



## eSafety Label - Action Plan for: ОУ "Христо Смирненски"

Формулярът за оценка е подаден от: Deyana Peykova - 2014-11-28 17:41:38

С подаването на Формуляра за оценка Вие направихте важна стъпка в посока по-доброто разбиране на ситуацията във Вашето училище. Планът за действие съдържа допълнителна информация и насоки в три ключови области: инфраструктура, политики и практики.

### Техническа сигурност

- Чудесно е, че всички компютри от училищната мрежа имат антивирусна защита. Уверете се, че сте включили защитата от вируси в правилата за употреба, за да се уверите, че всички са запознати с необходимите мерки. Разгледайте информационните брошури на тема *Защита на Вашите устройства от злонамерен софтуер* на [www.esafetylabel.eu/group/teacher/protecting-devices-against-malware](http://www.esafetylabel.eu/group/teacher/protecting-devices-against-malware).
- Имате разграничени нива на филтриране, което е отлична политика. Една добра политика трябва редовно да се актуализира – така ли е във вашия случай? Колко често има молби за блокиране или отблокиране на сайтове? Съобразете дали това е продуктивно и ангажирайте всички заинтересовани страни. Имайте предвид, че ключът към безопасното и отговорно онлайн поведение е педагогическият подход с цел изграждане на умения за онлайн безопасност у учениците. Организирайте среща с всички учители и обсъдете как всеки да говори със своите ученици как да бъдат добри и защитени граждани на дигиталното пространство. Разгледайте [www.paneuyouth.eu](http://www.paneuyouth.eu) за примерни дискусии по темата, които да осъществите чрез ролеви или групови игри.

### Достъп на ученици и учители до технологиите

- Щом потребителите могат да използват USB устройства само с разрешение, това налага учителят/координаторът по ИКТ да бъде обучен да осигурява безопасната им употребата. Това така ли е при Вас? За да поддържате системата защитена, трябва да заложите основни насоки в правилата за употреба. Разгледайте информационната брошура на тема *Употреба на външни устройства* на [www.esafetylabel.eu/group/teacher/removable-devices](http://www.esafetylabel.eu/group/teacher/removable-devices), за да се уверите, че покривате всички изисквания за безопасност.
- Има ясни преимущества и за училищния колектив, и за учениците, когато могат да използват лични устройства в училище. Това обогатява техническото оборудване, което е на разположение в училище, служи като важна връзка между обучението у дома и това в училище, а е и начин за възпитаване на младежите в отговорна употреба. Важно е, когато употребяват лични устройства в училищната мрежа, и училищният колектив, и учениците да разбират добре коя мрежа да ползват и защо. Тази информация трябва да е включена в Правилата за употреба с ясни насоки какво е позволено при употреба на училищната мрежа и какво не е.

### Защита на личните данни

- Добре е, че имате отделни сървъри за образователни и административни нужди. Уверете се, че училищният колектив е подготвен да управлява тези бази. Споделете своя правилник с други училища, като го качите на училищния си профил в платформата.
- Паролите предлагат уникален метод за вход в училищната компютърна система и има основни правила, които трябва стриктно да се прилагат. За допълнително информация прочетете информационната брошура

на тема *Надеждни пароли* на [www.esafetylabel.eu/group/teacher/safe-passwords](http://www.esafetylabel.eu/group/teacher/safe-passwords).

Допълнете правилата за употреба с информация за паролите и избягвайте употребата на стандартни пароли за новите потребители.

## Програмни лицензи

- Важно е всички нови членове на училищния колектив да се запознаят с политиката за инсталиране на нови компютърни програми. Това ще означава, че сигурността на Вашите системи се контролира, а училищният колектив може да използва нови софтуерни приложения, които да подпомагат образователния процес.
- Погрижете се целият училищен колектив да е запознат с процедурите за купуване на нов софтуер и лицензите да отговарят на броя ученици и служители, които ще ги ползват. Разделът [Потребителски лиценз](#) в Уикипедия, съдържа полезна информация за условията на различните софтуерни споразумения.

## Управление на ИКТ

- Погрижете се лицето, което отговаря за компютърните мрежи, да бъде запознато с компютърните програми, които са инсталирани на училищните устройства. Това трябва да бъде посочено в училищния правилник и в правилата за ползване. Лицето, отговорно за мрежата, трябва да може да гарантира, че всички продукти са лицензирани и че няма потенциален конфликт между работата в мрежа и индивидуалната работа на всяко устройство.
- Чудесно е, че имате система за обновяване на софтуера, която се контролира централно. Възможно ли е мениджърът по ИКТ да напише кратък наръчник за обновяване на софтуера, който да качите на профила на училището? Това ще е много полезно на другите училища.

