

**Обединено училище „Христо Ботев“ село Красново, община Хисаря,
област Пловдив, улица 1-ва, № 26, улица 22-ра, №10,
email: info-1603706@edu.mon.bg, телефон 0885515572**

УТВЪРЖДАВАМ:
Йонка Марковска
Директор на ОбУ“ Христо Ботев“
Село Красново

ВЪТРЕШНИ ПРАВИЛА

ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

2025г.

Раздел I.
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) Обединено училище“ Христо Ботев“ е юридическо лице със седалище село Красново,община Хисаря,улица 1-ва,№ 26, Република България, с основен предмет на дейност образование и образователни услуги и е Администратор на лични данни.

(2) Училището обработва лични данни във връзка със своята дейност (образователна, възпитаваща, социализираща) и сама определя целите и средствата за обработването им.

Чл. 2. (1) Настоящите вътрешни правила уреждат организацията на обработване и защитата на лични данни на учителите, служителите, обучаемите (ученици), посетителите, както и на други физически лица, свързани с осъществяването на дейността на училището.

(2) Целта на настоящите вътрешни правила е установяването на ясни правила при събиране, организиране, съхраняване и разгласяване на лични данни от водените от **ОбУ“ Христо Ботев“ село Красново** регистри, за да се гарантира неприкосновеността на личността и личния живот, като се защитят физическите лица при неправомерно обработване на свързаните с тях лични данни и се регламентира правото на достъп до събираните и обработвани такива данни.

(3) Вътрешните правила се приемат с цел да регламентират:

- Създаване на процедури и механизми за гарантиране на неприкосновеността на личността и личния живот чрез осигуряване на защита на физическите лица при неправомерно обработване на свързаните с тях лични данни в процеса на свободното движение на данните;

- Необходимите технически и организационни мерки за защита на личните данни на посочените по-горе лица от неправомерно обработване (случайно или незаконно унищожаване, случайна загуба, неправомерен достъп, изменение или разпространение, както и от всички други форми на обработване на лични данни).

- Правата и задълженията на длъжностните лица, обработващи лични данни и/или лицата, които имат достъп до лични данни и работят под ръководството на обработващите лични данни, тяхната отговорност при неизпълнение на тези задължения.

Чл. 3. Настоящите вътрешни правила се прилагат за лични данни по смисъла на Закона за защита на личните данни в Република България и Регламент (ЕС) 2016/679.

Чл. 4. (1) Обединено училище“ Христо Ботев“ село Красново е администратор на лични данни по смисъла на чл. 4, пар. 7 от Регламент (ЕС) 2016/679.

(2) Според чл. 4, пар. 1 на Регламент (ЕС) 2016/679 „субект на лични данни“ е: идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано.

(3) ***Лични данни*** (според чл. 4, пар. 1 на Регламент (ЕС) 2016/679) са: всяка информация, свързана с идентифицирано или подлежащо на идентификация физическо лице, което може да бъде идентифицирано, пряко или косвено, по-специално чрез посочване на идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

(4) ***Обработване на лични данни*** (според чл. 4, пар. 2 на Регламент (ЕС) 2016/679) е: 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. Процесът на обработване на личните данни има конкретно техническо, материално проявление, като в тази връзка следва да бъдат предприети и адекватни технически и организационни мерки за защита на данните.

(5) **„Обработващ лични данни“** означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора.

Когато се Администраторът на лични данни използва орбаботващ, то мужду тях следва да се сключи споразумение относно задълженията им при обработването на личните данни, а обработващият да не ги разгласява. Когато обработването се извършва от името администратора, администраторът използва само обработващи лични данни, които предоставят достатъчни гаранции за прилагането на подходящи технически и организационни мерки по такъв начин, че обработването да протича в съответствие с изискванията на настоящия регламент и да осигурява защита на правата на субектите на данни. Обработващият данни не включва друг обработващ данни без предварителното конкретно или общо писмено разрешение на администратора.

Чл. 5. (1) Личните данни се събират и обработват:
- за изпълнение на правомощията и присъщата дейност на училището, предоставени чрез Закона и училищното и предучилищно образование и законодателството на Република България и ЕС;
- въз основа на законови задължения, възложени чрез законодателството на Република България и ЕС /закони, наредби, инструкции, правилници, регламенти и др./;
- при сключване на договори или подготовка за тяхното сключване;
- за защита на жизненоважни интереси на субекта на данните или на друго физическо лице;
- при липса на някое от горепосочените основания – единствено след съгласие на субекта на лични данни, дадено чрез подписана декларация за съгласие по образец. *(Приложение № 1);*
- освен това когато обработването е необходимо за целите на легитимните интереси на администратора или на трета страна, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни, по-специално когато субектът на данните е дете;

(2) Личните данни се обработват при спазване на следните принципи, въведени чрез Регламент 2016/679 г.:

1. Законосъобразност, добросъвестност и прозрачност - обработване при наличие на законово основание, при полагане на дължимата грижа и при информиране на субекта на данни;

2. 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;

3. Свеждане на данните до минимум – данните да са подходящи, свързани със и ограничени до необходимото във връзка с целите на обработването;

4. 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;

5. 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;

6. Цялостност и поверителност – обработване по начин, който гарантира подходящо ниво на сигурност на личните данни, като се прилагат подходящи технически или организационни мерки;

7. Отчетност – администраторът носи отговорност и трябва да е в състояние да докаже спазването на всички принципи, свързани с обработването на лични данни.

(3) Събирането на лични данни трябва да бъде в рамките на необходимото. Информацията се събира по законен и обективен начин; личните данни не трябва да се използват за цели, различни от тези, за които са били събирани, освен със съгласието на лицето или в случаите, изрично предвидени в закона. Личните данни трябва да се съхраняват само толкова време, колкото е необходимо за изпълнението на тези цели; личните данни трябва да са прецизни, точни, пълни и актуални, доколкото това е необходимо за целите, за които се използват; личните данни трябва да са защитени с мерки за сигурност, съответстващи на чувствителността на информацията.

Чл. 6. Училището 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. Предприеманите мерки са съобразени със съвременните технологични постижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

Чл. 7. (1) Обединено училище“ Христо Ботев“ село Красново прилага адекватна защита на личните данни, съобразена с нивото на нейното въздействие.

(2) Тя включва:

1. Физическа защита.
2. Персонална защита.
3. Документална защита.
4. Защита на автоматизирани информационни системи и/или мрежи.

Чл. 8. (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 правни задължения на училището и/или нормалното й функциониране.

(3) Събирането, обработването и съхраняването на лични данни в регистрите на училището се извършва на хартиен, технически и/или електронен носител по централизиран и/или разпределен способ в помещения, съобразено с посочените мерки за защита и нивото на въздействие на съответния регистър.

Чл. 9. За всяка дейност по събиране на лични данни се поддържа регистър на дейностите в *(Приложение № 3)* към настоящите Вътрешни правила, където е посочено кой, за какви цели и на какво основание обработва личните данни.

Чл. 10. (1) Право на достъп до регистрите с лични данни имат само оторизираните длъжностни лица.

(2) Оторизирането се извършва на база длъжностна характеристика и/или чрез изрична заповед на Директора на училището.

(3) 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.

(4) Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

Чл. 11. (1) Документите и преписките, по които работата е приключила, се архивират.

(2) Трайното съхраняване на документи, съдържащи лични данни, се извършва на хартиен носител в помещението, определено за архив, за срокове, съобразени с действащото законодателство. Помещението, определено за архив, е оборудвано с пожарогасител и задължително се заключва.

(3) Съхранението на документите и преписките на хартиен носител, архивирането/унищожаването на тези с изтекъл срок, се извършва по реда на Закона за Националния архивен фонд.

(4) Документите на електронен носител се съхраняват на специализирани компютърни системи и/или външни носители на информация. Архивиране на личните данни на технически носител се извършва периодично от обработващия/оператора на лични данни с оглед запазване на информацията за съответните лица в актуален вид и възможността и за възстановяване, в случай на погиване на основния носител/система. Архивните копия се съхраняват на различно местоположение от мястото на компютърното оборудване, обработващо данните. Достъп до архивите имат само обработващият/операторът/ на лични данни и оторизираните длъжностни лица.

(5) Достъп до архивираните документи, съдържащи лични данни, имат единствено оторизирани със заповед лица.

Чл. 12. С оглед защита на хартиените, техническите и информационните ресурси всички служители са длъжни да спазват правилата за противопожарна безопасност, както и цялото българско законодателство регламентиращо безопасността на сградите.

Чл. 13. (1) При регистриране на неправомерен достъп до информационните масиви за лични данни или каквото и да е нарушение на сигурността на данни, служителят, констатирал това нарушение, докладва писмено за този инцидент на прекия си ръководител, който от своя страна е длъжен, своевременно да информира училищното ръководство, както и ДЛЗД като му предоставят цялата налична информация.

(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.

(3) Училищното ръководство трябва да уведоми Длъжностното лице по защита на личните данни по възможност веднага като му предоставят цялата налична информация, а Комисията за защита на личните данни до 72 часа от узнаването за неправомерния достъп.

(4) Ако нарушението на сигурността на данните представлява висок риск за засегнатите лица, всички те също трябва да бъдат информирани, освен ако не са въведени ефективни технически и организационни мерки за защита или други мерки, които гарантират, че вече няма вероятност рискът да се случи на практика.

(5) ДЛЗД извършва незабавно проверка по подадения сигнал, като се опитва да установи дали е осъществено нарушение на сигурността и кои данни са засегнати.

(6) ДЛЗД докладва незабавно на Директора на учебното заведение наличната информация за нарушението на сигурността, включително информация относно характера на инцидента, времето на установяването му, вида на щетите, предприетите към момента мерки и мерките, които счита, че трябва да се предприемат.

(7) След съгласуване с ръководството на учебното заведение ДЛЗД предприема мерки за предотвратяване или намаляване последиците от пробива и възможностите за възстановяване на данните.

(8) При спешност, когато съгласуване с ръководството би забавило реакцията и би нанесло големи щети, ДЛЗД може по своя преценка да предприеме мерки за предотвратяване или намаляване последиците от нарушението на сигурността. В този случай ДЛЗД уведомява незабавно ръководството за предприетите мерки и съобразява последващи действия с получените инструкции.

(9) Във всеки един случай на ДЛЗД следва да се оказва пълно съдействие от страна работниците/служителите в училището.

Чл. 14. При повишаване на нивото на чувствителност на информацията, произтичащо от изменение в нейния вид или в рисковете при обработването ѝ, училището може да определи друго ниво на защита за регистъра.

Чл. 15. (1) След постигане целта на обработване на личните данни или преди прехвърлянето на контрола върху обработването, личните данни, съдържащи се в поддържаните от училището регистри, следва да бъдат унищожени или прехвърлени на друг администратор на лични данни съобразно изискванията на Закона за защита на личните данни. При промени в структурата на училището, налагащи прехвърляне на регистрите за лични данни на друг администратор на лични данни, предаването на регистъра се извършва след разрешение на Комисията за защита на лични данни.

(2) В случаите, когато се налага унищожаване на носител на лични данни, училището прилага необходимите действия за тяхното заличаване по начин, изключващ възстановяване данните и злоупотреба с тях. Личните данни, съхранявани на електронен носител, се унищожават чрез трайно изтриване, вкл. презаписването на електронните средства или физическо унищожаване на носителите. Документите на хартиен носител, съдържащи данни, се унищожават чрез нарязване с шредер или по друг подходящ начин, който се протоколира.

(3) Унищожаването се осъществява от служителя, отговорен за архива на училището.

Чл. 16. (1) Достъпът до данните от регистъра и разкриването на личните данни се

осъществява при условията и по реда на Закона за защита на личните данни и Регламент 2016/679 от:

- физическите лица, за които се отнасят данните;
- трето лице, ако е предвидено в нормативен акт;
- обработващия личните данни.

(2) Достъп до лични данни може да бъде предоставен под формата на устна или писмена справка или на преглед на данните от съответното физическо лице или от изрично упълномощено от него друго лице.

(3) Физическото лице може да поиска копие от обработваните лични данни на предпочитан носител или предоставяне по електронен път, освен в случаите, когато това е забранено от закон.

(4) Достъп на лица до лични данни се предоставя единствено, ако те имат право на такъв достъп, съгласно действащото законодателство, след подаване на заявление*(Приложение № 2),* респ. искане за достъп до информация, и след тяхното легитимиране.

(5) Заявлението съдържа:

1. име, адрес и други необходими данни за идентифициране на съответното физическо лице;
2. описание на искането;
3. предпочитана форма за предоставяне на достъпа до личните данни;
4. подпис, дата на подаване на заявлението и адрес за кореспонденция.

