ВЪТРЕШНИ ПРАВИЛА

на ОУ "Христо Ботев"

за мерките за защита на личните данни съгласно Регламент 2016/679

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) ОУ "Христо Ботев" е юридическо лице и е регистрирано по Закона за регистър БУЛСТАТ с БУЛСТАТ: 000182154, със седалище в с. Глава община Червен бряг област Плевен ул. "Христо Ботев" 1.

(2) Когато ОУ "Христо Ботев" обработва лични данни във връзка със своята дейност и само определя целите и средствата за обработването им действа като администратор на лични данни.

(3) В случаите, в които ОУ "Христо Ботев" обработва лични данни за цели, определени самостоятелно от трето лице или целите са определени съвместно от ОУ "Христо Ботев" и трето лице, ОУ "Христо Ботев" има положението съответно на обработващ лични данни или на съадминистратор.

Чл. 2. Настоящите Вътрешни правила на ОУ "Христо Ботев" уреждат организацията на обработване и защитата на лични данни на ученици и техните родители/настойници, на работниците/служителите (включително и на кандидатите за работа), на контрагентите и партньорите на ОУ "Христо Ботев", както и на всички други групи физически лица, с които влиза в отношения при осъществяването на правомощията и дейността си.

Чл. 3.(1) „Лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни"); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

(2) „Обработване на лични данни“ означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване.

(3) „Регистър с лични данни“ представлява всеки структуриран набор от лични данни, независимо от неговия вид и носител, достъпът до които се осъществява съгласно определени критерии.

Чл. 4.(1) ОУ "Христо Ботев" е администратор на лични данни по смисъла на чл. 4, т. 7 от Общия регламент относно защитата на данните (ЕС) 2016/679.

(2) Като администратор на лични данни, при обработването на лични данни ОУ "Христо Ботев" спазва принципите за защита на личните данни, предвидени в Общия регламент относно защитата на данните (ЕС) 2016/679 и законодателството на Европейския съюз и Република България.

Чл. 5. Принципите за защита на личните данни са:

1. ***Законосъобразност, добросъвестност и прозрачност*** - обработване при наличие на законово основание, при полагане на дължимата грижа и при информиране на субекта на данни;
1. ***Ограничение на целите*** – събиране на данни за конкретни, изрично указани и легитимни цели и забрана за по-нататъшно обработване по начин, несъвместим с тези цели;
2. ***Свеждане на данните до минимум*** – данните да са подходящи, свързани със и ограничени до необходимото във връзка с целите на обработването;
3. ***Точност*** – поддържане в актуален вид и предприемане на всички разумни мерки за гарантиране на своевременно изтриване или коригиране на неточни данни, при отчитане на целите на обработването;
4. ***Ограничение на съхранението –*** данните да се обработват за период с минимална продължителност съгласно целите. Съхраняване за по-дълги срокове е допустимо за целите на архивирането в обществен интерес, за научни или исторически изследвания или статистически цели, но при условие, че са приложени подходящи технически и организационни мерки;
5. ***Цялостност и поверителност –*** обработване по начин, който гарантира подходящо ниво на сигурност на личните данни, като се прилагат подходящи технически или организационни мерки;
6. ***Отчетност –*** администраторът носи отговорност и трябва да е в състояние да докаже спазването на всички принципи, свързани с обработването на лични данни.

Чл. 6. (1) Личните данни се събират за конкретни, точно определени от закона цели, обработват се законосъобразно и добросъвестно и не могат да се обработват допълнително по начин, несъвместим с тези цели

(2) Личните данни се съхраняват на хартиен, технически и/или електронен носител, само за времето, необходимо за изпълнение на задълженията на ОУ "Христо Ботев" .

Чл. 7. Когато не са налице хипотезите на чл. 6, § 1, б. „б“ – „ е“ от Регламент 2016/679, физическите лица, чиито лични данни се обработват от ОУ "Христо Ботев", подписват декларация за съгласие, в която свободно, конкретно, информирано и недвусмислено изразяват своето съгласие за обработване. В тези декларации са описани видовете данни, целите, за които се изискват и сроковете им за съхранение.