## Правилник за употреба на ИКТ

- Наличието на правилник за употреба на ИКТ за учениците е похвално. Трябва да го разширите, за да обхваща училищния колектив и по-широката училищна общност. Уверете се, че разширеният правилник е пълен, като разгледате информационната брошура и списъка с препоръчителни елементи на [Правилник за употреба](#) на [www.esafetylabel.eu/group/teacher/acceptable-use-policy](http://www.esafetylabel.eu/group/teacher/acceptable-use-policy).
- Редовно преглеждайте наредбата за мобилни телефони, за да се уверите, че е актуална и че се спазва. Информационните брошури на тема *Употреба на мобилни телефони в училище* ([www.esafetylabel.eu/group/teacher/mobile-phones](http://www.esafetylabel.eu/group/teacher/mobile-phones)) и *Училищен правилник* ([www.esafetylabel.eu/group/teacher/school-policy](http://www.esafetylabel.eu/group/teacher/school-policy)) предлагат допълнителна информация.

## Докладване на инциденти и справяне с тях

- Запознат ли е всеки член на училищния колектив с процедурата за справяне с потенциално незаконно съдържание? Определен ли е човек от ръководния екип, който поема пълна отговорност при такива ситуации? Процедурата трябва добре да се разясни на преподавателите в училищния правилник и на учениците и преподавателите в правилата за употреба. Докладвайте при опасения за незаконно съдържание на Вашата национална интернет-гореща линия ([web112.net](http://web112.net)).
- Уверете се, че училищният колектив, включително новите членове, са запознати с процедурата за действие при наличие на незаконно съдържание на някои от училищните компютри. Уверете се, че правилникът се прилага безкомпромисно. Това трябва да се следи от представител на училищното ръководство.

## Правилник за училищния екип

- Нужно е да се съставят насоки за допустимото онлайн поведение на учителския колектив. Това е тема, която трябва редовно да се обсъжда на учителски срещи, да бъде включена в училищния правилник и правилата за употреба. Редовно преглеждайте и при нужда обновявайте и двата документа.
- Употребата на лични мобилни устройства по време на час носи своите рискове. Обмислете аргументите

училищният колектив да използва свои лични устройства и, ако е уместно, осигурете училищно устройство. Посъветвайте учителите да се запознаят с информационната брошура *Употреба на мобилни телефони в училище* ([www.esafetylabel.eu/group/teacher/mobile-phones](http://www.esafetylabel.eu/group/teacher/mobile-phones)) и се уверете, че насоките за училищния колектив са включени в училищния правилник.

## Поведение и навици на учениците

- В правилата за употреба на ИКТ трябва да бъдат включени насоки за допустимата електронна комуникация между учениците. Липсата на ясни стандарти може да доведе до увеличаване на случаите на онлайн насилие и тормоз между връстниците. Обучение по пълноценно и отговорно общуване трябва да се включи в училищната програма, защото това е необходимо умение за всеки млад човек. Обсъдете това на учителски срещи, за да приемете единни стандарти, които да въведете.
- В училището трябва да съществува система за поощряване на позитивното поведение и санкциониране на негативното, която да се отнася както за онлайн ситуациите, така и за взаимоотношенията в реалния живот. Всички членове на училищната общност трябва да бъдат въввлечени в процеса на създаването на такава система и трябва да поемат ангажимент да я съблюдават.

## Присъствие на училището в интернет

- Разгледайте информационната брошура *Заснемане и публикуване на снимки и видео записи в училище* ([www.esafetylabel.eu/group/teacher/photos-videos](http://www.esafetylabel.eu/group/teacher/photos-videos)) за да се уверите, че училищният правилник покрива всичко и публикувайте съответния текст на профила на Вашето училище *Моето училище*, за да може и други училища да използват Вашата добра практика.
- Редовно проверявайте съдържанието в профилите на училището Ви в социалните медии, за да се уверите, че няма неподходящи коментари. Опитвайте се да актуализирате информацията често. Повече информация можете да намерите в информационната брошура *Училищата в социалните мрежи* ([www.esafetylabel.eu/group/teacher/social-networks](http://www.esafetylabel.eu/group/teacher/social-networks)). Допитайте се до потребителите дали смятат, че профилът и информацията, която се публикува там, са полезни.