(6) Директорът разглежда заявлението за достъп и се произнася по него в 14-дневен срок.

(7) Директорът взема решение за предоставянето на пълен или частичен достъп на заявителя или мотивира отказ за предоставяне на достъп.

(8) Директорът писмено уведомява заявителя за решението си. Уведомяването е лично срещу подпис, по пощата с обратна разписка или по e-mail.

Раздел II.
МЕРКИ ПО ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 17. (1) ***Физическа защита*** в училището се осигурява чрез набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на сградите и помещенията, в които се обработват и съхраняват лични данни.

(2) Основните приложими *организационни мерки за физическа защита* в училището включват определяне на помещенията, в които ще се обработват лични данни, както и на тези, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни, вкл. и определяне на организацията на физическия достъп.

Като *помещения, в които ще се обработват лични данни,* се определят всички помещения, в които с оглед нормалното протичане на учебния и административния процес, се събират, обработват и съхраняват лични данни. Достъпът до тях е физически ограничен само за служители с оглед изпълнение на служебните им задължения. Когато в тези помещения имат достъп и външни лица, в помещенията се обособява непублична част, която е физически ограничена и достъпна само за служители, на които е необходимо да имат достъп с оглед изпълнението на служебните им задължения. Създава се подходяща работна среда, вкл. чрез поддържане на подходяща температура и нива на влажност, както и пожароизвестителна система, както и сигнално-охранителна техника.

Комуникационно-информационните системи, използвани за обработка на лични данни, се разполагат в помещения, 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.

Организацията на физическия достъп до помещения, в които се обработват лични данни, е базирана на ограничен физически достъп (на база заключващи системи). Достъп се

предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения.

Като *зони с контролиран достъп* се определят всички помещения на територията на училището, в които се събират, обработват и съхраняват лични данни.

Достъпът до системите, обработващи по електронен способ лични данни, е ограничен чрез уникални потребителски идентификатори и пароли, а електронните носители, са защитени по адекватен начин, в зони с контрол на достъпа.

(3) Основните приложими *технически мерки за физическа защита* в училището включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства.

(4) Помещенията, определени за архив, а по възможност и всички други, в които се обработват и съхраняват лични данни, следва да отговарят на следните изисквания, наред с тези за пожарна безопасност и цялото българско законодателство регламентиращо безопасността на сградите:

1. да бъдат сухи, леснопроветриви и изолирани от пряко действие на слънчеви лъчи;
2. през тях да не минават канализационни, топлопроводни и газоотоплителни пътища;
3. електрическата инсталация да е закрита; не се допуска използване на открити осветителни и отоплителни уреди;
4. пространствената подредба да осигурява лесен и удобен достъп до съхраняваните документи;
5. да е осигурено със средства за ограничаване на физическия достъп чрез надеждни заключващи системи и със средства за авариен достъп.

Чл. 18. (1) ***Персоналната защита*** представлява система от организационни мерки спрямо физическите лица, които обработват лични данни по указание на администратора.

(2) Основните мерки на персоналната защита са:

1. познаване на нормативната уредба в областта на защитата на личните данни;
2. познаване на политиката и ръководствата за защита на личните данни;
3. знания за опасностите за личните данни, обработвани от администратора;
4. поемане на задължение за неразпространение на личните данни; изразено в декларация по образец. *(Приложение 4).*

(3) Мерките за персонална защита гарантират достъпа до лични данни само на лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп, при спазване на принципа „Необходимост да знае". „Необходимост да знае" означава, че закон, друг нормативен акт или естеството на работата изисква лицето да получава дадена информация или без нея изпълнението на служебните му задължения би се затруднило неимоверно много или стане невъзможно.

(4) Лицата могат да започнат да обработват лични данни след запознаване със:

1. нормативната уредба в областта на защитата на личните данни;
2. политиката и ръководствата за защита на личните данни;
3. опасностите за личните данни, обработвани от администратора.

(5) Работници/служители имат право на достъп до регистрите с лични данни на база длъжностна характеристика или чрез изричен акт/заповед Директора.

(6) Работниците/служителите носят отговорност за осигуряване и гарантиране на регламентиран достъп до служебните помещения и опазване на регистрите, съдържащи лични данни.

Чл. 19. (1). Основните приложими *мерки за* ***документална защита*** на личните данни са:

1. *Определяне на регистрите, които ще се поддържат на хартиен носител:* 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 училището;

2. *Определяне на условията за обработване на лични данни:* личните данни се събират само с конкретна цел, пряко свързана с изпълнение на законовите задължения и/или нормалната дейност на училището, а начинът на тяхното съхранение се съобразява със специфичните нужди за обработка;
3. *Регламентиране на достъпа до регистрите*: достъпът до регистрите е ограничен и се предоставя само на упълномощените служители, в съответствие с принципа на „Необходимост да знае";
4. *Определяне на срокове за съхранение:* личните данни се съхраняват толкова дълго, колкото е необходимо, за да се осъществи целта, за която са били събрани и/или изискванията на действащото законодателство.
5. *Процедури за унищожаване:* Документите, съдържащи лични данни, които не подлежат на издаване към Държавен архив, и след изтичане на законовите срокове за тяхното съхранение, и не са необходими за нормалното функциониране на училището, се унищожават по подходящ и сигурен начин (напр. изгаряне, нарязване, електронно изтриване и други подходящи за целта методи). За всяко такова унищожаване се съставя протокол.

   (2.1) Изнасянето на документи извън училището за нуждите на специализирани държавни органи или други случаи предвидени със закон се извършва съобразно действащото законодателство и след писмено разрешение от директора.

   (2.2) За всяко изнасяне и връщане на документи извън училището се изготвя предавателно-приемателен протокол, в който се описват документите, определя се срокът за използване и се декларира ангажиментът за връщането им в архива. **(3.3)** При установяване на липси и увреждания след връщането на документите се съставя протокол и писмено се уведомява директора. **(2.4)** Лицето, отговарящо за съответните документи или за архива, ако са архивни, проверява състава и състоянието на документите преди и след използване.

Чл. 20. (1) ***Защитата на автоматизираните информационни системи и/или мрежи*** в училището включва набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп до системите и/или мрежите, в които се създават, обработват и съхраняват лични данни.

(2) Основните мерки за защита на автоматизираните информационни системи и/или мрежи, обработващи лични данни, оценени с ниско ниво на въздействие, включват:

1. *Идентификация* чрез използване на пароли за лицата, които имат достъп до мрежата и ресурсите на училището. Прилагането на тази мярка е с цел да се регламентират нива на 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 въвеждане, поддръжка и обработка;
3. *Защитата от вируси*, 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 ръководител направление ИКТ.
   - 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 Директора и оторизираните от него 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.

4. Политиката по *създаване и поддържане на резервни копия за възстановяване* има за цел предотвратяване на загуба на информация, свързана с лични данни, която би затруднила нормалното функциониране на училището.
5. Основни електронни *носители на информация са*: вътрешни твърди дискове, еднократно и/или многократно презаписваеми външни носители (външни твърди дискове, многократно презаписваеми карти, памети ленти и други носители на информация, еднократно записваеми носители и др.)
6. *Персоналната защита на данните* е част от цялостната охрана на училището.
7. *Личните данни в електронен вид се съхраняват* съгласно нормативно определените срокове и съобразно спецификата и нуждите на училището.
8. Следва да има определено лице, което да извършва периодични проверки на целостта на базата данни и актуализиране на системната информация, поддържане на системата за достъп до данните
9. Данните, които вече не са необходими за целите на училището и чиито срок за съхранение е изтекъл, се *унищожават чрез приложим способ* (напр. постоянно заличаване от електронните средства или друг приложим метод отговарящ на съвременните софтуерни изисквания, чието използване следва да бъде документирано).

Чл. 21. (1) Компютърен достъп 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 парола.

(2) С цел повишаване сигурността на достъпа до информация служителите задължително променят използваните от тях пароли на определен период. В случай на отпадане на основанието за достъп до лични данни правата на съответните лица се преустановяват (вкл. при необходимост и чрез изтриване на акаунта).

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

Чл. 22. (1) Използваният хардуер за съхранение и обработване на лични данни отговаря на съвременните изисквания и възможности за архивиране и възстановяване на данните и работното състояние на средата.

(2) При необходимост от ремонт на компютърната техника, предоставянето й на сервизната организация се извършва, по възможност, без устройствата, на които се съхраняват лични данни.

Чл. 23. (1) В училището се използва единствено софтуер с уредени авторски права.

(2) На служебните компютри се използва само софтуер, който е инсталиран от оторизирано лице – ръководител направление ИКТ.

(3) При внедряване на нов програмен продукт за обработване на лични данни се тестват и проверяват възможностите на продукта с оглед спазване изискванията на Закона за защита на личните данни и осигуряване максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.

(4) Системите, обработващи и/или съхраняващи лични данни, включват система за контрол, регистрираща следните действия в журнал (log) за одит: опити за влизане и ефективно влизане и излизане от системата, действията на потребителите в процеса на всяка работна сесия, смяна на пароли. Когато бъде установена нетипична активност (например влизане в нетипично време, неизключане на работна станция след изтичане на работното време и др.п.), системният администратор незабавно уведомява Диретора и Длъжностното лице по защита на данните за извършване на проверка по случая.

Чл. 24. (1)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 училището. 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 училището.
• Регламентиране на достъпа до вътрешната мрежа: Достъп до вътрешната мрежа имат единствено работниците/служителите и/или специално упълномощени от Директора лица. 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 училището, вкл. и чрез използване на защитни стени и други адекватни мерки и инструменти.
• На работници/служители на училището може да бъде предоставен Интернет достъп (отдалечен достъп) за изпълнение на служебните им задължения до електронните регистри с лични данни. Обхватът на достъпа и типа достъпни ресурси (вкл. сайтове, файлове, услуги и др.) се определя по преценка на Директора, съгласувана с оторизираните Директора лица, отговарящи за мрежите и защитата им, за степента на осъществимост, в пряка връзка с изпълняваните задължения и свързаните с този достъп рискове.
Отдалечен достъп чрез Интернет до определени ресурси, вкл. и вътрешните такива, може да бъде прекратен по всяко време по преценка на Директора, както и в случаите на заплаха за сигурността на данните.
• Публикуването на служебна информация в Интернет, независимо под каква форма и на каква платформа, се извършва единствено след писмена оторизация от Директора или посочено от него лице.
(2) Мерките, свързани с текущото поддържане и експлоатация на информационните системи и ресурси на училището, включват:
• Оценка на сигурността, включваща периодични тестове и оценки на уязвимостта на мрежите и системите на училището от външни и вътрешни атаки (Vulnerability test), включително оценка на въздействието, адекватността на използваните мерки и способи за защита, както и препоръки за нейното техническо и организационно подобряване. Оценката включва посочените аспекти и по отношение сигурността на събираните, обработвани и съхранявани лични данни.
• Забрана за притежание и ползване на хардуерни или софтуерни инструменти от работници/служители на училището, които биха могли да бъдат използвани, за да се компрометира сигурността на информационните системи. Към тази група се отнасят и инструменти, способстващи за нарушаване на авторските права, разкриване на тайни пароли, идентифициране на уязвимост в сигурността или дешифриране на криптирани файлове. Забранено е използването и на хардуер или софтуер, който отдалечено наблюдава трафика в мрежа или оперираш компютър. За неоторизирано използване на подобни инструменти служителят се наказва дисциплинарно, а ако науршението е не само дисциплинарно или представлява престъпление – и по предвидения за санкциониране на това нарушение/престъпление ред.
• По отношение на личните данни по възможност се прилагат и мерки, свързани с криптографска защита на данните чрез стандартните криптографски възможности на операционните системи, на системите за управление на бази данни и на

комуникационното оборудване. Криптирането се използва и за защита на личните данни, които се предават от училището по електронен път или на преносими носители.

Чл. 25. Служителите, на които е възложено да подписват служебна кореспонденция с универсален електронен подпис (УЕП), нямат право да предоставят издадения им УЕП на трети лица.

Раздел III.
ПОДДЪРЖАНИ РЕГИСТРИ И ТЯХНОТО УПРАВЛЕНИЕ

Чл. 26. (1) Поддържаните регистри в училището са:

1. Трудови правоотношения
2. Болнични листове
3. Подбор на персонал
4. Проекти по Еразъм
5. Видеонаблюдение
6. Основна образователна дейност
7. Поддържане на необходимата документация, свързана с образователната дейност
8. Издаване на видове удостоверения за ученици/ бивши ученици
9. Квалификация на персонала
10. Прием на ученици
11. Трудова медицина
12. Здравно обслужване
13. Издаване на служебни бележки, справки и удостоверения на настоящи и бивши служители
14. Дарения
15. Изпити
16. Състезания, олимпиади
17. Стипендии
18. Участие в национални програми
19. Регистър „библиотека“
20. Осъществяване на обща и/или на допълнителна подкрепа
21. Счетоводство
22. Архив
23. Входящ регистър
24. Изходящ регистър
25. Регистър на договорите

(2) Всички регистри са подробно описани в Приложение № 3 към правилата, което представлява Регистър на дейностите. В него е посочено кой работи с данните от всеки един регистър и какви мерки за защитата им се предприемат.

