyberbullying and gradually added other users to the group. In these situations, we recommend contacting a professional institution (e.g. the staff of the E-Bezpečí project, the Seznam se sévěčné! project, or criminalists of the information crime department of the Police of the Czech Republic) who can help to secure evidentiary materials in other ways.
We will further use the evidentiary materials as part of the investigation, when communicating with the parents of the aggressors and the parents of the victim, as part of interviews with the aggressors, etc. However, it is always necessary to ensure the safety of witnesses - i.e. the evidentiary material should not be clear as to how it was obtained (e.g. in the header the name of the student from whose profile the record was obtained).

3. Always investigate the incident
All cases must be thoroughly investigated - if we are unable to investigate the incident ourselves, we can use the support of external institutions. The investigation includes finding out where the incident took place, how long it lasted, who was involved in it, what impact it had on the victim, what technical means can be used to stop the attack, etc.

4. Inform parents
It is necessary to inform the parents of the victim and the parents of the aggressor about the incident, the procedures defined in the scenario for

solving traditional bullying can be used. Let's educate the parents about what the resolution process will be at the school level, or about the fact that a given case of cyberbullying does not fall within the competence of the school and that it is possible to use, for example, legal services. In the event that the case of cyberbullying does not fall within the competence of the school (e.g. the attack took place outside of class and has no connection to the bullying that takes place at school), parents can, for example, sue the aggressor in civil court for harassment, intentional exposure to unpleasant experiences, stress, etc. also emphasize new legislative norms - especially the new Civil Code.

5. Consult solutions with other institutions
In some cases, it is appropriate to consult the solution procedure and especially the chosen punishments with other entities - the founder of the school, possibly the Czech School Inspectorate and other institutions. However, the Czech School Inspectorate is not entrusted with methodological management (its competences are defined by the Education Act). In a number of cases, the school did not proceed correctly and, for example, offered students a reduced grade for behavior even in situations that were demonstrably not taking place during school hours or as part of the activities requested by the school.

6. Request a final verdict and information
After examining the entire situation, it is necessary to insist on the final opinion of all interested institutions (e.g. Police of the Czech Republic, OSPOD, pedagogical-psychological counseling center...) and other entities (e.g. parents) (Ministry of Education, 2009).

7. Choose appropriate measures
It is very important that when punishing aggressors, the school proceeds in accordance with the school rules in combination with other strategic documents of the school - e.g. crisis plan, minimum prevention program of the school, etc. When determining the punishment, we use the options offered in the scenario for solving traditional bullying (Kolář, 2011).
In cases of less serious forms of cyberbullying, it is recommended to use informal solutions (Jurková, 2010) - for example, create a set of preventive materials in the area of risky behavior on the Internet, prepare a lecture on the importance of responsible use of modern technologies, etc.

8. Implement preventive measures
Preventive measures must be taken so that undesirable behavior does not repeat itself in the future. These can be secured - for example, through the realization of project days focused on prevention, preparation of materials to support prevention, through so-called role-playing within or outside of regular education, strengthening good relations between pupils, etc.

C. Addressing cyberbullying from a parent's perspective

If a parent discovers that their child has become a participant in cyberbullying – i.e. a victim of it – they have several options for how to proceed. First of all, it is necessary to support the victim himself according to the procedures defined in the previous part of the work (solutions from the victim's point of view) - i.e. end communication, block the attacker, etc. Other important steps from the parent's point of view include:

1. Ensure the safety and support of the child
The first step is to ensure that the child feels safe in the home environment and that he has unconditional support in his parent. Parents must therefore show by words and actions that they, too, want to achieve the same result as their child - to stop cyberbullying (Jurková, 2010).

2. Investigate the situation
The next step is the examination of the situation by the parent himself - the parent must understand what exactly happened, who was involved in the cyberbullying, what was the initial cause, etc. Finding the cause will help the parent choose an adequate procedure and solution - whether their child was the victim or the aggressor.

3. Avoid the immediate ban of the child's access to IT
The parent should not try to solve the situation by banning the child's access to the communication technologies that he used until that moment (e.g. instant messengers, social networks). This strategy does not solve the situation in any way, nor does it have a preventive effect. Bans on the use of electronic communication tools limit the natural communication of children who are used to actively using Internet services. Banning the use of IT tools or blocking objectionable content does not solve cyberbullying by itself.