## Управление на онлайн безопасността

- Освен ясно разпределени отговорности, което е гаранция, че всички защити на системата и всички проверки за защита на потребителя са в изправност, е важно училищата редовно да извършват одит и проверки. Без тях училището ще стане уязвимо. Разгледайте информационните ни брошури на тема *Училищен правилник* at [www.esafetylabel.eu/group/teacher/school-policy](http://www.esafetylabel.eu/group/teacher/school-policy). Трябва винаги да има отговорник за онлайн безопасността, но както Вие, така и всеки в училището следва да споделя обща отговорност да защитава всяка „чувствителна“ информация, която използва при изпълнение на ежедневните си задължения. Дори лица, чиито задължения не са пряко свързани с ползване на данни, трябва да се запознаят с рисковете и мерките за сигурност. Използвайте нашата информационна брошура *Правилник за употреба*, ([www.esafetylabel.eu/group/teacher/acceptable-use-policy](http://www.esafetylabel.eu/group/teacher/acceptable-use-policy)) за да се уверите, че всеки познава мерките за безопасност и отговорно поведение в интернет.
- Обмислете варианта за избор на представител на администрацията или на училищното настоятелство, който да координира програмата за онлайн безопасност и пред когото да докладвате броя и типа инциденти, с които се сблъсквате, веднъж в годината. Използвайте тази информация, за да актуализирате училищния правилник. Разгледайте нашата информационна брошура *Училищен правилник* [www.esafetylabel.eu/group/teacher/school-policy](http://www.esafetylabel.eu/group/teacher/school-policy).

## Онлайн безопасността в учебния план

- Добре е, че обучението по онлайн безопасност е включено в учебния план. Погрижете се всеки член на училищния колектив да развива уменията по онлайн безопасност на учениците във всеки подходящ момент дори извън часовете по ИКТ и тези по лична, социална и здравна култура. Можете да откриете полезни идеи и източници в информационната брошура *Онлайн безопасността - част от учебния план* at [www.esafetylabel.eu/group/teacher/esafety-in-curriculum](http://www.esafetylabel.eu/group/teacher/esafety-in-curriculum).

- Опитвайте се да предлагате информация по онлайн безопасност, която е актуална и има отношение към нуждите на учениците. Опитвайте се да надграждате познанията на учениците, като се съобразявате с нивото на опит и предпочитаните средства, които използват.

### Извънкласни занимания

- Чудесно е, че оказвате подкрепа на учениците и извън учебната програма. Споделете казусите, с които се сблъсквате, на платформата, за да запознаете и другите училища. От голяма полза може да бъде намесата ви в конкретни случаи, като промяна на настройките на профил, изтриване на снимка, докладване и други. Повече информация можете да намерите в информационната брошура *Ученици използват онлайн технологии извън училище* на [www.esafetylabel.eu/group/teacher/social-media-pupils](http://www.esafetylabel.eu/group/teacher/social-media-pupils).
- Споделете наблюденията си върху навиците и поведението на учениците в платформата. Например можете да публикувате резултатите от скорошни анкети в профила на Вашето училище в секцията [Моето училище](#).

### Източници на подкрепа

- Педагогическите съветници, медицинските сестри и други членове на екипа извън преподавателския състав, могат да предложат съвети и насоки по тези въпроси, да участват при съставянето и при редовното преглеждане на училищния правилник. Преценете дали е възможно да им осигурите обучение.
- Чудесна практика е да предоставяте съвет и подкрепа на родителите. Предоставяйте информация за всички родители на сайта на училището или чрез училищния бюлетин. Възможно е да организирате и вечер за информиране на родителите. Разгледайте информационната брошура *Информация за родители* на [www.esafetylabel.eu/group/teacher/info-for-parents](http://www.esafetylabel.eu/group/teacher/info-for-parents) за допълнителни идеи.

### Обучение за учители

- Екипът трябва да се информира за тенденциите в поведението на децата онлайн. Анализирайте обучителните нужди на училищния колектив и се запознайте с възможностите за обучение [www.esafetylabel.eu/group/teacher/esafety-training-courses](http://www.esafetylabel.eu/group/teacher/esafety-training-courses).
- Всички учители трябва да могат да разпознават признаците за онлайн тормоз и да знаят как да постъпят в такива ситуации. Уверете се, че учителите са запознати с начина, по който учениците използват новите технологии злонамерено. Разгледайте и информационната брошура *Онлайн тормоз* на [www.esafetylabel.eu/group/teacher/cyberbullying](http://www.esafetylabel.eu/group/teacher/cyberbullying).

Формата за оценка, която подадохте, е автоматично генерирана извадка от множество въпроси. За нас ще бъде много полезно, ако ни разкажете за работата си в други области на онлайн безопасността, които не са засегнати в този въпросник. Сведения за такива дейности можете да качите тук: [Качи доказателства](#) в секцията [Моето училище](#). Не забравяйте, че попълването и подаването на формата за оценка е само част от процеса по акредитация. Доказателствата, които качвате, контактите ви с другите във [форума](#), както и активното [докладване на инциденти](#), също имат роля в процеса.