(3) Всяка година Директорът издава заповед, с която определя кой да отговаря за всеки отделен регистър.

Чл.27. За всеки регистър се оценява рискът по следния начин:

(1) Ниско ниво на риска – когато загубата или неправомерното обработване на личните данни от конкретен регистър не биха имали значителни последствия, застрашаващи живота на физическо лице или кражба на самоличността му.

(2) Средно ниво на риска - когато загубата или неправомерното обработване на личните данни от конкретен регистър биха имали последствия, довеждащи до кражба на самоличност на физическо лице.

(3) Високо ниво на риск - когато загубата или неправомерното обработване на личните данни от конкретен регистър биха имали последствия, довеждащи до кражба на самоличност на група от физически лица.

(4) Изключително високо ниво на риск - когато загубата или неправомерното обработване на личните данни от конкретен регистър биха имали последствия, застрашаващи живота на физическо лице.

Чл. 28. (1) При „изключително високо ниво на риск“, констатирано при условията на предходния член, се извършва „Оценка на въздействието“ спрямо начина и критериите, залегнали в Регламент (ЕС) 2016/679.

(2) Когато съществува вероятност определен вид обработване, по-специално при което се използват нови технологии, и предвид естеството, обхвата, контекста и целите на обработването, да породи висок риск за правата и свободите на физическите лица, преди да бъде извършено обработването, администраторът извършва оценка на въздействието на предвидените операции по обработването върху защитата на личните данни.

(3) „Оценка на въздействието“ се извършва и когато дейността по обработване попада в списъка, изготвен от надзорния орган.

(4) За оценката се съставя протокол, който се предоставя при поискване от страна на КЗЛД.

Раздел IV.
ПРАВА И ЗАДЪЛЖЕНИЯ НА ЛИЦАТА, РАБОТЕЩИ С ЛИЧНИ ДАННИ

Чл. 29. (1) Длъжностното лице по защита на данните е длъжно:

а) да информира и съветва администратора или обработващия лични данни и служителите, които извършват обработване, за техните задължения по силата на Общия регламент за защита на данните и на други разпоредби за защитата на данни на равнище Съюз или национално законодателство;

б) да наблюдава спазването на Общия регламент и на други разпоредби за защитата на данни на равнище Съюз или национално законодателство и на политиките на администратора или обработващия лични данни по отношение на защитата на личните данни;

в) да участва в повишаването на осведомеността и обучението на персонала, участващ в операциите по обработване, и съответните одити;

г) при поискване да предоставя съвети по отношение на оценката на въздействието върху защитата на данните и да наблюдава извършването на оценката;

д) надлежно да отчита рисковете, свързани с операциите по обработване, и да се съобразява с естеството, обхвата, контекста и целите на обработването;

е) да участва в заседания на ръководството, когато се обсъждат въпроси от областта на защитата на личните данни;

ж) да дава становище/съвет/мнение по всички въпроси, свързани със защитата на личните данни, да консултира администратора или обработващия лични данни;

з) да си сътрудничи с надзорния орган;

и) да действа като точка за контакт за надзорния орган по въпроси, свързани с обработването, и по целесъобразност да се консултира по всякакви други въпроси с надзорния орган;

й) ДЛЗД може да дава и други съвети, ако притежава необходимата компетентност, стига да не водят до конфликт на интереси.

(2) ДЛЗД има право:

а) да събира информация за определяне на дейностите по обработване;

б) да анализира и проверява изпълнението на дейностите по обработване;

в) да информира, съветва и отправя препоръки към администратора или обработващия лични данни;

д) да получава информация и необходимото съдействие от страна на ръководните органи в предприятието, от администратора/обработващия лични данни, от всички релевантни отдели и вътрешни структури, имащи отношение към операциите по обработване на лични данни.

(3) При изпълнение на своите задачи ДЛЗД действа напълно независимо и свободно от указанията на АДМИНИСТРАТОРА НА ЛИЧНИ ДАННИ

Чл. 30. (1) Служителите на училището са длъжни:

1. да обработват лични данни законосъобразно, добросъвестно и прозрачно;
2. 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;
3. да актуализират регистрите на личните данни (при необходимост);
4. да заличават или коригират личните данни, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;
5. 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;
6. да не разгласяват лични данни, до които са получили достъп при и по повод изпълнение на задълженията си;
7. незабавно да уведомяват администратора на лични данни в случай, че установят изтичане на лични данни, независимо дали при извършване на своята работа или при друго лице, което обработва лични данни.

(2) За неспазването на разпоредбите на Настоящите вътрешни правила служителите носят административна, дисциплинарна отговорност по Кодекса на труда, административно-наказателна, а в определени случаи и наказателна отговорност.

(3) Ако в резултат на действията на съответен служител по обработване на лични данни са произтекли вреди за трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство или по наказателен ред, ако стореното представлява по-тежко деяние, за което се предвижда наказателна отговорност.

Чл. 31. (1.1) Информацията съдържаща се в известието по Приложение 5 се публикувана интернет страницата на училището, както и на хартиен носител до входа, като се пригоди в необходимия формат и наименува коректно.

(1.2) Копие от известието се дава на ученик, а когато е непълнолетен - съответно негов родител, само при изрично искане за това и срещу подпис от тяхна страна на екземпляр, който остава в училището.

(2.1) Информацията съдържаща се в известието по Приложение 6 се публикувана интернет страницата на училището, само ако има секция достъпна единствено за служители/работници в училището, както и на хартиен носител в учителската стая и счетоводството.

(2.2) Копие от известието се дава на работник/служител срещу подпис от негова страна на екземпляр, който остава в училището.

(3.1) Декларация по образец по Приложение 1 се дава в случаите, когато за обработването на лични данни е необходимо съгласие и, разбира се, тази обработка не е на друго основание като законово, договорно или друго. В този вариант тя се нагажда към конкретния случай с упоменати в нея точни цели и средства на обработка на данните, както и всяка друго необходима информация.

(3.2) Изразеното съгласие трябва да бъде свободно дадено, конкретно, информирано и недвумислено заявление. Ако съгласието за обработка на лични данни се дава чрез документ,

който урежда и други въпроси, то следва да бъде изискано отделно от съгласието по други въпроси. Съгласието трябва да бъде дадено свободно. Такова съгласие е налично в случаите, когато субектът на данни има истински и свободен избор и е в състояние да откаже или да оттегли съгласието си, без това да доведе до вредни последици за него.

(3.3) Субектите на данни трябва да могат лесно да оттеглят съгласието си за обработване по всяко време, и оттеглянето трябва да бъде уважено своевременно. Ако не съществува друго условие за законосъобразност на обработването, с оттеглянето на съгласието то следва да се прекрати.

(3.4) Декларациите за съгласие се съхраняват от учебното заведение, докато се извършват действия по обработване на данни на това основание, с оглед спазването на принципа на отчетност. Съгласието остава едно от алтернативните условия за обработване на личните данни.

(3.5) Учебното заведение трябва да може да докаже неговото наличие. Субектът на данните следва да бъде информиран за последиците при отказ да даде съгласие за обработване на отделни категории лични данни.

(3.6) Съгласието може да бъде дадено онлайн. Това може да бъде осъществено чрез отбелязване на отметка в поле, избиране на технически настройки за услуги на информационното общество или друго заявление или поведение, което ясно показва, че субектът на данни е съгласен с предложеното обработване на неговите лични данни. Мълчанието, предварително отметнатите полета или липсата на действие не представляват съгласие.

(3.7) Във всеки един случай на субекта на лично данни трябва да се разяснят последиците от недаването на съгласие или оттеглянето му.

(4.1) Когато субект на данните желае да упражни правата си чрез заявленията по Приложение 2 (предоставяне на лични данни), Приложение 7 **(**„да бъде забравен“) и Приложение 8 (възражение срещу обработването на личните данни), следва да му бъде предоставена тази възможност по възможно най-бързия начин.

(**4.2**) Използването на тези образци не е задължително и всеки един субект на личните данни може да упражни правата си в свободна писмена форма, а когато е устна формата – то трябва да се протоколира от работник/служител в училището, като протоколът се подписва от съставителя му и субекта на личните данни.

(4.3) Желателно е субектът на данните да посочи в какво форма да му се отговори (например – по имейл, поща и др.)

(4.4) Работниците/служителите в училището трябва да оказват съдействие на всички субекти на данните.

(4.5) Администраторът на лични данни трябва да отговори в разумен и законоустановен срок.

(5) Във всеки един случай Администраторът на лични данни следва да потърси становището на ДЛЗД или друго компетентно лице.

Чл. 32. Когато се работи онлайн или се преминава към ОРЕС следва да се спазват, освен настоящите правила, и издадените за това правила, с които се запознават всички участници в процеса.

Раздел V.
ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Всички педагогически специалисти и служители в Обединено училище“ Христо Ботев“ село Красново са длъжни срещу подпис да се запознаят с настоящите вътрешните правила за защита на личните данни и да ги спазват.

§ 2. Вътрешните правила се издават на основание Закона за защита на личните данни и Регламент (ЕС) 2016/679 и влизат в сила незабавно.

§ 3. За всички неуредени в настоящите вътрешни правила въпроси са приложими

разпоредбите на Регламент (ЕС) 2016/679, Закона за защита на личните данни и действащото приложимо законодателство на Република България.

§ 4. Настоящите вътрешни правила отменят действието на съществуващата до сега Инструкция за защита на личните данни.

§ 5. Администраторът на лични данни може да променя тези Правила по всяко време. Всички промени следва да бъдат незабавно сведени до знанието на работниците/служителите.

§6. Вътрешните правила се утвърждават със Заповед на Директора № РД-10-150/25.11.2025 година.

Приложение 1.

. . . . . .

ДЕКЛАРАЦИЯ ЗА СЪГЛАСИЕ

Долуподписаният/ата……
…….ЕГН: ……

ДЕКЛАРИРАМ:

Съгласен/а съм ……...
да обработва личните ми данни, съгласно изискванията на Регламент 2016/679/ЕС и Закона за защита на личните данни.

Запознат/а съм с:

- целта и средствата на обработка на личните данни;
- доброволния характер на предоставянето на данните и последиците от отказа за предоставянето им;
- правото ми на достъп и на коригиране на събраните данни;
- правото да оттегля съгласието си;
- получателите или категориите получатели, на които могат да бъдат разкрити данните.
- правото ми на възражения и жалби във връзка с обработването и съхраняването на личните данни пред Комисия за защита на личните данни, която е надзорен орган в Република България.

Декларирам, че ще уведомявам администратора на лични данни за всяка промяна в личните ми данни.

Декларирам, че давам своето съгласие за обработване на лични данни свободно, съгласно волята си, и гарантирам верността на посочените данни:……

Дата: …… ДЕКЛАРАТОР:……

гр./с……..

Приложение 2.

До Директора на
.....

ЗАЯВЛЕНИЕ
за предоставяне на лични данни

От…… с ЕГН ……

Пълномощник…… с ЕГН ……

Пълномощно №.....,от ..... (нотариално заверено, приложено към заявлението)

Относно: Предоставяне на лични данни .....
(описание на искането)

Уважаема г-жо Директор,

Във връзка с и на основание Регламент (ЕС) 2016/679 с настоящото заявление се обръщам към Вас да получа лични данни относно:

1 .....

2 .....

3 .....

Предпочитам формата на предоставената информация да бъде във вид на

.....
(електронен вариант или на хартиен носител, електронна поща и др.)

Адрес за кореспонденция :

гр....., ул. “..... ” №....., бл.,вх...., ет., ап ....., тел.

Получател: .....
(име, презиме, фамилия)

Дата: С уважение:

Получено от:..... на .....г.

Приложение 3.

РЕГИСТЪР

Името и координатите за връзка на
- администратора и — когато това е приложимо — на всички съвместни администратори;
- на представителя на администратора;
- на обработващия лични данни;
- на длъжностното лице по защита на данните.