Чл. 8. ОУ "Христо Ботев" организира и предприема мерки за защита на личните данни от случайно или незаконно унищожаване, от неправомерен достъп, от изменение или разпространение както и от други незаконни форми на обработване на лични данни. Предприеманите мерки са съобразени със съвременните технологични достижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

Чл. 9. (1) При регистриране на неправомерен достъп до информационните масиви за лични данни, или при друг инцидент, нарушаващ сигурността на личните данни, служителят, констатирал това

нарушение/инцидент, незабавно докладва за това на прекия си ръководител, който от своя страна е длъжен, своевременно да информира Длъжностното лице по защита на данните за инцидента. Уведомяването за инцидент се извършва писмено, по електронен път или по друг начин, който позволява да се установи извършването му и да се спази изискването за уведомяване на Комисията за защита на личните данни в срок от 72 часа от узнаването за инцидента.

(2) Процесът по докладване и управление на инциденти задължително включва регистрирането на инцидента, времето на установяването му, лицето, което го докладва, лицето, на което е бил докладван, последствията от него и мерките за отстраняването му.

Чл. 10. ОУ "Христо Ботев" прилага адекватна защита на личните данни, която включва:

1. Физическа защита (система от технически и организационни мерки);
1. Персонална защита (система от организационни мерки);
2. Документална защита (система от организационни мерки);
3. Защита на автоматизирани информационни системи и мрежи (система от технически и организационни мерки);

II. МЕРКИ ПО ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 11. ***Физическата защита*** в ОУ "Христо Ботев" се осигурява чрез набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на помещенията, в които се извършват дейности по обработване на лични данни.

Чл. 12. (1). Основните ***организационни мерки за физическа защита*** в ОУ "Христо Ботев" включват:

1. определяне на помещенията, в които ще се обработват лични данни;
2. определяне на помещенията, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни;
3. определяне на организацията на физическия достъп.

(2) Като *помещения, в които ще се обработват лични данни,* се определят всички помещения, в които с оглед нормалното протичане на работния процес, се събират, обработват и съхраняват лични данни. Достъпът до тях е физически ограничен и контролиран – само за служители с оглед изпълнение на служебните им задължения и ако мястото им на работа или длъжностната им характеристика позволява достъп до съответното помещение и съответния регистър с лични данни. Когато в тези помещения имат достъп и външни лица, в помещенията се обособява „непублична“ част, в която се извършват дейностите по обработване на лични данни, която е физически ограничена и достъпна само за служители, на които е необходимо да имат достъп с оглед на изпълнението на служебните им задължения, и „публична част“ – до която имат достъп външни лица и в която не се извършват дейности по обработване, включително не се съхраняват данни, независимо от техния носител.

(3) *Комуникационно-информационните системи, използвани за обработка на лични данни, се разполагат в специални физически защитени помещения или защитени шкафове*, достъпът до които е ограничен само до тези служители, които за изпълнение на служебните си задължения се нуждаят от такъв достъп до данните, както и лицата, натоварени със служебни ангажименти за поддръжката на нормалното функциониране на тези системи. Последните нямат достъп до съхраняваните в електронен вид данни.

(4) *Организацията на физическия достъп до помещения*, в които се извършват дейности по обработка на лични данни, е базирана на ограничен физически достъп (на база заключващи системи и механизми) до зоните в обекта с ограничен достъп, включително и тези, в които са намират информационните системи. Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения.

(5) Зони с контролиран достъп са всички помещения на територията на ОУ "Христо Ботев", в които се събират, обработват и съхраняват лични данни.

Чл. 13. (1). Основните ***технически мерки за физическа защита*** в ОУ "Христо Ботев" включват:

1. използване на ключалки и заключващи механизми;
1. шкафове, метални каси;
2. оборудване на помещенията;
3. пожарогасителни средства.