4. Contact the school, a specialized institution or directly the parents of the aggressor
A common part of the process of dealing with cyberbullying is contacting the school, the service provider in which the cyberbullying takes place, specialized institutions or directly the aggressor's parents. Together with them, the parent can ensure the removal of objectionable materials, implement blocking, think through the solution procedure, etc. In some cases, it is also advisable to contact the Police of the Czech Republic - especially if the victim is threatened with physical assault or if there is a suspicion that a criminal offense has been committed .

5. Demand a final verdict
As with the solution procedures from the perspective of the victim and the school, the parent should always demand the final verdict - how the perpetrators were punished, what measures the school will continue to implement to improve the safety of its students, etc.

3. Draw consequences and determine measures

	If a child has become a perpetrator of cyberbullying, it is necessary to punish him, and in case of repeated cyberbullying, the punishment should be increased proportionately so that he realizes that his behavior is unacceptable and really serious. At the same time, however, it is necessary to positively motivate him so that he does not fix an undesirable pattern of behavior (e.g. if he is labeled an aggressor, he will behave like an aggressor in the future). Always be consistent - if the parent is inconsistent and does not demand compliance with the rules, the offender will understand that he can behave this way in the future because he "got away" with cyberbullying. ***4. Cooperate with the school*** Even after the cyberbullying has ended, it is advisable to continue to cooperate with the school that dealt with the child's cyberbullying, and to support its efforts to ensure the safety of students and teachers. However, the school does not always proceed actively in the case of cyberbullying and in some cases even ignores the situation for various reasons. In the event that the school demonstrably does not want to deal with the child's cyberbullying, it is possible to consider transferring the child to another school (often this is also the only possible solution, especially in a situation where bullying at school has become common and "normal"). All of the above-mentioned procedures make it possible to minimize the impact of the incident on the victim, to ensure that the culprits are punished and to increase the chance that the incident will not be repeated in the future. However, this can only be achieved through the active cooperation of the school and the families of the offender and the victim, and especially active work with the specific class in which the incident occurred.
Possibilities and limits of the school, the teacher	The school has a clear responsibility for children and pupils. In accordance with the provisions of § 29 of Act No. 561/2004 Coll., on pre-school, primary, secondary, higher vocational and other education (Education Act) (Act 561/2004 Coll., 2012), as amended, schools and school facilities are obliged to ensure the safety and health protection of children, pupils and students during all educational and related activities and at the same time create conditions for their healthy development and for the prevention of risky behaviour. For this reason, the teacher must immediately deal with bullying among students and provide immediate help to each of its victims. The school or school facility has responsibility for children and pupils during classes and school events, according to "§ 391 of Act No. 262/2006 Coll., Labor Code and according to the Work Regulations for employees of schools and school facilities, e.g. Article 2 (Decree No. 263/2007 Coll., 2007) and is also responsible for damage caused to pupils during temporary supervision, i.e. during and in direct connection with teaching. The school director is also responsible for ensuring the safety and health protection of his employees according to § 101 and § 102 of Act No.

262/2006 Coll., Labor Code (Act No. 262/2006 Coll., 2006), as amended.

When determining competences in dealing with cyberbullying, it is necessary to determine whether the conduct is demonstrably related to the school's activities (it concerns pupils or school employees and at the same time has a significantly negative impact on the school environment or there is an intense and immediate threat of such disruption).

If yes:

• The school will help the victim secure evidence.
• The school is proceeding according to the crisis plan.
• The School Act newly (as of September 1, 2017) defines the formulation of a particularly serious violation of the School Act, when the school principal is obliged to expel a secondary school student in the aforementioned case. It is about rude and repeated verbal or physical violence against other students or teachers. In the case of pupils who have committed such a particularly serious violation of the school law and who are still in compulsory school attendance, the school principal will report the incident to the Department of Social and Legal Protection of Children. He then has to solve the case. At the same time, in both cases, the director is also obliged to report such behavior to the public prosecutor's office, which will proceed within its competences.
• In more serious cases of cyberbullying (cyberbullying fulfills the factual essence of the crime), the school contacts the Police of the Czech Republic and the child social-legal protection authority.
• The school informs the affected pupils about the results of the investigation at the school and the punishments given.
• In the case of solving individual situations, you can also use the methodological tool of the Ministry of Education, Culture, Sports and Science containing anonymized cases and their solution options (http://www.msmt.cz/file/43418/download/).