1. Описание на регистъра.
2. Служители, които работят с регистъра.
3. Описание на дейността по събиране на лични данни.
4. Цели на събирането.
5. Законово основание.
6. Категории лични данни, които се обработват.
7. Категории субекти на лични данни.
8. Получатели на лични данни.
9. Име на държавата или международната организация в случай на предаване на лични данни в друга държава.
10. Гаранции за прехвърляния на лични данни към трети държави или международни организации (ако е приложимо).
11. График със срокове на изтриване и основанието за срока, ако е възможно.
12. Локация на личните данни.
13. Общо описание на техническите и организационните мерки за сигурност.
14. Оценка на риска.
15. Изисква ли се оценка на въздействие? Ако да – оценката.

Регистър на дейностите в
……

Администратор на личните данни - …… с адрес ул. „……..“ № …., тел.: ……., e-mail: .....
Длъжностно лице по защита на личните данни ……. – e-mail: ……

1. Трудови правоотношения

1. Необходима документация, съдържаща и лични данни за започване, изпълнение и прекратяване на трудово правоотношение.
2. Данните ще се обработват Директор, Счетоводител, ЗАС, заместник-директори и учители участващи в комисиите за подбор.
3. Събират се от работниците/служителите, а когато има законово изискване и от други публични органи.
4. Цели на събирането: сключването, изпълнението и прекратяването на трудовия договор и произхождащото от него трудово правоотношение
5. Законово основание - чл. 6, пар. 1, т. “Б” от ОРЗД – сключване на трудовия договор и произхождащото от него трудово правоотношение, както и законовите задължения, предвидени в КТ и всички други приложими нормативни актове - чл. 6, пар. 1, т. “В” от ОРЗД.
6. Видове лични данни, които се обработват: име, ЕГН, номер и дата на издаване на лична карта, адрес, семейно положение и деца (в определени случаи: лични данни на съпруг/съпруга и други близки за упражняване на трудови права, напр. при отпуски по майчинство), информация за трудовия стаж и професионалния опит (включително заемани длъжности, работно време, стаж по специалността), информация за банкови сметки, заплата и социални придобивки, месторабота, информация за подбор (включително копия от разрешителни за работа, препоръки и друга информация, посочени в автобиография и придружително писмо или предоставена по друг начин в процеса на кандидатстване, информация относно трудова дисциплина.
Специални категории: членство в синдикални организации, информация за наказателни присъди и нарушения, тъй като това е предвидено задължение в закона.
7. Субекти на лични данни – работници и служители.
8. Получатели на лични данни – НАП, НОИ и др. предвидени по закон публични органи само в предвидените по закон случаи и цели.
9. Име на държавата или международната организация в случай на предаване на лични данни в друга държава – няма.
10. Гаранции за прехвърляния на лични данни към трети държави или международни организации (ако е приложимо) – няма.
11. График със срокове на изтриване и основанието за срока, ако е възможно – съхраняват се 50 години, впоследствие предвидените в закона документи се изтриват, а другите се предават в държавния архив.
12. Локация на личните данни – в коя стая и шкаф се съхраняват.

13. Общо описание на техническите и организационни мерки за сигурност - охрана на сградата, видеонаблюдение, контролиран достъп до тях, шкаф с ключ, копие от който имат хората, които работят с тях- Директор, ЗАС, специалист ТРЗ, администратор, домакин - пожарогасители, преминато обучение на персонала за познаване на нормативната уредба в областта на защитата на личните данни и опасностите за личните данни, обработвани от администратора; съгласие от всички работници/ служители на администратора за поемане на задължение за неразпространение на личните данни.
14. Оценка на риска – нисък.
15. Изисква ли се оценка на въздействие? Ако да – оценката. – НЕ.

2. Болнични листове

1. Описание на регистъра - установяване на неработоспособност на работниците/служителите и поддържане на законово необходимата документация в тази връзка.
2. Служители, които работят с регистъра – Директор, домакин-касиер, специалист ТРЗ, Счетоводител, ЗАС
3. Описание на дейността по събиране на лични данни – предоставя се от субектите на данни.
4. Цели на събирането - установяване на неработоспособност на работниците/служителите.
5. Законово основание - чл. 6, пар. 1, т. "В" от ОРЗД – КТ, КСО и приложимите към тях нормативни актове.
6. Категории лични данни, които се обработват – име, ЕГН, здравословно състояние, адрес
7. Категории субекти на лични данни – работници/служители.
8. Получатели на лични данни –НОИ, НАП, ТЕЛК
9. Име на държавата или международната организация в случай на предаване на лични данни в друга държава – няма.
10. Гаранции за прехвърляния на лични данни към трети държави или международни организации (ако е приложимо) – няма.
11. График със срокове на изтриване и основанието за срока, ако е възможно – 5 години, след приключване
12. Локация на личните данни – дирекцията на училището и учителската стая.
13. Общо описание на техническите и организационни мерки за сигурност - охрана на сградата, СОТ, видеонаблюдение, контролиран достъп до тях, шакф с ключ, копие от който имат хората, които работят с тяхспециалист – специалист ТРЗ, Счетоводител, директор, длъжностно лице отговарящо за архивохранилището, определено със Заповед на Директор и Дииректорът, пожарогасители, преминато обучение на персонала за познаване на нормативната уредба в областта на защитата на личните данни и опасностите за личните данни, обработвани от администратора; съгласие от всички работници/ служители на администратора за поемане на задължение за неразпространение на личните данни. Болничните листове се съхраняват отделно от трудовите досиета на работниците/служителите.
14. Оценка на риска – нисък.
15. Изисква ли се оценка на въздействие? Ако да – оценката. – НЕ.

3. Подбор на персонал

1. Описание на регистъра – извършване на подбор на персонала и поддържане на

необходимата в тази връзка документация.
2. Служители, които работят с регистъра – директор, заместник-директори, други работници/служители, които участват в даден подбор.
3. Описание на дейността по събиране на лични данни – от самите субекти на данните.
4. Цели на събирането – извършване на подбор на кандидатите за работа в училището, избиране на определен кандидат, с когото да бъде сключен договор.
5. Законово основание – договорно основание (чл. 6, пар. 1, т. "Б" от ОРЗД)
6. Категории лични данни, които се обработват – име, ЕГН, адрес, контакти (телефон или e-mail), информация за трудовия стаж и професионалния опит (включително заемани длъжности, работно време, стаж по специалността), информация за подбор (включително копия от разрешителни за работа, препоръки и друга информация, посочени в автобиография и придружително писмо или предоставена по друг начин чрез процеса на кандидатстване), информация относно трудова дисциплина.
7. Категории субекти на лични данни – кандидати за работа.
8. Получатели на лични данни - МОН или друга държавна/общинска институция, извършваща проверка относно процеса по подбор на персонал.
9. Име на държавата или международната организация в случай на предаване на лични данни в друга държава – няма.
10. Гаранции за прехвърляния на лични данни към трети държави или международни организации (ако е приложимо) – няма.
11. График със срокове на изтриване и основанието за срока, ако е възможно – Според Типова номенклатура на делата със срокове за съхраняване, утвърдена от Държавен архив Пловдив-м. Декември 2016г. -3 год.
12. Локация на личните данни –в стаята на специалист ТРЗ с контролиран достъп до документите, шкаф с ключ и СОТ
13. Общо описание на техническите и организационни мерки за сигурност - охрана на сградата, видеонаблюдение, контролиран достъп до тях, шкаф с ключ, копие от който имат хората, които работят с тях специалист ТРЗ, Счетоводител, директор, длъжностно лице отговарящо за архивохранилището, определено със Заповед на Директор и Директор на училището, пожарогасители, преминато обучение на персонала за познаване на нормативната уредба в областта на защитата на личните данни и опасностите за личните данни, обработвани от администратора; съгласие от всички работници/ служители на администратора за поемане на задължение за неразпространение на личните данни.
14. Оценка на риска – нисък.
15. Изисква ли се оценка на въздействие? Ако да – оценката. – НЕ.

4. Проекти по Еразъм

1. Описание на регистъра – осъществяване на самия проект (кратко описание в 1 изр. на проекта).
2. Служители, които работят с регистъра – Директор, Счетоводител, специалист ТРЗ, ЗАС, ръководителят на проекта, МОН, учители определени със заповед на директора, участващи в проекта. и организатори или участници, имащи законен достъп до лични данни и упълномощените потребители на електронната деловодна система .
3. Описание на дейността по събиране на лични данни – от самите субекти.
4. Цели на събирането - осъществяване на самия проект и поддържане на необходимата документация, свързана с него.
5. Законово основание – договорно основание (чл. 6, пар. 1, т. "Б" от ОРЗД).

6. Категории лични данни, които се обработват – име, ЕГН , телефон , адрес, номер на лична карта, образователан степен и номер на диплома, квалификации.
7. Категории субекти на лични данни – работници/служители или ученици.
8. Получатели на лични данни –
9. Име на държавата или международната организация в случай на предаване на лични данни в друга държава –
10. Гаранции за прехвърляния на лични данни към трети държави или международни организации (ако е приложимо) - Определяне на задълженията на страните спрямо личните данни и изискване от международната оргаизация да поеме задължение за неразпространението им.
11. График със срокове на изтриване и основанието за срока, ако е възможно – 5 год след приключване на проекта в архивихранилището на Училището.
12. Локация на личните данни – къде се
13. Общо описание на техническите и организационни мерки за сигурност - охрана на сградата, СОТ, видеонаблюдение, контролиран достъп до тях, шакф с ключ, копие от който имат хората, които работят с тях Директор, Счетоводител, специалист ТРЗ, ръководителят на проекта, пожарогасители, преминато обучение на персонала за познаване на нормативната уредба в областта на защитата на личните данни и опасностите за личните данни, обработвани от администратора; съгласие от всички работници/ служители на администратора за поемане на задължение за неразпространение на личните данни. Определяне на задълженията на страните спрямо личните данни и изискване от международната оргаизация да поеме задължение за неразпространението им.
14. Оценка на риска – нисък.
15. Изисква ли се оценка на въздействие? Ако да – оценката. – НЕ.

5. Видеонаблюдение

1. Описание на регистъра – извършване на видеонаблюдение в сградите и двора на училището.
2. Служители, които работят с регистъра – Домакин, ЗАС, администратор, Директор
3. Описание на дейността по събиране на лични данни – чрез видеокамери.
4. Цели на събирането – опазване живота и здравето на учениците, работниците/служителите и всички посетители в училището. Опазване имуществото на училището, в това число и всички документи, повечето от които съдържат лични данни.
5. Законово основание - легитимен интерес на администратора и жизненоважни интереси (чл. 6, пар. 1, т. "е" и б. "г" от ОРЗД).
6. Категории лични данни, които се обработват – физическа идентичност – образ и звук.
7. Категории субекти на лични данни – всички посетители на училището.
8. Получатели на лични данни - МВР и други оправомощени органи в предвидените от закон случаи.
9. Име на държавата или международната организация в случай на предаване на лични данни в друга държава – няма.
10. Гаранции за прехвърляния на лични данни към трети държави или международни организации (ако е приложимо)- няма.
11. График със срокове на изтриване и основанието за срока, ако е възможно – 2 месеца.
12. Локация на личните данни – сървър, който се намира в определено за целта помещение – в канцеларията на домакин, чиято врата се заключва с ключ.

13. Общо описание на техническите и организационни мерки за сигурност - охрана на сградата, СОТ, видеонаблюдение, контролиран достъп до тях, шакф с ключ, копие от който имат хората, които работят с тях Директор, домакин, ЗАС, пожарогасители, преминато обучение на персонала за познаване на нормативната уредба в областта на защитата на личните данни и опасностите за личните данни, обработвани от администратора; съгласие от всички работници/ служители на администратора за поемане на задължение за неразпространение на личните данни. Достъп до записите в сървъра имат само определените със заповед служители- администратор. Като сървърт е в помещение, чиято врата се заключва с ключ, който имат само домакин, директор, ЗАС
14. Оценка на риска – нисък.
15. Изисква ли се оценка на въздействие? Ако да – оценката. – НЕ.