(2) *Използваните технически средства за физическа защита* на личните данни в ОУ "Христо Ботев" са съобразени с нивото на риска и нивото на въздействие на тези данни за правата и свободите на физическите лица.

(3) Документите, съдържащи лични данни, се съхраняват в *шкафове или картотеки, които могат да се заключват*, като последните са разположени в зони с ограничен (контролиран) достъп. Ключ за шкафовете притежават единствено изрично натоварените лица (с изрична заповед или по силата на служебните им задължения и длъжностната характеристика).

(4) *Оборудването на помещенията*, където се събират, обработват и съхраняват лични данни, включва: сигнално - охранителна техника, *ключалки* (механични или електронни) за ограничаване на достъпа единствено от оторизираните лица; заключваеми шкафове и пожарогасителни средства.

(5) *Пожарогасителните средства* се разполагат в съответствие с изискванията на приложната нормативна уредба.

Чл. 14. (1) Основните ***организационни мерки за персонална защита*** на личните данни, приложими в ОУ "Христо Ботев", са:

1. познаване на нормативната уредба в областта на защитата на личните данни;
2. знания за опасностите за личните данни, обработвани от администратора;
3. съгласие за поемане на задължение за неразпространение на личните данни.

(2) Задължение на служителите да преминат обучение и да се запознаят с нормативната уредба в областта на защитата на лични данни и настоящите Вътрешни правила, като преминатото обучение и инструктаж с правилата за защита на личните данни се удостоверява с подпис върху протокол за извършен инструктаж за защита на личните данни по образец (Приложение № 4);

(3) Запознаване и осъзнаване за опасностите за личните данни, обработвани от ОУ "Христо Ботев";

(4) Забрана за споделяне на критична информация (идентификатори, пароли за достъп и др.п.) между персонала и всякакви други лица, които са неоторизирани;

(5) Служителите преминават задължителен инструктаж за запознаване с правилата за Противопожарна безопасност най-малко веднъж годишно. За проведения инструктаж се съставя Протокол по образец, съгласно Приложение № 1. С оглед защита на хартиените, техническите и информационните ресурси всички служители са длъжни да спазват правилата за противопожарна безопасност.

(6) Деклариране на съгласие за поемане на задължение за неразпространение на личните данни.

Чл. 15. (1)**.** Основните ***организационни мерки за документална защита*** на личните данни, са:

1. Определяне на регистрите, които ще се поддържат на хартиен носител;
2. Определяне на условията за обработване на лични данни (вкл. архивиране);
3. Регламентиране на достъпа до регистрите с лични данни;
4. Определяне на срокове за съхранение;
5. Процедури за унищожаване:

(2) На хартиен носител се съхраняват всички лични данни, които изискват попълването им върху определени бланкови документи и/или формуляри, свързани с изпълнение на изисквания на действащото законодателство или пряко свързани с осъществяването на нормалната дейност на ОУ "Христо Ботев", сключване на договори, изпълнение на договори, упражняване на предвидени в закона права и установени от закона задължения;

(3) Личните данни се събират и обработват само с конкретна цел, пряко свързана с изпълнение на законовите задължения и/или нормалната дейност на ОУ "Христо Ботев", а начинът на тяхното съхранение се съобразява със специфичните нужди за обработка и физическия носител на данните;

(4) Документите, по които работата е приключила, се архивират.

Трайното съхраняване за нуждите на архивирането на документи, съдържащи лични данни, се извършва на хартиен носител в помещения, определени за архив, за срокове, съобразени с действащото законодателство. Помещенията, определени за архив, са оборудвани с пожарогасители, със системи за контрол на достъпа и задължително се заключват.

(5) Право на достъп до регистрите с лични данни и архивираните документи имат оторизираните служители на ОУ "Христо Ботев". Оторизирането на служители се извършва на база длъжностна характеристика. Служителите носят отговорност за осигуряване и гарантиране на регламентиран достъп до служебните помещения и опазване на регистрите, съдържащи лични данни. Всяко умишлено нарушение на правилата и ограниченията за достъп до личните данни от персонала може да бъде основание за налагане на дисциплинарни санкции по отношение на съответните служители.