If not:
The school cannot impose disciplinary punishments, or reduced marks for behavior for activities that did not occur during classes or as part of events organized and provided by the school, where the teacher supervises the students - during courses, excursions and other activities resulting from school educational programs or teaching documents, when participating in competitions, parades , or during their preparation and at other events organized by the school or school facility.

However, this does not mean that the school should not deal with cyberbullying at least in the following basic points:
• Find out which classes are involved in a cyberbullying incident. Then perform sociometry in all affected classes, which can reveal the presence of a risky communication phenomenon. Then proceed according to the elaborated crisis plan. Sociometric methods, where this is required, must be carried out by a trained professional.

Č.j.: MSMT–
32550/2017–1

	• Recommend the victim's parents to contact the Police of the Czech Republic, or filed a lawsuit in court. • Recommend parents to contact a specialized institution in the event of cyberbullying of their child (Safety Line, Children's Crisis Center, PPP, etc.). In more serious cases of cyberbullying (cyberbullying fulfills the factual nature of the crime), recommend that parents contact the Police of the Czech Republic and the child social-legal protection authority. • Inform affected pupils (with the consent of the adult pupil or the legal representative of the minor pupil) about the procedure for dealing with cyberbullying. Tell them that the school cannot punish in this case and therefore the case has been referred to the police/court. Children need to know that any inappropriate behavior will be punished.
When, whom and in what case to notify (parents, PPP, OSPOD, Police of the Czech Republic, etc.).	**The school has a reporting obligation when bullying occurs in the following cases (Ministry of Education, 2016a):** A. If bullying/cyberbullying occurs during classes, related activities or the provision of school services, the school is obliged to report this fact to the legal representative of both the student who was the attacker and the student who was the victim. This obligation follows from the Education Act (Section 21(2) of the Education Act, according to which the legal representatives of children and minor pupils have the right, among other things, to information about the progress and results of the child's or pupil's education and the right to comment on all decisions concerning the essential matters of their education). B. The school reports to the authority for the social and legal protection of children facts that indicate that the child is in danger either because someone else is threatening him or because he is endangering himself by his own behavior (see Sections 6, 7 and 10 of Act No. 359/1999 Coll., on social and legal protection of children, as amended (Act No. 359/1999 Coll., 2012)); in the case of bullying, this includes all cases that the school reported to the police or the public prosecutor, as well as cases that were not reported to the aforementioned even though something serious happened because there was no legal reason. C. If in connection with bullying there is an action that could fulfill the characteristics of a misdemeanor or a criminal act, the school contacts the Police of the Czech Republic. A criminal complaint can also be filed with the public prosecutor's office. The principal of the school or another authorized person shall report this fact in any form (in writing, by telephone, in person) to the Police of the Czech Republic, ideally directly to the youth specialist of the Criminal Police and Investigation Service, otherwise to the nearest district police department. In such a case, this person acts as the notifier and has the right to be notified within one month