6. Основна образователна дейност

1. Описание на регистъра – осъществяване на обучението на учениците и оценяването им.
2. Служители, които работят с регистъра – директор, заместник-директори, всички учители.
3. Описание на дейността по събиране на лични данни – от субекта на данните (или неговия родител/настойник), а о ценките – от учителите.
4. Цели на събирането - осъществяване на обучението на учениците и оценяването им.
5. Законово основание - чл. 6, пар. 1, т. “В” от ОРЗД – ЗПУО, Наредба № 8/11.08.2016 г. на МОН и приложимите нормативни актове.
6. Категории лични данни, които се обработват – име, дата на раждане, адрес, оценки и др., които са в дневниците, име на родители, телефони за връзка, имейли, образобателна степен
7. Категории субекти на лични данни – ученици и родители
8. Получатели на лични данни – МОН, предвидени в закон други организации.
9. Име на държавата или международната организация в случай на предаване на лични данни в друга държава – няма.
10. Гаранции за прехвърляния на лични данни към трети държави или международни организации (ако е приложимо) – няма.
11. График със срокове на изтриване и основанието за срока, ако е възможно – личните данни, съдържащи се в дневниците – 5 години.
12. Локация на личните данни – дневниците се съхраняват в учителската стая.
13. Общо описание на техническите и организационни мерки за сигурност - охрана на сградата, СОТ, видеонаблюдение, контролиран достъп до тях, пожарогасители, преминато обучение на персонала за познаване на нормативната уредба в областта на защитата на личните данни и опасностите за личните данни, обработвани от администратора; съгласие от всички работници/служители на администратора за поемане на задължение за неразпространение на личните данни. С дневника на определен клас може да работи само директорът, заместник-директорите, класният ръководител и учителите само на този определен клас.
14. Оценка на риска – нисък.
15. Изисква ли се оценка на въздействие? Ако да – оценката. – НЕ.

7. Поддържане на необходимата документация, свързана с образователната дейност

1. Описание на регистъра – документи, съдържащи лични данни.
2. Служители, които работят с регистъра – директор, заместник-директори, учители.
3. Описание на дейността по събиране на лични данни – от самите субекти на данните (или

техните родители/настойници), от учителите.
4. Цели на събирането - Поддържане на необходимата документация, свързана с образователната дейност.
5. Законово основание - чл. 6, пар. 1, т. "В" от ОРЗД – ЗПУО, Наредба № 8/11.08.2016 г. на МОН и приложимите нормативни актове.
6. Категории лични данни, които се обработват – име, ЕГН, дата на раждане, адрес на учениците, родителите/настойниците, данни за общопрактикуващия им лекар, оценки на учениците, здравословното им състояние, имейли, номера на телефони, Решения на ТЕЛК.
7. Категории субекти на лични данни – ученици.
8. Получатели на лични данни – МОН чрез системата НЕИСПУО.
9. Име на държавата или международната организация в случай на предаване на лични данни в друга държава – няма.
10. Гаранции за прехвърляния на лични данни към трети държави или международни организации (ако е приложимо) – няма.
11. График със срокове на изтриване и основанието за срока, ако е възможно –
Книга за подлежащите на задължително обучение до 16 години, Регистрационни книги за издадените документи за завършена степен на образование, Регистър на издадени удостоверения за придобита квалификационна степен, лични картони на учениците, – 50 години,
Дневник – 5 години,
Копия от документи на кандитатстващи ученици, Отпускни удостоверения, Съобщения, (уведомителни писма) до родители за допуснати неизвинени отсъствия и последващи наказателни актове, Заявления за участие в класиране, заявления за записване, Документи за прием след I, II и III класиране -списъци, заявления, тетрадки за завеждане на класирани ученици, Удостоверения за преместване на ученик- срок на съхранение 3 години.
Протокол за резултатите от писмен, устен, приравнителен и поправителен изпит, Протокол на зрелостната комисия за окончателните резултати, Протокол на комисията за придобиване на професионална квалификация за окончателните резултати от държавните квалификационни и зрелостни изпити, Протокол на комисията за удостоверяване на завършено начално образование – срок на съхранение 50 години.
Справки за успеха по години и хорариум учебни часове- срок на съхранение 3 години. Молби и заявления за ЗИП,СИП и др. форми на обучение- срок на съхранение 3 години.

Учебни планове и програми, Годишни планове и отчети, Отчети на документите с фабрична номерация- срок на съхранение постоянен
12. Локация на личните данни – След приключване на текущата учебна година, се архивират в архивохранилището на училището
13. Общо описание на техническите и организационни мерки за сигурност - охрана на сградата, СОТ, видеонаблюдение, контролиран достъп до тях, пожарогасители, преминато обучение на персонала за познаване на нормативната уредба в областта на защитата на личните данни и опасностите за личните данни, обработвани от администратора; съгласие от всички работници/служители на администратора за поемане на задължение за неразпространение на личните данни. С дневника на определен клас може да работи само директорът, заместник-директорите, класният ръководител и учителите, които преподават само на този определен клас.
14. Оценка на риска – нисък.
15. Изисква ли се оценка на въздействие? Ако да – оценката. – НЕ.

8. Издаване на видове удостоверения за ученици/ бивши ученици

1. Описание на регистъра - видове удостоверения и техните дубликати за ученици/бивши ученици като такива за завършен клас или степен на образование.
2. Служители, които работят с регистъра – директор; заместник директори; учител, определен със заповед на директора, и длъжностно лице работещо с електронната деловодна система
3. Описание на дейността по събиране на лични данни – някои данни – от самите субекти (или техните родители/настойници), други – от документите, поддържани от училището.
4. Цели на събирането – да се издадат необходимите в даден момент удостоверения на ученици/бивши ученици като такива за завършен клас или степен на образование.
5. Законово основание - чл. 6, пар. 1, т. "В" от ОРЗД – ЗПУО, Наредба № 8/11.08.2016 г. на МОН, както и упражняването на официални правомощия, които са предоставени на администратора (чл. 6, пар. 1, т. "Д" от ОРЗД) (чл. 6, пар. 1, т. "Б" от ОРЗД).
6. Категории лични данни, които се обработват – име, ЕГН, оценки, завършени клас или степен на образование.
7. Категории субекти на лични данни – ученици/бивши ученици.
8. Получатели на лични данни – в предвидените от закон случаи – МОН или други образователни институции.
9. Име на държавата или международната организация в случай на предаване на лични данни в друга държава – няма.
10. Гаранции за прехвърляния на лични данни към трети държави или международни организации (ако е приложимо) – няма.
11. График със срокове на изтриване и основанието за срока, ако е възможно – Според Наредба № 8/11.08.2016 г. и типова номенклатура, утвърдена Държавен архив –Пловдив съхранението е според ценността на документа.
12. Локация на личните данни – След приключване на текущата учебна година, се архивират в архивохранилището на училището
13. Общо описание на техническите и организационни мерки за сигурност сигурност - охрана на сградата, СОТ, видеонаблюдение, контролиран достъп до тях, пожарогасители, преминато обучение на персонала за познаване на нормативната уредба в областта на защитата на личните данни и опасностите за личните данни, обработвани от администратора; съгласие от всички работници/служители на администратора за поемане на задължение за неразпространение на личните данни. Удостоверенията могат да се издават и да се работи по тях само от директора или оправомощено от него лице.
14. Оценка на риска – нисък.
15. Изисква ли се оценка на въздействие? Ако да – оценката. – НЕ.

9. Квалификация на персонала

1. Описание на регистъра – осъществяване на обучения на персонала.
2. Служители, които работят с регистъра – директор, заместник-директори зас, Счетоводител и специалист ТРЗ
3. Описание на дейността по събиране на лични данни – от самите субекти.
4. Цели на събирането - актуализиране и усъвършенстване на придобити и/или придобиване на нови допълнителни компетентности в научната, педагогическата и методическата подготовка за професионалното развитие на педагогическите специалисти - въвеждаща и продължаваща квалификация.
5. Законово основание - чл. 6, пар. 1, т. "В" от ОРЗД – ЗПУО, Наредба № 12/01.09.2016 г. на

МОН и приложимите нормативни актове
6. Категории лични данни, които се обработват – име, ЕГН, професионална квалификация, резултати от проведените обучения/квалификации.
7. Категории субекти на лични данни – работници/служители.
8. Получатели на лични данни – Организации и фирми, по одобрен спъсък на МОН, свързани с професионална квалификация на учителите.
9. Име на държавата или международната организация в случай на предаване на лични данни в друга държава – няма.
10. Гаранции за прехвърляния на лични данни към трети държави или международни организации (ако е приложимо) - няма.
11. График със срокове на изтриване и основанието за срока, ако е възможно – Според Наредба № 8/11.08.2016 г., наредба № 12 от 1 септември 2016 г. за статута и професионалното развитие на учителите, директорите и другите педагогически специалисти и типова номенклатура, утвърдена Държавен архив –Пловдив съхранението е според ценността на документа
12. Локация на личните данни – дирекция и учителска стая.
13. Общо описание на техническите и организационни мерки за сигурност - охрана на сградата, СОТ, видеонаблюдение, контролиран достъп до тях, пожарогасители, преминато обучение на персонала за познаване на нормативната уредба в областта на защитата на личните данни и опасностите за личните данни, обработвани от администратора; съгласие от всички работници/ служители на администратора за поемане на задължение за неразпространение на личните данни.
14. Оценка на риска – нисък.
15. Изисква ли се оценка на въздействие? Ако да – оценката. – НЕ.

10. Прием на ученици

1. Описание на регистъра – прием на ученици.
2. Служители, които работят с регистъра – директор, заместник-директор, учители, определени с заповед на директор, длъжностно лице, работещо с електронната деловодна система на училището
3. Описание на дейността по събиране на лични данни – от самите субекти на данни (съответно техните родители/настойници).
4. Цели на събирането – да се получи необходимата информация относно ученика, за да може да се провежда нормално учебния процес и да се поддържа необходимата по закон документация свързана с него.
5. Законово основание - чл. 6, пар. 1, т. “В” от ОРЗД – ЗПУО, Наредба № 8/11.08.2016 г. на МОН и други приложими нормативни актове.
6. Категории лични данни, които се обработват –име, ЕГН, дата на раждане, адрес на учениците, родителите/настойниците, данни за общопрактикуващия им лекар, оценки на учениците, здравословното им състояние, имейли, номера на телефони, Решения на ТЕЛК
7. Категории субекти на лични данни– ученици и техните родители/настойници.
8. Получатели на лични данни – МОН.
9. Име на държавата или международната организация в случай на предаване на лични данни в друга държава – няма.
10. Гаранции за прехвърляния на лични данни към трети държави или международни организации (ако е приложимо) – няма.

11. График със срокове на изтриване и основанието за срока, ако е възможно - Книга за подлежащите на задължително обучение до 16 години – 50 години, Дневник – 5 години и Документи за прием след I, II и III класиране -списъци, заявления, тетрадки за завеждане на класирани ученици, Удостоверения за преместване на ученик- срок на съхранение 3 годин.
12. Локация на личните данни – В дирекция до приключване на книгите.
13. Общо описание на техническите и организационни мерки за сигурност - охрана на сградата, СОТ, видеонаблюдение, контролиран достъп до тях, пожарогасители, преминато обучение на персонала за познаване на нормативната уредба в областта на защитата на личните данни и опасностите за личните данни, обработвани от администратора; съгласие от всички работници/служители на администратора за поемане на задължение за неразпространение на личните данни.
14. Оценка на риска – нисък.
15. Изисква ли се оценка на въздействие? Ако да – оценката. – НЕ.

11. Трудова медицина

1. Описание на регистъра – извършване на необходимите прегледи на работниците/служителите; превенция на заболяванията; поддържане на необходимата документация за това.
2. Служители, които работят с регистъра – Заместник-директор УПД, ЗАС, специалист ТРЗ
3. Описание на дейността по събиране на лични данни - от самите субекти на данните и от проведените им прегледи.
4. Цели на събирането - извършванена необходимите прегледи на работниците/служителите и превенция на заболяванията, и поддържане на необходимата документация за това.
5. Законово основание - чл. 6, пар. 1, т. “В” от ОРЗД - Закона за здравословни и безопасни условия на труд.
6. Категории лични данни, които се обработват – име, ЕГН, здравословно състояние.
7. Категории субекти на лични данни – работници/служители.
8. Получатели на лични данни – няма.
9. Име на държавата или международната организация в случай на предаване на лични данни в друга държава – няма.
10. Гаранции за прехвърляния на лични данни към трети държави или международни организации (ако е приложимо) – няма.
11. График със срокове на изтриване и основанието за срока.
12. Локация на личните данни – в канцелария на специалист ТРЗ

13. Общо описание на техническите и организационни мерки за сигурност - охрана на сградата, СОТ, видеонаблюдение, контролиран достъп до тях, пожарогасители, преминато обучение на персонала за познаване на нормативната уредба в областта на защитата на личните данни и опасностите за личните данни, обработвани от администратора; съгласие от всички работници/служители на администратора за поемане на задължение за неразпространение на личните данни.
14. Оценка на риска – нисък.
15. Изисква ли се оценка на въздействие? Ако да – оценката – НЕ.