(6) Достъп на външни лица (напр. НАП, НОИ и др.п.) до лични данни се предоставя единствено, ако те имат право на такъв достъп, съгласно действащото законодателство, след подаване на искане за достъп на информация, и след тяхното легитимиране. Решението си за предоставяне или отказване на достъп до лични данни за съответното лице, ОУ "Христо Ботев" съобщава в 1-месечен срок от подаване на искането. Информацията може да бъде предоставена под

формата на устна справка, писмена справка, преглед на данните от самото лице, предоставяне на исканата информация на технически и/или електронен носител.

(7) Личните данни се съхраняват не по-дълго от колкото е необходимо, за да се осъществи целта, за която са били събрани или до изтичане на определения в действащото законодателство срок;

(8) Най-малко веднъж годишно се извършват периодични проверки за състоянието и целостта на личните данни, съдържащи се в обработваните от ОУ "Христо Ботев" регистри. Проверките се извършват от комисия, включваща служители на ОУ "Христо Ботев", които изготвят Доклад за резултата от проверката, който трябва да включва преценка на необходимостта за обработка на личните данни или унищожаване. Докладите се адресират до Длъжностното лице по защита на данните и до Директора на ОУ "Христо Ботев".

(9) Документите, съдържащи лични данни, сроковете за съхранение на които са изтекли и не са необходими за нормалното функциониране на ОУ "Христо Ботев" или за установяването, упражняването или защитата на правни претенции, се унищожават по подходящ начин, изключващ възстановяването на данните и злоупотребата с тях (напр. изгаряне, нарязване). Унищожаване се осъществява от служители, упълномощени с изричен писмен акт на Директора на ОУ "Христо Ботев" и след уведомяване на Длъжностното лице по защита на данните. За извършеното унищожаване на лични данни и носители на лични данни се съставя Протокол, съгласно образец, представляващ ***Приложение № 2***.

Чл. 16. ***Защитата на автоматизираните информационни системи и/или мрежи*** в ОУ "Христо Ботев" включва набор от приложими организационни и технически мерки за предотвратяване на нерегламентиран достъп до системите и/или мрежите, в които се създават, обработват и съхраняват лични данни.

Чл. 17. (1)**.** Основните ***организационни мерки за защитата на автоматизираните информационни системи и/или мрежи***, са:

1. Персонална защита;
2. Определяне на срокове за съхраняване на личните данни;
3. Процедура за унищожаване / заличаване / изтриване на носители;

(2) Компютърен достъп през локалната мрежа към файлове, съдържащи лични данни, се осъществява само от длъжностни лица с регламентирани права, единствено от тяхното физическо работно място, от специално определения за целта компютър и след идентификация чрез име и парола към системата. При приключване на работното време служителите изключват локалния си компютър.

(3) ОУ "Христо Ботев" прилага адекватни мерки за технически и административен контрол (уникално потребителско име и парола, настройка на всички работни станции в режим „автоматично заключване на екрана“ при липса на активност), като по този начин гарантира, че само упълномощени служители получават достъп до данните за изпълнение на възложените им функции.

(4) Потребителският акаунт се заключва след три неуспешни опита за регистрация в системата, а неговото отключване може да бъде извършено само от системния администратор.

(5) С цел повишаване сигурността на достъпа до информация служителите задължително променят използваните от тях пароли на определен период, не по-дълъг от 3 месеца. В случай на отпадане на основанието за достъп до лични данни правата на съответните лица се преустановяват (вкл. и чрез изтриване на акаунта).