	of submitting the notification. The notification can also be submitted by the child's legal representative.
	D. In case of a more serious level of bullying/cyberbullying, the school founder should also be informed.
Recommended links (Internet, literature, etc.)	The best is the help that is closest and can be the fastest. Try contacting a pedagogical-psychological counseling center, an educational care center or any psychologist in your place of residence. If you feel that no one is helping you, contact the school unions of the local self-government bodies or the Czech school inspectorate. **E-Bezpečí (www.e-bezpeci.cz)** – projekt zaměřený na prevenci rizikového chování na internetu (kyberšikana, kybergrooming, sexting, kyberstalking, sociální sítě, sociální inženýrstvi apod.). **Poradna E-Bezpečí (www.napisnam.cz)** – poradenská linka zaměřená na prevenci rizikového chování na Internetu, jen za letošní rok řešila pres 100 případů kyberšikany, stalkingu, sextingu apod. **Projekt E-Nebezpečí pro učitele (www.e-nebezpeci.cz)** – obsahuje řadu prezentací pro učitele. **Centrum prevence rizikové virtuální komunikace PdF UPOL (http://prvok.upol.cz)** – centrum realizující řadu projektů zaměřených na rizikové chování na internetu. Centrum realizuje výzkumy zaměřené na rizikové chování spojené s internetem a mobilními telefony. V sekci „Výzkum" jsou pravidelně zveřejňovány výsledky jednotlivých výzkumů. **Projekt Seznam se bezpečně (www.seznamsebezpecne.cz)** – projekt zaměřený na prevenci rizikového chování na internetu. Na stránkách je zřízen formulář pro dotazy týkající se nejrůznějších problémů spojených s on-line prostředím. **Linka bezpečí (www.linkabezpeci.cz)** – poradenská linka zaměřená na prevenci rizikového chování apod. **Bezpečně on-line (www.bezpecne-online.cz)** – stránky pro teenagery, rodiče a učitele s informacemi o bezpečném používání internetu, prevenci a řešení kyberšikany. **Dětské krizové centrum (www.ditekrize.cz)** – poradenství, pomoc v krizi. **Úřad pro ochranu osobních údajů (www.uoou.cz)** – institut zaměřený na ochranu osobních údajů, poradenství apod. **Minimalizace šikany MIŠ (www.minimalizacesikany.cz)** – praktické rady pro rodiče, učitele a děti, jak řešit šikanu a jak jí předcházet. **Poradna MIŠ (www.minimalizacesikany.cz/poradna)** – poradna zaměřená na problémy týkající se šikany a kyberšikany. **Projekt NNTB "Nenech to být" (www.nntb.cz)** – internetový systém a mobilní aplikace bojující proti šikaně a vylučování z kolektivu na školách po celé ČR. **Projekt Nebuď oběť! (www.nebudobet.cz)** – projekt zaměřený na rizika internetu a komunikačních technologií. **Projekt Internetem Bezpečně (www.internetembezpecne.cz)** – formou různorodých vzdělávacích aktivit klade za cíl zvýšit povědomí uživatelů o rizicích v internetovém prostředí.

<table>
<tr><td></td><td>

Společenství proti šikaně (www.sikana.org) – stránky občanského sdružení Společenství proti šikaně obsahují aktuality z oblasti šikany, související odkazy apod.
Projekt Saferinternet.cz (www.saferinternet.cz) – projet zaměřený na rizika internetu a komunikačních technologií.

Další doporučené odkazy:
Server Hoax.cz (www.hoax.cz) – cílem serveru je informovat uživatele internetu o poplašných, nebezpečných a zbytečných řetězových zprávách, tzv. hoaxů.

Materiály pro podporu výuky ke stažení (E-bezpečí) –
https://www.e-bezpeci.cz/index.php/component/content/article/7-o-proje
ktu/925-materialy

Publikace a osvětové materiály ke stažení (E-bezpečí) –
https://www.e-bezpeci.cz/index.php/ke-stazeni
Domácí webové stránky s tématikou šikany:
Internet poradna, **www.internetporadna.cz**
Amnesty International ČR, **www.amnesty.cz**

Další důležité dokumenty a odkazy on-line
- **[ZÁKON 561/2004 Sb.,](#)** o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon), ve znění pozdějších předpisů
- **[Vyhláška č. 48/2005 Sb.,](#)** o základním vzdělávání a některých náležitostech plnění povinné školní docházky
- **[Metodický pokyn](#)** ministryně školství, mládeže a tělovýchovy k prevenci a řešení šikany ve školách a školských zařízeních čj. MSMT-21149/2016
- **[Využití právních opatření](#)** při řešení problémového chování žáků na školách (MŠMT, 2014)
- **[Metodické doporučení](#)** MŠMT pro práci s Individuálním výchovným programem v rámci řešení rizikového chování žáků, č. j. MSMT-43301/2013
- **[Databáze](#)** všech certifikovaných poskytovatelů programů primární prevence rizikového chování
- **[Dítě v ohrožení](#)** – první pomoc pro pedagogy a vychovatele