12. Здравно обслужване

1. Описание на регистъра – информация за здравния статус на учениците.
2. Служители, които работят с регистъра – медицинско лице на трудов договор към

общината (обработващ личните данни).
3. Описание на дейността по събиране на лични данни – от самите субекти на данните.
4. Цели на събирането - информация за здравния статус на учениците и превенция на заболяванията.
5. Законово основание - чл. 6, пар. 1, т. “В” от ОРЗД - ЗПУО.
6. Категории лични данни, които се обработват – име, ЕГН, клас, здравословно състояние.
7. Категории субекти на лични данни – ученици.
8. Получатели на лични данни – РЗИ, общопрактикуващи лекари.
9. Име на държавата или международната организация в случай на предаване на лични данни в друга държава – няма.
10. Гаранции за прехвърляния на лични данни към трети държави или международни организации (ако е приложимо) – няма.
11. График със срокове на изтриване и основанието за срока, ако е възможно – до завършване на учениците
12. Локация на личните данни – в медицинския кабинет.
13. Общо описание на техническите и организационни мерки за сигурност - охрана на сградата, СОТ, видеонаблюдение, контролиран достъп до тях, пожарогасители, преминато обучение на персонала за познаване на нормативната уредба в областта на защитата на личните данни и опасностите за личните данни, обработвани от администратора; съгласие от всички работници/служители на администратора за поемане на задължение за неразпространение на личните данни. Договор с обработващия лични данни (медицинското лице). не
14. Оценка на риска – нисък.
15. Изисква ли се оценка на въздействие? Ако да – оценката. – НЕ.

13. Издаване на служебни бележки, справки и удостоверения на настоящи и бивши служители

1. Описание на регистъра - издаване на служебни бележки, справки и удостоверения на настоящи и бивши служители.
2. Служители, които работят с регистъра – в зависимост от вида удостоверение - директор, ЗАС, счетоводител, касиер, специалист ТРЗ, секретар .
3. Описание на дейността по събиране на лични данни – от самите субекти и от документите, поддържани в училището.
4. Цели на събирането - издаване на служебни бележки, справки и удостоверения на настоящи и бивши служители по инициатива на настоящи и бивши служители.
5. Законово основание - чл. 6, пар. 1, т. “В” от ОРЗД – КТ, КСО, ЗПУО и други.
6. Категории лични данни, които се обработват – в зависимост от вида удостоверение - име, ЕГН, трудов стаж, заплата, лекторски часове, хорариуми и др.
7. Категории субекти на лични данни - настоящи и бивши служители.
8. Получатели на лични данни – няма.
9. Име на държавата или международната организация в случай на предаване на лични данни в друга държава – няма.
10. Гаранции за прехвърляния на лични данни към трети държави или международни организации (ако е приложимо) – няма.
11. График със срокове на изтриване и основанието за срока, ако е възможно.
12. Локация на личните данни –във входяща или изходяща документация с определените

от Държавен архив срокове на съхранение
13. Общо описание на техническите и организационни мерки за сигурност - охрана на сградата, СОТ, видеонаблюдение, контролиран достъп до тях, пожарогасители, преминато обучение на персонала за познаване на нормативната уредба в областта на защитата на личните данни и опасностите за личните данни, обработвани от администратора; съгласие от всички работници/ служители на администратора за поемане на задължение за неразпространение на личните данни.
14. Оценка на риска – нисък.
15. Изисква ли се оценка на въздействие? Ако да – оценката. – НЕ.

14. Дарения

1. Описание на регистъра – поддържане на регистър на даренията, направени за училището, и издаване на свидетелство за дарение.
2. Служители, които работят с регистъра – Домакин,ЗАС и членовете на комисията , определени за всяка календарна година със Заповед на директора
3. Описание на дейността по събиране на лични данни – от самите субекти на данните.
4. Цели на събирането – поддържане на регистър с описани направените дарения за училището и издаване на свидетелства за дарение.
5. Законово основание - чл. 6, пар. 1, т. “В” от ОРЗД – ЗПУО, Наредба № 8/11.08.2016 г. на МОН и др.
6. Категории лични данни, които се обработват – име, ЕГН, вид на дарението.
7. Категории субекти на лични данни – дарители.
8. Получатели на лични данни – няма.
9. Име на държавата или международната организация в случай на предаване на лични данни в друга държава – няма.
10. Гаранции за прехвърляния на лични данни към трети държави или международни организации (ако е приложимо) – няма.
11. График със срокове на изтриване и основанието за срока, ако е възможно – 20 години. (Наредба № 8/11.08.2016 г.)
12. Локация на личните данни – В канцеларията на домакин
13. Общо описание на техническите и организационни мерки за сигурност - охрана на сградата, СОТ, видеонаблюдение, контролиран достъп до тях, пожарогасители, преминато обучение на персонала за познаване на нормативната уредба в областта на защитата на личните данни и опасностите за личните данни, обработвани от администратора; съгласие от всички работници/служители на администратора за поемане на задължение за неразпространение на личните данни.
14. Оценка на риска – нисък.
15. Изисква ли се оценка на въздействие? Ако да – оценката. – НЕ.

15. Изпити

1. Описание на регистъра – провеждане на изпити.
2. Служители, които работят с регистъра – директор, заместник-директори, учители.
3. Описание на дейността по събиране на лични данни – от самите субекти на данни.
4. Цели на събирането – да се идентифицират коректно участниците в изпитите и да им се поставят заслужените оценки.
5. Законово основание - чл. 6, пар. 1, т. “В” от ОРЗД – ЗПУО, Наредба № 8/11.08.2016 г. на

МОН.
6. Категории лични данни, които се обработват – име, ЕГН, резултат (оценка) от изпита.
7. Категории субекти на лични данни – ученици.
8. Получатели на лични данни – МОН.
9. Име на държавата или международната организация в случай на предаване на лични данни в друга държава – няма.
10. Гаранции за прехвърляния на лични данни към трети държави или международни организации (ако е приложимо) – няма.
11. График със срокове на изтриване и основанието за срока, ако е възможно – Протокол за резултатите от писмен, устен, приравнителен и поправителен изпит, Протокол на зрелостната комисия за окончателните резултати, Протокол на комисията за придобиване на професионална квалификация за окончателните резултати от държавните квалификационни и зрелостни изпити, Протокол на комисията за удостоверяване на завършено средно образование – срок на съхранение 50 години.

12. Локация на личните данни – До приключване на учебната година в дирекцията, след това се архивират в архивохранилището на училището.
13. Общо описание на техническите и организационни мерки за сигурност - охрана на сградата, СОТ, видеонаблюдение, контролиран достъп до тях, пожарогасители, преминато обучение на персонала за познаване на нормативната уредба в областта на защитата на личните данни и опасностите за личните данни, обработвани от администратора; съгласие от всички работници/служители на администратора за поемане на задължение за неразпространение на личните данни. Резулатите се псевдонимизират.
14. Оценка на риска – нисък.
15. Изисква ли се оценка на въздействие? Ако да – оценката. – НЕ.

16. Състезания, олимпиади

1. Описание на регистъра – провеждане на състезания и олимпиади.
2. Служители, които работят с регистъра – директор, учители, домакин, заместни-директори,
3. Описание на дейността по събиране на лични данни – от самите субекти на данни.
4. Цели на събирането - да се идентифицират коректно участниците в състезанията или олимпиадите и да им се поставят заслужените оценки.
5. Законово основание - чл. 6, пар. 1, т. “В” от ОРЗД – ЗПУО, Наредба № 8/11.08.2016 г. на МОН.
6. Категории лични данни, които се обработват - име, ЕГН, резултат (оценка) от изпита.
7. Категории субекти на лични данни – ученици.
8. Получатели на лични данни – МОН.
9. Име на държавата или международната организация в случай на предаване на лични данни в друга държава – няма.
10. Гаранции за прехвърляния на лични данни към трети държави или международни организации (ако е приложимо) – няма.
11. График със срокове на изтриване и основанието за срока, ако е възможно – Една календарна година
12. Локация на личните данни – В архив на училището
13. Общо описание на техническите и организационни мерки за сигурност - охрана на сградата, СОТ, видеонаблюдение, контролиран достъп до тях, пожарогасители, преминато

обучение на персонала за познаване на нормативната уредба в областта на защитата на личните данни и опасностите за личните данни, обработвани от администратора; съгласие от всички работници/служители на администратора за поемане на задължение за неразпространение на личните данни. Резулатите се псевдонимизират.
14. Оценка на риска – нисък.
15. Изисква ли се оценка на въздействие? Ако да – оценката. – НЕ.

17. Стипендии

1. Описание на регистъра – изплащане на стипендии.
2. Служители, които работят с регистъра – учители, счетоводител, директор, заместник-директори.
3. Описание на дейността по събиране на лични данни – от самите субекти, а оценките се сравняват от учителите в дневниците на класовете.
4. Цели на събирането – коректно определяне и изплащане на стипендиите.
5. Законово основание - чл. 6, пар. 1, т. “В” от ОРЗД – ЗПУО, Заповеди на Община Марица.
6. Категории лични данни, които се обработват – име, ЕГН, успех (оценки), клас, информация за родители/настойници, братя, сестри, банкова информация.
7. Категории субекти на лични данни – ученици.
8. Получатели на лични данни – банката – само информацията, необходима за изплащане на стипендията на всеки ученик.
9. Име на държавата или международната организация в случай на предаване на лични данни в друга държава – няма.
10. Гаранции за прехвърляния на лични данни към трети държави или международни организации (ако е приложимо) – няма.
11. График със срокове на изтриване и основанието за срока, ако е възможно – До завършване на учениците в счетоводство и след това се архивират според нужните срокове за съхранение
12. Локация на личните данни – В счетоводство или архивохранилището на училището
13. Общо описание на техническите и организационни мерки за сигурност - охрана на сградата, СОТ, видеонаблюдение, контролиран достъп до тях, пожарогасители, преминато обучение на персонала за познаване на нормативната уредба в областта на защитата на личните данни и опасностите за личните данни, обработвани от администратора; съгласие от всички работници/ служители на администратора за поемане на задължение за неразпространение на личните данни.
14. Оценка на риска – нисък.
15. Изисква ли се оценка на въздействие? Ако да – оценката. – НЕ.

18. Производствени практики/Стажове на ученици извън училище

1. Описание на регистъра - стажове на ученици извън училище.
2. Служители, които работят с регистъра – директор, заместник-директори, учители.
3. Описание на дейността по събиране на лични данни – от самите субекти.
4. Цели на събирането – провеждане на стажовете.
5. Законово основание - чл. 6, пар. 1, т. “В” от ОРЗД, ЗПУО,
6. Категории лични данни, които се обработват – име, ЕГН, клас, професия, оценки.
7. Категории субекти на лични данни – ученици.
8. Получатели на лични данни – съответната фирма/организация, в която се осъществява

стажът.
9. Име на държавата или международната организация в случай на предаване на лични данни в друга държава – няма.
10. Гаранции за прехвърляния на лични данни към трети държави или международни организации (ако е приложимо) – няма.
11. График със срокове на изтриване и основанието за срока, ако е възможно – до завършването ученицте.
12. Локация на личните данни – договорите между фирмите осъществяващи практическото обучение се съхраняват в дирекцията, след това се архивират и се съхраняват в архивохранилището на училището.
13. Общо описание на техническите и организационни мерки за сигурност - охрана на сградата, СОТ, видеонаблюдение, контролиран достъп до тях, пожарогасители, преминато обучение на персонала за познаване на нормативната уредба в областта на защитата на личните данни и опасностите за личните данни, обработвани от администратора; съгласие от всички работници/ служители на администратора за поемане на задължение за неразпространение на личните данни. Определяне на задълженията на страните спрямо личните данни и изискване от организацията, в която се провежда стажът, да поеме задължение за неразпространението им.
14. Оценка на риска – нисък.
15. Изисква ли се оценка на въздействие? Ако да – оценката. – НЕ.

19. Участие в национални програми

1. Описание на регистъра – реализиране на целите на програмата.
2. Служители, които работят с регистъра – директор, заместник-директори, счетоводители, домакин, ЗАС, учители
3. Описание на дейността по събиране на лични данни – от самите субекти.
4. Цели на събирането - реализиране на целите на програмата.
5. Законово основание - чл. 6, пар. 1, т. “В” от ОРЗД – ЗПУО,
6. Категории лични данни, които се обработват – име, ЕГН, адрес, данни на родители ако ученика е под 18 години и няма права да подписва договори, телефон за връзка, имейл
7. Категории субекти на лични данни – ученици.
8. Получатели на лични данни – МОН, ЦРЧР- София, партньорски организации по НП
9. Име на държавата или международната организация в случай на предаване на лични данни в друга държава – няма.
10. Гаранции за прехвърляния на лични данни към трети държави или международни организации (ако е приложимо) – няма.
11. График със срокове на изтриване и основанието за срока, ако е възможно – До приключване на Националната програма в дирекция, счетоводство . След това се архивират със срок на съхранение 5 години.
12. Локация на личните данни – дирекция, счетоводство, архивохранилище
13. Общо описание на техническите и организационни мерки за сигурност - охрана на сградата, СОТ, видеонаблюдение, контролиран достъп до тях, пожарогасители, преминато обучение на персонала за познаване на нормативната уредба в областта на защитата на личните данни и опасностите за личните данни, обработвани от администратора; съгласие от всички работници/служители на администратора за поемане на задължение за неразпространение на личните данни.