(6) При необходимост от ремонт на компютърната техника, предоставянето ѝ на сервизната организация се извършва без устройствата, на които се съхраняват лични данни или след подписване на писмено споразумение (***Приложение № 3***), че сервизната организация ще предприеме и поддържа необходимите технически и организационни мерки за защита срещу неразрешено или незаконосъобразно обработване на личните данни, срещу случайна загуба, унищожаване или повреждане на лични данни. Сервизната организация да гарантира, че служителите и подизпълнителите, които извършват ремонта, са обвързани със задължение за поверителност по отношение на обработването на лични данни и че са преминали необходимото обучение за спазване изискванията на законодателството за защита на личните данни

(7) Служителите, на които е възложено да подписват служебна кореспонденция с квалифициран електронен подпис (КЕП), нямат право да предоставят издадения им КЕП на трети лица, респ. да споделят своя PIN с трети лица.

(8) Публикуването на служебна информация в Интернет, независимо под каква форма и на каква платформа, се извършва единствено след писмена оторизация от Ръководството на ОУ "Христо Ботев".

(9) *Личните данни в електронен вид се съхраняват* съгласно нормативно определените срокове и съобразно спецификата и нуждите на ОУ "Христо Ботев".

(10) Данните, които вече не са необходими за целите на ОУ "Христо Ботев" и чийто срок за съхранение е изтекъл, се *унищожават чрез приложим способ* (напр. чрез трайно изтриване, вкл. презаписването на електронните средства или физическо унищожаване на носителите).

Чл. 18. (1)**.** Основните ***технически мерки за защитата на автоматизираните информационни системи и/или мрежи***, са:

1. Идентификация и автентификация;
2. Управление на регистрите;
3. Управление на външни връзки и/или свързване;
4. Защитата от зловреден софтуер;
5. Създаване и поддържане на резервни копия за възстановяване;
6. Носители на информация;
7. Физическа среда / обкръжение.

(1) Идентификация и автентификация чрез използване на уникални потребителски акаунти и пароли за всяко лице, осъществяващо достъп до мрежата и ресурсите на ОУ "Христо Ботев". Прилагането на тази мярка е с цел да се регламентират нива на достъп и да се въведе достъп, съобразен с принципа „Необходимост да знае";

(2) *Управление на регистрите*, съобразено с ограничаване на достъпа до съответния регистър единствено до лица, които са пряко натоварени и/или служебно ангажирани с неговото водене, поддръжка и обработка;

(3) Управление на *външни връзки и/или свързване*, включващо от своя страна:

- Дефиниране на обхвата на вътрешните мрежи: Като *вътрешни мрежи* се разглеждат всички локални жични мрежи и/или телекомуникационни връзки тип „точка – точка", които се намират под контрола и администрацията на ОУ "Христо Ботев". Като *външни мрежи* се разглеждат всички мрежи, вкл. и безжични мрежи, интернет, интернет връзки, мрежови връзки с трети страни, мрежови сегменти на хостинг системи на трети страни, които не са под административния контрол на ОУ "Христо Ботев";

- Регламентиране на достъпа до вътрешната мрежа: Достъп до вътрешната мрежа имат единствено служителите и/или специално упълномощени от Директора. Достъпът до мрежата и обработваните лични данни се предоставя с оглед изпълнение на техните преки служебни задължения и е съобразен с принципа „Необходимо да знае“. Минимално изискваното ниво на сигурност за достъп до вътрешните мрежи изисква идентифициране с уникално потребителско име и парола;
- Администриране на достъпа до вътрешната мрежа: Отговорностите, свързани с осъществяване на администрация на достъпа, са възложени на лица с необходимата квалификация. В отговорностите са включени и дейности, свързани с одобряване на инсталирането на всички устройства, технологии и софтуер за достъп до мрежата, включително суичове, рутери, безжични точки за достъп, точки за достъп до мрежата, интернет връзки, връзки към външни мрежи и други устройства, технологии и софтуер, които могат да позволят достъп до вътрешните мрежи на Администратора;
- Контрол на достъпа до вътрешната мрежа: Отговорностите, свързани с осъществяване на контрола на достъпа са възложени на лица с необходимата квалификация. Те са задължени да предприемат адекватни мерки за минимализиране на риска от неоторизиран (физически и/или отдалечен) достъп до мрежите на ОУ "Христо Ботев", вкл. и чрез използване на защитни стени и други адекватни мерки и инструменти.