</td></tr>
<tr><td>

Attachments

</td><td>

o **Annex No. 1 – Legislative framework**
o **The Education Act (Act 561/2004 Coll.)**
o **Criminal Code (Act 40/2009 Coll.)**
Crimes against freedom
• § 175 Blackmail
• § 176 Restriction of freedom of religion
Ϯ Criminal acts against the rights to the protection of personality, privacy and correspondence
• § 182 Violation of the confidentiality of transmitted messages
•   § 183 Violation of the secrecy of documents and other documents kept in private

</td></tr>
</table>

| | • § 184 Defamation
⌐ Crimes against human dignity in the sexual area
• § 191 Spreading pornography
• § 192 Production and other handling of child pornography
• § 193 Abuse of a child to produce pornography
• § 193b Establishing unauthorized contact with a child
⌐ Crimes against family and children
• § 201 Endangering the upbringing of a child
• § 202 Seduction to sexual intercourse
⌐ Crimes against property
• § 230 Unauthorized access to the computer system and information carrier
• § 231 Measures and storage of access device and password to the computer system and other such data
• § 232 Damage to a record in a computer system and on an information carrier and interference with computer equipment due to negligence
⌐ Crimes that are generally threatening
• § 287 Spread of drug addiction
⌐ Criminal acts disrupting the coexistence of people
• § 352 Violence against a group of residents and against an individual
• § 353 Dangerous threats
• § 354 Dangerous pursuit
• § 355 Defamation of a nation, race, ethnic or other group of persons
o • § 356 Inciting hatred towards a group of persons or restricting their rights and freedoms

o Civil Code (Act 89/2012 Coll.)
o Section 6 Personality of a person
o Chapter III, Part 1 Compensation for property and non-property damage
o Electronic Communications Act (127/2005 Coll.)
  § 67 Identification of malicious or harassing calls
o § 93 Misuse of the sender's electronic address
o Personal Data Protection Act (101/2000 Coll.)
o § 9 – § 11 Sensitive data
o § 44, paragraph 2, letter c
o § 44a, paragraph 3 |
| | **Appendix No. 2 – Recommended wording of the texts in the school regulations for the issue of bullying**
(Taken from the Minister's Methodological Instruction
of education, youth and physical education to prevent and solve bullying in schools and school facilities ref. MSMT-21149/2016)

Text related to the area of prevention, safe environment, risky behavior, etc. can appear in practically all chapters: |

• Rights and obligations of pupils and their legal representatives at school and details on the rules of mutual relations with teaching staff

• Operation and internal regime of the school

• Conditions for ensuring the safety and health protection of children (very well described in the publication: Miovský, M. et al. (2012). Proposal of the recommended structure of the MPP for the prevention of risky behavior for primary schools (Chapter 3). Prague: Klinika aktologie 1. LF UK)

• Conditions for handling school property or school facilities by pupils

• Rules for evaluating the results of pupils' education

• Conditions for ensuring the protection of pupils against risky behavior and against manifestations of discrimination, hostility or violence

Pro prevenci a řešení šikanování doporučujeme využít dvě z uvedených kapitol a pravidla pro hodnocení výsledků vzdělávání žáků (klasifikační řád).

1. Rights and obligations of pupils and legal representatives

In this chapter, it is possible to expand the existing ones or add completely new points mentioning the rights of pupils. Examples of specific text:

• To freely express his opinion in all matters that concern him; this opinion should be expressed in an adequate form, while due attention must be paid to it.

• Recommendation: Specify here specific persons according to the realities of the school, to whom you can direct your opinions - e.g. class teacher, school prevention methodologist, school psychologist, etc.

• To be protected from physical or psychological violence and negligent treatment.

• Recommendation: Also state the opposite point of view, i.e. no one has the right to harm another in any way.

• Ask for help or advice from any school staff – if the pupil feels any discomfort or has any distress.

• Recommendation: At the same time mention the obligation of school staff to always pay due attention to this.