14. Оценка на риска – нисък.
15. Изисква ли се оценка на въздействие? Ако да – оценката – НЕ.

20. Регистър „библиотека“

1. Описание на регистъра – библиотечна дейност.
2. Служители, които работят с регистъра – библиотекар.
3. Описание на дейността по събиране на лични данни – от самите субекти.
4. Цели на събирането – водене на библиотечен „картон“.
5. Законово основание - чл. 6, пар. 1, т. “В” от ОРЗД – ЗОБ.
6. Категории лични данни, които се обработват – име, клас, адрес, телефон.
7. Категории субекти на лични данни – ученици, работници/ служители.
8. Получатели на лични данни – няма.
9. Име на държавата или международната организация в случай на предаване на лични данни в друга държава – няма.
10. Гаранции за прехвърляния на лични данни към трети държави или международни организации (ако е приложимо) – няма.
11. График със срокове на изтриване и основанието за срока, ако е възможно – До приключване на библиотечния картон на ученика.
12. Локация на личните данни – в библиотеката.
13. Общо описание на техническите и организационни мерки за сигурност - охрана на сградата, СОТ, видеонаблюдение, контролиран достъп до тях, пожарогасители, преминато обучение на персонала за познаване на нормативната уредба в областта на защитата на личните данни и опасностите за личните данни, обработвани от администратора; съгласие от всички работници/служители на администратора за поемане на задължение за неразпространение на личните данни.
14. Оценка на риска – нисък.
15. Изисква ли се оценка на въздействие? Ако да – оценката. – НЕ.

21. Осъществяване на обща и/или на допълнителна подкрепа

1. Описание на регистъра - НАРЕДБА за приобщаващото образование Обн. - ДВ, бр. 86 от 27.10.2017 г., в сила от 27.10.2017 г. Приета с ПМС № 232 от 20.10.2017 ,обществените отношения, свързани с осигуряване на приобщаващото образование на децата и учениците в системата на предучилищното и училищното образование, както и дейността на институциите в тази система за предоставяне на подкрепа за личностно развитие на децата и учениците
2. Служители, които работят с регистъра – педагогически съветник, психолог, учители, директор, заместник-директори и стуктури и организации осъществяващи на обща и/или допълнителна подкрепа.
3. Описание на дейността по събиране на лични данни – име, ЕГН, адрес , телефон, здравословно състочние, дании на родител или настойник
4. Цели на събирането – според Наредба за приобщаващото образование и ЗПУО
5. Законово основание – Наредба за приобщаващото образование.
6. Категории лични данни, които се обработват -
7. Категории субекти на лични данни -
8. Получатели на лични данни -
9. Име на държавата или международната организация в случай на предаване на лични

данни в друга държава -
10. Гаранции за прехвърляния на лични данни към трети държави или международни организации (ако е приложимо) -
11. График със срокове на изтриване и основанието за срока, ако е възможно .
12. Локация на личните данни – дирекция и учителска стая.
13. Общо описание на техническите и организационни мерки за сигурност -
14. Оценка на риска -
15. Изисква ли се оценка на въздействие? Ако да – оценката.

22. Счетоводство

1. Описание на регистъра – счетоводство.
2. Служители, които работят с регистъра – счетоводител, счетоводител, домакин-касиер.
3. Описание на дейността по събиране на лични данни – от самите субекти на данните.
4. Цели на събирането – за осъществяване на счетоводната дейност.
5. Законово основание - чл. 6, пар. 1, т. "В" от ОРЗД – ЗАКОН за счетоводството.
6. Категории лични данни, които се обработват – име, ЕГН, банкова и финансова информация.
7. Категории субекти на лични данни – ученици, работници/служители.
8. Получатели на лични данни – банки, Община Марица, МОН, РУО.
9. Име на държавата или международната организация в случай на предаване на лични данни в друга държава – няма.
10. Гаранции за прехвърляния на лични данни към трети държави или международни организации (ако е приложимо) – няма.
11. График със срокове на изтриване и основанието за срока - Според утвърдена **Типова номенклатура** на делата със срокове за съхраняване на професионалните гимназии в Област Пловдив от м. Декември 2016г.

12. Локация на личните данни – В счетоводство или архивихранилище
13. Общо описание на техническите и организационни мерки за сигурност - охрана на сградата, СОТ, видеонаблюдение, контролиран достъп до тях, пожарогасители, преминато обучение на персонала за познаване на нормативната уредба в областта на защитата на личните данни и опасностите за личните данни, обработвани от администратора; съгласие от всички работници/служители на администратора за поемане на задължение за неразпространение на личните данни.
14. Оценка на риска – нисък.
15. Изисква ли се оценка на въздействие? Ако да – оценката. – НЕ.

23. Архив

1. Описание на регистъра - Закона за Националния архивен фонд, чл. 37, 38, 39 и 40 от Наредбата за реда за организирането, обработването, експертизата, съхраняването и използването на документите в учрежденските архиви на държавните и общинските институции
2. Служители, които работят с регистъра - ЗАС, секретар, специалист ТРЗ
3. Описание на дейността по събиране на лични данни.
4. Цели на събирането.
5. Законово основание.
6. Категории лични данни, които се обработват.

7. Категории субекти на лични данни.
8. Получатели на лични данни.
9. Име на държавата или международната организация в случай на предаване на лични данни в друга държава.
10. Гаранции за прехвърляния на лични данни към трети държави или международни организации (ако е приложимо).
11. График със срокове на изтриване и основанието за срока, ако е възможно.
12. Локация на личните данни.
13. Общо описание на техническите и организационните мерки за сигурност.
14. Оценка на риска.
15. Изисква ли се оценка на въздействие? Ако да – оценката.

24. Входящ регистър

1. Описание на регистъра. – Всички документи, които се получават в училището.
2. Служители, които работят с регистъра. – ЗАС, секретар, заместник-директори,
3. Описание на дейността по събиране на лични данни. – от подателите на документите (самите субекти на данните)
4. Цели на събирането. – администриране на входящите документие в училището
5. Законово основание. - чл. 6, пар. 1, т. “В” от ОРЗД – ЗПУО, Наредба № 8/11.08.2016 г. на МОН
6. Категории лични данни, които се обработват. – име на подателя и, при възможност, кратко описание на документа
7. Категории субекти на лични данни. – податели надокументи
8. Получатели на лични данни. - няма
9. Име на държавата или международната организация в случай на предаване на лични данни в друга държава. - няма
10. Гаранции за прехвърляния на лични данни към трети държави или международни организации (ако е приложимо). - няма
11. График със срокове на изтриване и основанието за срока, ако е възможно. – 10 г. (Наредба № 8 на МОН)
12. Локация на личните данни. – В канцелария.
13. Общо описание на техническите и организационните мерки за сигурност. - охрана на сградата, СОТ, видеонаблюдение, контролиран достъп до тях, пожарогасители, преминато обучение на персонала за познаване на нормативната уредба в областта на защитата на личните данни и опасностите за личните данни, обработвани от администратора; съгласие от всички работници/служители на администратора за поемане на задължение за неразпространение на личните данни.
14. Оценка на риска. – нисък.
15. Изисква ли се оценка на въздействие? Ако да – оценката. - не

25. Изходящ регистър

1. Описание на регистъра. - Всички документи, които излизат от училището
2. Служители, които работят с регистъра. – ЗАС, секретар, заместник-директори,
3. Описание на дейността по събиране на лични данни. – от самите субекти
4. Цели на събирането. - администриране на изходящите документие в училището
5. Законово основание. чл. 6, пар. 1, т. “В” от ОРЗД – ЗПУО, Наредба № 8/11.08.2016 г. на

МОН
6. Категории лични данни, които се обработват. - име на получателя и, при възможност, кратко описание на документа
7. Категории субекти на лични данни. - получатели
8. Получатели на лични данни. - няма
9. Име на държавата или международната организация в случай на предаване на лични данни в друга държава. - няма
10. Гаранции за прехвърляния на лични данни към трети държави или международни организации (ако е приложимо). - няма
11. График със срокове на изтриване и основанието за срока, ако е възможно. – 10 г. (Наредба № 8 на МОН)
12. Локация на личните данни. – В канцелария.
13. Общо описание на техническите и организационните мерки за сигурност. - охрана на сградата, СОТ, видеонаблюдение, контролиран достъп до тях, пожарогасители, преминато обучение на персонала за познаване на нормативната уредба в областта на защитата на личните данни и опасностите за личните данни, обработвани от администратора; съгласие от всички работници/служители на администратора за поемане на задължение за неразпространение на личните данни.
14. Оценка на риска. - нисък
15. Изисква ли се оценка на въздействие? Ако да – оценката. - не

26. Регистър на договорите

1. Описание на регистъра. - Всички договори, с изключение на трудовите
2. Служители, които работят с регистъра. – Счетоводител, секретар, ЗАС
3. Описание на дейността по събиране на лични данни. – от самите субекти
4. Цели на събирането. - администриране на договорите в училището
5. Законово основание. чл. 6, пар. 1, т. “В” от ОРЗД – ЗПУО, Наредба № 8/11.08.2016 г. на МОН
6. Категории лични данни, които се обработват. – Име на фирма или организация, Булстат, адрес, телефон , банкови сметки
7. Категории субекти на лични данни. - получатели
8. Получатели на лични данни. - няма
9. Име на държавата или международната организация в случай на предаване на лични данни в друга държава. - няма
10. Гаранции за прехвърляния на лични данни към трети държави или международни организации (ако е приложимо). - няма
11. График със срокове на изтриване и основанието за срока, ако е възможно. – 10 г. (Наредба № 8 на МОН) След изтичане на договора и одит 5 години
12. Локация на личните данни. – До приключване на класьора с договорите в дирекция. След архивиране в архивохранилището на училището.
13. Общо описание на техническите и организационните мерки за сигурност. - охрана на сградата, СОТ, видеонаблюдение, контролиран достъп до тях, пожарогасители, преминато обучение на персонала за познаване на нормативната уредба в областта на защитата на личните данни и опасностите за личните данни, обработвани от администратора; съгласие от всички работници/служители на администратора за поемане на задължение за

неразпространение на личните данни.
14. Оценка на риска. - нисък
15. Изисква ли се оценка на въздействие? Ако да – оценката. - не

Приложение 4.

... ...

ДЕКЛАРАЦИЯ
за неразпространение на лични данни

Подписаният/та *(име, презиме и фамилия)*
.....
На длъжност *(по длъжностна характеристика)*
.....
.....

Д Е К Л А Р И Р А М, ЧЕ :

1. Няма да разпространявам информация за личните данни на трети лица, станали ми известни при изпълнение на служебните ми задължения и няма да ги използвам за други цели, освен за прякото изпълнение на служебните ми задължения.
2. Запознат/а/ съм със законодателството за защита на личните данни.
3. Нося отговорност за опазване на документите, съдържащи лични данни.
4. Запознат/а/ съм, че при разгласяване, предоставяне, публикуване, използване или разпространяване по друг начин на факти и обстоятелства, представляващи лични данни, нося административно-наказателна отговорност по Закона за защита на личните данни, дисциплинарна отговорност по Кодекса на труда, а в предвидените случаи и наказателна отговорност, ако деянието съставлява състав на престъпление по Наказателния кодекс.

Дата: …… ДЕКЛАРАТОР:…….....
(подпис)

гр.……..

Приложение 5.

. . . . . .

Известие за обработване на лични данни
при обучение на ученици в училището

Администратор на лични данни: **.....**
Субект на лични данни:.....
/име, презиме, фамилия на ученика/

Относно следните лични данни: лични данни на ученика – егн, имена, адрес, гражданство, месторождение; здравна и медицинска информация (вкл. личен лекар, здравно-профилактични карти, заболявания, наличие на трайни увреждания и др.); информация за специални образователни потребности на лицата; информация за присъствие, отсъствия (причини за отсъствието) и успех (оценяване) на ученика; информация за полагане на изпити (национално външно оценяване, олимпиади, състезания, конкурси и др.); информация за издаване на удостоверения, свидетелства, ученически книжки и ученически лични карти; информация, необходима за предоставяне на награди; данни за родители и деца във връзка с предоставяне на социално подпомагане; данни за родители – име, телефон, ЕГН, месторабота, адрес, e-mail и др.; информация за членовете на обществения съвет – трите имена, адрес, месторабота, телефон, e-mail; информация за получени дарения; фото и видеоматериали, включително снимки на учениците за техни досиета или документи.