(4) *Защитата от зловреден софтуер* включва:

- използването на стандартни конфигурации за всяка компютърна и/или мрежова платформа, като системният, а при възможност и приложният, софтуер се контролира, инсталира и поддържа от оторизирани от Ръководството на ОУ "Христо Ботев" лица.
- използване на вградената функционалност на операционната система и/или хардуера, които се настройват единствено от оторизирани от Ръководството на ОУ "Христо Ботев" лица. Всяка промяна и/или деактивация на системите за защита от неоторизирани лица е забранена;
- активиране на автоматична защита и сканиране за зловреден софтуер и обновяване на антивирусни дефиниции. Забранено е потребителите да отказват автоматични софтуерни процеси, които актуализират вирусните дефиниции;
- забрана за пренос на данни от заразени компютри. При съмнение или установяване на заразяване на компютърна система работещият с нея е задължен да уведоми оторизираните от Ръководството на ОУ "Христо Ботев" лица и да преустанови всякакви действия за работа и/или изпращане на информация от заразения компютър (чрез външни носители, електронна поща и/или други способи за електронна обмяна на информация). До премахване на зловредния софтуер заразеният компютър следва да бъде незабавно изолиран от вътрешните мрежи.
- В ОУ "Христо Ботев" се използва единствено софтуер с уредени авторски права. Инсталирането и/или използването на всякакъв друг тип софтуер с неуредени авторски права е забранено.
- На служебните компютри се използва само софтуер, който е инсталиран от оторизирано от Ръководството на ОУ "Христо Ботев" лице. Забранено е самоволното инсталиране на всякакъв друг вид софтуер.
- При внедряване на нов програмен продукт за обработване на лични данни се тестват и проверяват възможностите на продукта с оглед спазване изискванията на Регламент 2016/679, Закона за защита на личните данни и осигуряване максималната защита на данните от неправомерен достъп, загубване, повреждане или унищожаване.

(5) Политика по *създаване и поддържане на резервни копия за възстановяване,* която регламентира:

- Основната цел на архивирането е свързана с предотвратяване на загуба на информация, свързана с лични данни, която би затруднила нормалното функциониране на ОУ "Христо Ботев";
- Начина на архивиране: информацията следва да бъде архивирана по подходящ способ и на носител, извън конкретния физически компютър, и да позволява пълното възстановяване на данните, в случай на погиване на техния основен носител;
- Отговорност за архивиране има лицето, обработващо личните данни;
- Срокът на архивиране следва да е съобразен с действащото законодателство;
- Съхраняването на архива следва да бъде в друго физическо помещение. Всички архиви, съдържащи поверителна и/или служебна информация, трябва да се съхраняват с физически контрол на достъпа.

(6) Основни електронни носители на информация са: вътрешни твърди дискове (част от компютърна система), еднократно и/или многократно презаписваеми външни носители (външни твърди дискове, многократно презаписваеми карти и други носители на информация, еднократно записваеми носители и др.). Използваният хардуер за съхранение и обработване на лични данни отговаря на съвременните изисквания и позволява гарантиране на разумна степен на отказоустойчивост, възможности за архивиране и възстановяване на данните и работното състояние на средата.

(7) Мерките, свързани със създаване на физическа среда (обкръжение), включват физически контрол на достъпа (сигнално-охранителна техника, ключалки, метални решетки и други приложими способи), създаване на подходяща работна среда, вкл. чрез поддържане на подходяща температура и нива на влажност, както и пожароизвестителна система. Те са насочени към осигуряване на среда за нормално функциониране, за защита на ИТ оборудването от неоторизиран достъп и контрол на риска от повреда и унищожаване.