• Compliance with the rules for the use of information communication technologies, the Internet and mobile phones (during lessons, during breaks, on the school premises) can be incorporated into the pupils' duties. It must not be forgotten to determine the penalties for non-compliance with these rules.

3. Conditions for ensuring the protection of pupils against risky behavior and against manifestations of discrimination, hostility or violence

In the chapter, it is possible to specify exactly the term bullying, incl. attitudes of the school. E.g.:

• Manifestations of bullying between pupils, i.e. physical violence, restriction of personal freedom, humiliation, misuse of

| | information |

technology to undermine dignity, etc., which anyone would commit against anyone (pupils and adults), are on school premises and during all school events and activities strictly prohibited and are considered a serious offense against school rules.

Recommendation: At the same time, inform that in case of such behavior the school proceeds according to the given school anti-bullying program (or according to internal strategic documents).

The educational committee is always convened, the legal representatives are informed and, according to the applicable laws, the school has a reporting obligation towards certain other institutions (such as the social-legal child protection authority, the Police of the Czech Republic, etc.)

4. Rules for evaluating the results of pupils' education (classification rules)

In the rules for evaluating the results of pupils' education (as part of the school rules), it is possible to specify for what, i.e. for what types of incorrect, intolerable or unacceptable behavior, the school grants appropriate educational measures. The enumeration can be very specific or more general. A description as specific as possible is recommended.

Recommendation: It is better to leave room for decisions about educational measures in specific cases.

Example wording:
Manifestations of bullying, i.e. targeted and repeated hurtful aggressive attacks, are considered gross violations of school rules. It can also include mild forms of psychological oppression that have been proven before and are repeated again.

The school principal decides on a specific educational measure after discussion in the educational committee and the pedagogical council. A reprimand, a reprimand from the class teacher (or a teacher of vocational training at a secondary school, a secondary vocational school), a reprimand from the school director, or conditional suspension and expulsion from school.

6.2   Statutory Guidance (UK)

As an international school in the Czech Republic, [PHBS] is not bound by UK-laws. However, an interpretation of Department of Education policy, guidance and advice is applied to [PHBS] in a "best fit" scenario. Below are some examples of UK policies (please know that the guidance and education given by [PHBS] is not restricted to the documents please - they are presented in this policy as "sample guidance").

The following DofE documents and policies are important in the above context:

(6.2.3) Searching, Screening & Confiscation: Advice for School (July 2022)

Full policy document link: https://tinyurl.com/zjrez6vm

The above document specifically outlines guidance for confiscation of personal devices (reference to as 'electronic devices'. Specifically:

(Electronic Devices | para. 72) Electronic devices, including mobile phones, can contain files or data which relate to an offence, or which may cause harm to another person. This includes, but is not limited to, indecent images of children, pornography, abusive messages, images or videos, or evidence related to suspected criminal behaviour.

(Electronic Devices | para. 73) As with all prohibited items, staff should first consider the appropriate safeguarding response if they find images, data or files on an electronic device that they reasonably suspect are likely to put a person at risk.

(6.2.4) Behaviour in Schools: Advice for Headteachers & School Staff (September 2022)

Full policy document link: https://tinyurl.com/23bzsjrr

Perrott Hill British School refers specifically to the revised guidance released by the Department of Education, which believes that "pupils should be taught explicitly what good behaviour looks like" in schools, and that staff should define "the expected behaviours in school, rather than only a list of prohibited behaviour".

Page 34 (Behaviour in Schools, September 2022)

(Mobile Phones | para. 122) Headteachers should decide if mobile phones can be used during the school day. Many pupils, especially as they get older, will have one of their own. Allowing access to mobile phones in school introduces complexity and risks, including distraction, disruption, bullying and abuse, and can be a detriment to learning. Headteachers should consider restricting and prohibiting mobile phones to reduce these risks.

(6.2.5) Sharing Nudes & Semi-Nudes: Advice for Education Settings Working With Children & Young People (December 2022)

Full website guidance link: https://tinyurl.com/5s6dree5

(1.4 'Sharing nudes and semi-nudes': definition) This advice uses the term 'sharing nudes and semi-nudes' to mean the sending or posting of nude or semi-nude images, videos or live streams by young people under the age of 18 online. This could be via social media, gaming platforms, chat apps or forms. It could also involve sharing between devices like Apple's AirDrop which works offline.