В качеството си на администратор на лични данни и изпълнявайки задълженията си съгласно Общия регламент за защита на данните декларирам, че ще използвам Вашите лични данни и личните данни на детето Ви, описани по-горе, за следната цел:
Попълване на необходимата документация и осъществяване на дейността на училището.

Законът изисква от нас да определим въз основа на кое законово основание обработваме различни категории лична информация и да Ви уведомим за основанията и нашите цели, спрямо всяка категория обработвани лични данни.

Ако основанието, на което обработваме Вашата лична информация, вече не е приложимо, ние незабавно ще прекратим обработването на Вашите данни.

Ако основанието се промени, тогава, ако това се изисква от закона, ние ще Ви уведомим за промяната, както и за всяко ново основание, при което сме установили, че можем да продължим да обработваме Вашата информация.

В повечето случаи ние обработваме съответните лични данни на базата на законово задължение, произтичащо от приложимата правна уредба *(Закон за предучилищното и училищното образование; НАРЕДБА № 8 от 11.08.2016 г. за информацията и документите за системата на предучилищното и училищното образование; НАРЕДБА № 10 от 2017 г. за познавателните книжки, учебниците и учебните помагала; НАРЕДБА за приобщаващото образование; НАРЕДБА за финансирането на институциите в системата на предучилищното и училищното образование; Наредба № 11 от 2016 г. за оценяване на резултатите от обучението на учениците; Наредба № 10 от 2016 г. за организация на дейностите в училищното образование; НАРЕДБА № 3 от 6 април 2017 г. за условията и реда за приемане и обучение на лицата, търсещи или получили*

международна закрила; НАРЕДБА № 2 от 24.01.2017 г. за регистъра на институциите в системата на предучилищното и училищното образование; НАРЕДБА за детските и ученическите туристически пътувания с обща цена, инициирани от институциите в системата на предучилищното и училищното образование; НАРЕДБА № 15 от 08.12.2016 г. за инспектирането на детските градини и училищата; НАРЕДБА № 13 от 21.09.2016 г. за гражданското, здравното, екологичното и интеркултурното образование; НАРЕДБА № 12 от 01.09.2016 г. за статута и професионалното развитие на учителите, директорите и другите педагогически специалисти; Наредба № 9 от 19 август 2016 г. за институциите в системата на предучилищното и училищното образование; Наредба № 6 от 11 август 2016 г. за усвояването на българския книжовен език; Конвенция за правата на детето; Закон за закрила на детето; Правилник за прилагане на закона за закрила на детето; ПМС № 100 от 08.06.2018 г. за създаване и функциониране на Механизъм за съвместна работа на институциите по обхващане и включване в образователната система на деца и ученици в задължителна предучилищна и училищна възраст).

Записи от системи за видеонаблюдение с охранителна цел - опазване на живота и здравето на учениците и служителите в училището, получени от разположените видеокамери.

Училището декларира, че личните Ви данни ще бъдат третирани като строго поверителни и няма да бъдат споделяни.

Ще се съхраняват Вашите лични данни не повече от предвидените в закона срокове: личните данни в личните картони/личните образователни дела на учениците се пазят 50 години, в дневниците - 5 години, Книга за подлежащите на задължително обучение до 16 години – 50 години, като данните ще бъдат съхранявани по следния начин: всички документи, съдържащи лични данни, се съхраняват при необходимите технически и организационни мерки за защита.

Вашите права във връзка с настоящото събиране и обработване на личните Ви данни и личните данни на детето Ви са следните:

- имате право да поискате копие от Вашите лични данни и право на достъп по всяко време до личните си данни; имате право да прехвърлите личните си данни на друг администратор на лични данни, без да бъдете възпрепятствани от наша страна при налична такава законова възможност;

- имате право да поискате да се коригират без ненужно забавяне неточните Ви лични данни, както и данните, които не са вече актуални. За целите на коригиране или допълване на личните Ви данни трябва да подадете отделна декларация, в която да посочите актуални лични данни;

- имате право да поискате от администратора личните Ви данни да бъдат изтрити без ненужно забавяне при наличието на някое от следните основания: личните данни повече не са необходими за целите, за които са били събрани; когато сте оттеглил своето съгласие; когато сте възразил срещу обработването, когато обработването е незаконосъобразно; когато личните данни трябва да бъдат изтрити с цел спазването на правно задължение по правото на ЕС или правото на държава членка, което се прилага спрямо администратора; когато личните данни са били събрани във връзка с предлагането на услуги на информационното общество. Администраторът може да откаже да заличи личните данни по следните причини: упражняване на правото на свобода на изразяването и правото на информация; за спазване на правно задължение от администратора или за изпълнението на задача от обществен интерес, или при упражняването на официални правомощия, които са

предоставени на администратора; по причини от обществен интерес и в областта на общественото здраве; за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, доколкото съществува вероятност заличаването да направи невъзможно или сериозно да затрудни постигането на целите на това обработване; или за установяването, упражняването или защитата на правни претенции.

- имате право да поискате администратора на личните Ви данни, да ограничи обработването на личните Ви данни, като в този случай данните ще бъдат само съхранявани, но не и обработвани. Ако администраторът откаже да ограничи личните Ви данни, той следва да направи това само изрично и в писмен вид, като се мотивира за законосъобразната причина за този отказ.
- имате право да оттеглите Вашето съгласие за обработване на личните Ви данни по всяко време с отделна молба, депозирана пред администратора в случаите, когато обработването се осъществява въз основа на дадено от Вас съгласие; имате право на възражения и жалби във връзка с обработването и съхраняването на личните данни пред Комисия за защита на личните данни, която е надзорен орган в Република България; при нужда Вашите лични данни ще бъдат използвани за нова цел, която не е обхваната от настоящото известие за защита на данните, ще Ви се предостави ново известие за защита на данните, когато и където е необходимо, ще изискаме Вашето предварително съгласие за новото обработване.

Данни за контакт на администратора: …….

Данни за контакт на длъжностното лице по защита на личните данни: ……..

Долуподписаният ..... с подписването потвърждавам, че съм прочел това известие за защита на данните, като съм получил разяснение на зададените от мен въпроси във връзка с личните данни.

Разбирам напълно описаното в настоящото известие и ще се възползвам от предоставените ми права при необходимост.

Декларирам истинността на посочените от мен лични данни. За неверни данни нося наказателна отговорност.

Дата…….. Подпис на родител:……..

Приложение № 6

. . . . . .

Известие за обработване на лични данни
при сключване на трудови договори

Администратор на лични данни: .....
Субект на лични данни:……..……
(име, презиме, фамилия на педагогически специалист/служител)

Относно следните лични данни: име, ЕГН, номер и дата на издаване на лична карта, адрес, семейно положение и деца (в определени случаи: лични данни на съпруг/съпруга и други близки за упражняване на трудови права, напр. при отпуск по майчинство), информация за трудовия стаж и професионалния Ви опит (включително заемани длъжности, работно време, стаж по специалността), информация за банкови сметки, заплата и социални придобивки, месторабота, информация за подбор (включително копия от разрешителни за работа, препоръки и друга информация, посочена във Вашата автобиография и придружително писмо или предоставена по друг начин чрез процеса на кандидатстване, информация относно трудова дисциплина, получени от Вас при сключването на трудовия договор или впоследствие при изпълняването му и на произхождащото от него трудово правоотношение.

В качеството си на администратор лични данни и изпълнявайки задълженията си съгласно Общия регламент за защита на данните декларирам, че ще използвам Вашите лични данни, описани по-горе, за следната цел: сключване, изпълнение и прекратяване на трудовия договор и произхождащото от него трудово правоотношение.

Основание за обработването: сключване на трудовия договор и произхождащото от него трудово правоотношение, както и законовите задължения, предвидени в Кодекса на труда и всички други приложими нормативни актове.

Записи от системи за видеонаблюдение с охранителна цел - опазване на живота и здравето на служителите и учениците, сред които има и деца, в училището, получени от разположените видеокамери.

Ще бъдат обработвани и следните специални категории по-чувствителни данни за Вас:

- Членство в синдикални организации, получени от Вас и от синдикалната организация с цел да се ползвате от правата си при членуване в такава организация.
- Информация за Вашето здравословно състояние, получена от Вас при евентуално представяне от Ваша страна на болничен лист или решение на ТЕЛК, с цел да се изпълнят предвидените в закона права и задължения.
- Информация за наказателни присъди и нарушения, получени от Вас чрез задължително подадена декларация и получена от нас информация от съда, тъй като това е предвидено задължение в закона.

Декларирам, че личните Ви данни ще бъдат третирани като строго поверителни и няма да бъдат споделяни.

Ще съхранявам Вашите лични данни не повече от предвидените в закона срокове, за трудовото правоотношение – трудово досие 5 години след напускане или пенсиониране на служителя, ведомости за заплати – 50 години, болнични листове - 3 години след одит,

видеонаблюдение – 6 месеца, като всички документи, съдържащи лични данни, се съхраняват при необходимите технически и организационни мерки за защита.

Вашите права във връзка с настоящото събиране и обработване на личните Ви данни са следните:

- имате право да поискате копие от Вашите лични данни и право на достъп по всяко време до личните си данни;
- имате право да прехвърлите личните си данни на друг администратор на лични данни, без да бъдете възпрепятствани от наша страна при налична такава законова възможност;
- имате право да поискате да коригирам без ненужно забавяне неточните Ви лични данни, както и данните, които не са вече актуални. За целите на коригиране или допълване на личните Ви данни трябва да подадете отделна декларация, в която да посочите актуални лични данни;
- имате право да поискате от администратора личните Ви данни да бъдат изтрити без ненужно забавяне при наличието на някое от следните основания: личните данни повече не са необходими за целите, за които са били събрани; когато сте оттеглил своето съгласие; когато сте възразил срещу обработването, когато обработването е незаконосъобразно; когато личните данни трябва да бъдат изтрити с цел спазването на правно задължение по правото на ЕС или правото на държава членка, което се прилага спрямо администратора; когато личните данни са били събрани във връзка с предлагането на услуги на информационното общество.
- Администраторът може да откаже да заличи личните данни по следните причини:

1. упражняване на правото на свобода на изразяването и правото на информация;
2. за спазване на правно задължение от администратора или за изпълнението на задача от обществен интерес, или при упражняването на официални правомощия, които са предоставени на администратор;
3. по причини от обществен интерес в областта на общественото здраве;
4. за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, доколкото съществува вероятност заличаването да направи невъзможно или сериозно да затрудни постигането на целите на това обработване; или за установяването, упражняването или защитата на правни претенции.

- имате право да поискате администраторът на личните Ви данни, да ограничи обработването на личните Ви данни, като в този случай данните ще бъдат само съхранявани, но не и обработвани. Ако администраторът откаже да ограничи личните Ви данни, той следва да направи това само изрично и в писмен вид, като се мотивира за законосъобразната причина за този отказ;
- имате право да оттеглите Вашето съгласие за обработване на личните Ви данни по всяко време с отделна молба, депозирана пред администратора в случаите, когато обработването се осъществява въз основа на дадено от Вас съгласие;
- имате право на възражения и жалби във връзка с обработването и съхраняването на личните данни пред Комисията за защита на личните данни, която е надзорен орган в Република България;
- при нужда Вашите лични данни ще бъдат използвани за нова цел, която не е обхванатa от настоящото известие за защита на данните, ще Ви се предостави ново известие за защита на данните, когато и където е необходимо, ще изискаме Вашето предварително съгласие за новото обработване.

Данни за контакт на администратора:

Данни за контакт на длъжностното лице по защита на личните данни: ……..

Долуподписаният.....

(субект на лични данни)

с подписването потвърждавам, че съм прочел това известие за защита на данните, като съм получил разяснение на зададените от мен въпроси във връзка с текста.

Разбирам напълно описаното в настоящия и ще се възползвам от предоставените ми права при необходимост.

Дата…….. Подпис:……..

Приложение № 7

... ...

МОЛБА

До Директора на
……..

Долуподписаният……..…… с ЕГН ……, относно личните ми данни, а именно……., за които съм дал съгласие да обработвате.

Желая да прекратите обработването им и „да бъда забравен“, като за целта ги изтриете.

Дата…… Подпис:……..

Получено от:..... на .....г.

Приложение№ 8

. . . . . .

Възражение

До Директора на
…….,

Долуподписаният……...…… с ЕГН
……

С настоящото възразявам срещу обработването на личните ми данни от . . . . . .
. . . . . поради следната причина:
……
……
……

Дата . . . . . Подпис . . . . . .

Получено от:..... на .....г.