III. ПОДДЪРЖАНИ РЕГИСТРИ С ЛИЧНИ ДАННИ И ТЯХНОТО УПРАВЛЕНИЕ

Чл. 19. Поддържаните от ОУ "Христо Ботев" регистри с лични данни са:

1. *Регистър „Служители и Персонал“*, в който се вписват следните видове лични данни:
   - *Физическа идентичност* – имена, паспортни данни (ЕГН, номер на лична карта, дата и място на издаване, адрес, телефон за връзка и други необходими за идентифициране на субекта на данни);
   - *Социална идентичност* – данни относно образование и допълнителна квалификация, трудова дейност и професионална биография;
   - *Семейна идентичност* – данни относно семейното положение на лицето и деца;
   - *Икономическа идентичност* – информация за номер на банкова сметка;
   - *Лични данни относно съдебното минало на лицето* -свидетелство за съдимост в зависимост от длъжността;
   - *Данни за здравословно състояние* – медицинско свидетелство, данни, съдържащи се в болнични листове, представяни от самите служители като субекти на данните, решения на ТЕЛК/НЕЛК и др. п.
2. *Регистър “Ученици“,* в който се вписват следните видове лични данни:

- *Физическа идентичност* -ЕГН, имена, адрес, гражданство, месторождение;
- *Данни за здравословно състояние* – здравно - профилактични карти, заболявания и др.,информация за СОП, личен лекар и др.;
- *Икономическа идентичност* – обща банкова информация, информация за номер на банкова сметка.
- *Лични данни, относно образователния процес* - информация за присъствие, отсъствия (причини за отсъствието), успех (оценяване на ученика), информация за полагане на изпити (вкл. олимпиади, състезания, конкурси и др.), информация за издаване на документи (дипломи, удостоверения, свидетелства, ученически книжки и ученически лични карти), фото и видеоматериали (вкл. снимки за документи);
- *Лични данни за контакт* в случай на спешност (с родител / настойник).

3. *Регистър "Родители/настойници",* в който се вписват следните видове лични данни:
   - *Физическа идентичност* - ЕГН, имена, адрес, телефон за връзка, e-mail адрес;
4. *Регистър "Контрагенти и партньори",* в който се вписват следните видове лични данни:
   - *Физическа идентичност* – имена, паспортни данни (ЕГН, номер на лична карта, дата и място на издаване, адрес, телефон за връзка и други необходими за идентифициране на субекта на данни);
   - *Икономическа идентичност* – обща банкова информация, информация за номер на банкова сметка.
5. *Регистър „Видеонаблюдение",* в който ще се съхраняват и обработват лични данни чрез създаване на видеозапис от средства за наблюдение в сградите и помещенията на ОУ "Христо Ботев", включващ следните видове лични данни:
   - *Физическа идентичност* – запис на образи и звук.
6. *Регистър „Посетители"*
   - *Физическа идентичност* – имена;
7. *Регистър „Дарители",* в който се вписват следните видове лични данни*:*
   - *Физическа идентичност* – имена, адрес, телефон за връзка;
8. *Регистър „Обществен съвет",* в който се вписват следните видове лични данни*:*
   - *Физическа идентичност* – имена, телефон за връзка;
9. *Регистър „Сигнали за нарушения",* в който се вписват следните видове лични данни*:*
   - *Физическа идентичност* – имена, адрес, телефон за връзка, електронна поща, качество на сигнализиращото лице (служител, съдружник и др); качество на лицата свързани с лицето, подаващо сигнал (колега, роднина и др.).

Чл. 20. За обработване на данните от регистрите по чл. 27 ОУ "Христо Ботев" води Регистър на дейностите по обработка по образец, съгласно ***Приложение № 5***.

IV. ЗАДЪЛЖЕНИЯ НА ДЛЪЖНОСТНОТО ЛИЦЕ ПО ЗАЩИТА НА ДАННИТЕ И ЛИЦАТА, ОБРАБОТВАЩИ ЛИЧНИ ДАННИ

Чл. 21. (1) Длъжностно лице по защита на данните се определя от Ръководството на ОУ "Христо Ботев".