The term 'nudes' is used as it is most commonly recognised by young people and more appropriately covers all types of image sharing incidents. Alternative terms used by children and young people may include 'dick pics' or 'pics'.

The motivations for taking and sharing nude and semi-nude images, videos and live streams are not always sexually or criminally motivated. Such images may be created and shared consensually by young people who are in relationships, as well as between those who are not in a relationship. It is also possible for a young person in a consensual relationship to be coerced into sharing an image with their partner. Incidents may also occur where:

- children and young people find nudes and semi-nudes online and share them claiming to be from a peer

- children and young people digitally manipulate an image of a young person into an existing nude online

- images created or shared are used to abuse peers e.g. by selling images online or obtaining images to share more widely without consent to publicly shame

The sharing of nudes and semi-nudes can happen publicly online, in 1:1 messaging or via group chats and closed social media accounts.

Nude or semi-nude images, videos or live streams may include more than one child or young person.

Creating and sharing nudes and semi-nudes of under-18s (including those created and shared with consent) is illegal which makes responding to incidents involving children and young people complex. There are also a range of risks which need careful management from those working in education settings.

(6.2.6) Cyberbullying: Advice for Headteachers and School Staff

Full policy document link: https://tinyurl.com/59h7acbz

(Overview) All forms of bullying (including cyberbullying) should be handled as a community issue for the whole school. It is important that schools take measures to prevent and tackle bullying among pupils. But it is equally important that schools make it clear that bullying of staff, whether by pupils, parents or colleagues, is unacceptable. Evidence indicates that one in five (21%) teachers have reported having derogatory comments posted about them on social media sites from both parents and children.

School leaders, teachers, school staff, parents and pupils all have rights and responsibilities in relation to cyberbullying and should work together to create an environment in which pupils can learn and develop and staff can have fulfilling careers free from harassment and bullying.

Schools can offer support to parents on how to help their children engage safely and responsibly with social media, perhaps through a parents' evening, advice in a school newsletter or signposting to other sources of support and advice. Creating a good school-parent relationship can help create an atmosphere of trust that encourages parents to raise concerns in an appropriate manner. Part of this is making sure that parents and carers are aware and understand how to communicate with the school. Schools should also make clear that it is not acceptable for pupils, parents or colleagues to denigrate and bully school staff via social media in the same way that it is unacceptable to do so face to face.

Schools should encourage all members of the school community including parents to use social media responsibly. Parents have a right to raise concerns about the education of their child, but they should do so in an appropriate manner.

(6.2.7) Keeping Children Safe in Education (September, 2002)

Full policy document link: https://tinyurl.com/59h7acbz

Page 104/105/106 (Part Five: Child-on-Child Sexual Violence & Sexual Harrassment)

(Sexual harrassment | para. 452) When referring to sexual harrassment we mean 'unwanted conduct of a sexual nature' that can occur online and offline and both inside and outside of school/college. When we reference sexual harrassment, we do so in the context of child-on-child sexual harrassment. Sexual harrassment is likely to: violate a child's dignity, and/or make them feel intimidated, degraded or humiliated and/or create hostile, offensive or sexualized environment.

(Sexual harrassment | para. 453) Whilst not intended to be an exhausative list, sexual harrassment can include:

- sexual comments, such as: telling sexual stories, making lewd comments, making sexual remarks about clothes and appearance and calling someone sexualised names

- sexual "jokes" or taunting

- physical behaviour, such as: deliberately brushing against someone, interfering with someone's clothes. Schools and colleges should be considering when any of this crosses a line into sexual violence - it is important to talk to and consider the experience of the victim.

- displaying pictures, photos or drawings of a sexual nature

- upskirting (this is a criminal offence138), and

- online sexual harassment. This may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence

  - o sharing of unwanted explicit content

  - o sexualised online bullying

  - o unwanted sexual comments and messages, including, on social media

  - o sexual exploitation; coercion and threats, and

  - o coercing others into sharing images of themselves or performing acts they're not comfortable with online.