(2) Длъжностно лице по защита на данните има следните правомощия и длъжностни задължения:

- да информира и консултира администратора, обработващия и служителите, които извършват обработване с цел да им разясни техните задължения, произтичащи от ОРЗД и от други разпоредби за защита на данните в Европейския съюз или държава членка. Длъжностното лице по защита на данните трябва не само да представи уредбата, но и да даде съвет как да бъдат изпълнени задълженията в конкретния случай.

- да следи за спазването на Регламента и на други разпоредби за защита на данните и на политиките на администратора или обработващия. Това задължение не отменя задължението на администратора или обработващия да контролира спазването на ОРЗД. Ролята на длъжностното лице по защита на данните е да подпомага администратора или обработващия в тази му дейност.

- да допринесе за повишаване на защитата на личните данни чрез идентифициране на операциите по обработване, анализ и проверка за съответствието на обработването с установените изисквания, информиране и даване на конкретни препоръки до администратора.

- да повишава осведомеността и обучението на персонала, ангажиран с операциите по обработване като механизъм с мощно превантивно действие, който може да даде своевременна информация за рисковете пред защитата на данните и да води до усъвършенстване на прилаганите мерки за защита.

- да сътрудничи с надзорния орган като действа като точка за контакт за надзорния орган по различни въпроси. Те могат да бъдат свързани с обработването на лични данни, с предварителната консултация, а по целесъобразност консултирането може да обхваща и всякакви други въпроси.

- да води регистър на дейностите по обработване на лични данни в ОУ "Христо Ботев" съгласно образеца в Приложение 5.

- да спазва конфиденциалност при изпълнение на неговите задачи. Това е важна гаранция за субектите на данни, които могат да се обръщат към него по всички въпроси, свързани с обработването на лични данни и с упражняването на техните права съгласно ОРЗД. Задължението за поверителност по отношение на конкретните обстоятелства, станали известни на длъжностното лице при или по повод изпълнение на неговите задачи. Неговото спазване обаче не изключва възможността за контакт и търсенето на съдействие от надзорния орган, тъй като това е част от задачите на длъжностното лице по защита на данните.

- да участва в курсове за обучение по защита на личните данни и в други тематики, които имат отношение към професионалното му развитие и повишаване на нивото на експертиза.

Чл. 22. Служителите на ОУ "Христо Ботев" са длъжни:

1. да обработват лични данни законосъобразно и добросъвестно;
1. да използват личните данни, до които имат достъп, съобразно целите, за които се събират, и да не ги обработват допълнително по начин, несъвместим с тези цели;
2. да актуализират при необходимост регистрите на личните данни;
3. да заличават или коригират личните данни, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;
4. да поддържат личните данни във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват.

Чл. 23. (1) За неспазването на разпоредбите на настоящите Вътрешни правила служителите носят дисциплинарна отговорност.

(2) Ако в резултат на действията на съответен служител по обработване на лични данни са произтекли вреди за ОУ "Христо Ботев" или за трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство.

V. ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

Чл. 24. Всички служители на ОУ "Христо Ботев" са длъжни да се запознаят с настоящите Вътрешни правила и да ги спазват ежедневно при изпълняване на заемната от тях длъжност и възложената им работа.

Чл. 25.(1) За всички неуредени в настоящите Вътрешни правила въпроси, са приложими разпоредбите на Общия регламент относно защитата на данните (ЕС) 2016/679, приложимото право на Европейския съюз и законодателството на Република България относно защитата на личните данни.

(2) Приложение към настоящите Вътрешни правила са образци на следните документи, съставяни при и по повод обработката на лични данни:

- Приложение № 1 – образец Протокол за задължителен инструктаж за запознаване с правилата за Противопожарна безопасност;

- Приложение № 2 –образец Протокол за унищожаване на лични данни и носители на лични данни;

- Приложение № 3 – Споразумение за обработка на данни;

- Приложение № 4–Протокол за преминато обучение по защита на личните данни и инструктаж за приложимите в ОУ "Христо Ботев" правила и мерки за защита на личните данни;

- Приложение № 5–Регистър на дейностите по обработка.

Директор: _____