СРЕДНО УЧИЛИЩЕ “ЛЮБЕН КАРАВЕЛОВ”
гр. Димитровград 6400; ул. ”Захари Зограф” № 27; тел.(0391) 6-21-00;
E-mail: info-2602018@edu.mon.bg, **http***://www.lubenkaravelov.eu*

УТВЪРЖДАВАМ:

ДИРЕКТОР:……/П/……
(Валентин Христов)

ВЪТРЕШНИ ПРАВИЛА ЗА СИГУРНОСТ ПРИ АДМИНИСТРИРАНЕ НА ЛИЧНИ ДАННИ В СУ «ЛЮБЕН КАРАВЕЛОВ» ЗА УЧЕБНАТА 2024/2025 ГОДИНА

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) Средно училище „Любен Каравелов“ е юридическо лице със седалище гр. Димитровград, с основен предмет на дейност образование и образователни услуги.

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

Чл. 2. Настоящата инструкция урежда организацията на обработване и защитата на лични данни на преподавателите, служителите, обучаемите (ученици), посетителите, както и на други физически и юридически лица, свързани с осъществяването на нормалната дейност на гимназията.

Чл. 3. (1) Като „обработване на лични данни" се възприема всяко действие или съвкупност от действия, които могат да се извършват по отношение на личните данни с автоматични или други средства, като събиране, записване, организиране, съхраняване, адаптиране или изменение, възстановяване, консултиране, употреба, разкриване чрез предаване, разпространяване, предоставяне, актуализиране или комбиниране, блокиране, заличаване или унищожаване на данните.

(2) Обработването на лични данни се състои и в осигуряване на достъп до определена информация само за лица, чиито служебни задължения или конкретно възложени задачи налагат такъв достъп.

Чл. 4. Училището е администратор на лични данни по смисъла на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) обнародван в Официален вестник на Европейския съюз от 04.05.2016 г. /GDPR/ и спазва принципите за защита на личните данни, предвидени в регламента и законодателството на Европейския съюз и Република България.

Чл. 5. (1) „Лични данни" са всяка информация, отнасяща се до физическо и/или юридическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко чрез идентификационен номер или чрез един или повече специфични признаци.

(2) Принципите за защита на личните данни са:

1. *Законосъобразност, добросъвестност и прозрачност* - обработване при наличие на законово основание, при полагане на дължимата грижа и при информиране на субекта на данни;
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) В съответствие с чл. 11 ал. 3 от Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, оценката на въздействието се извършва периодично на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица (Приложение № 1).

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) Средно училище „Любен Каравелов“ 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 гимназията 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. В съответствие с Глава четвърта "а" от ЗЗЛД, физическите лица, чиито лични данни се обработват, подписват декларация за съгласие по образец.

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, които обработват лични данни попълват декларация и 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 рафтове, 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 на лични данни с

оглед запазване на информацията за съответните лица в актуален вид и възможността й 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 лични данни и оторизираните длъжностни лица.

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

Чл. 12. С оглед защита на хартиените, техническите и информационните ресурси всички служители са длъжни да спазват правилата за противопожарна безопасност.

Чл. 13. (1) При регистриране на неправомерен достъп до информационните масиви за лични 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.

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

Чл. 14. (1) При повишаване на нивото на чувствителност на информацията, произтичащо от изменение в нейния вид или в рисковете при обработван ето й, гимназията 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 гимназията регистри, следва да бъдат унищожени или прехвърлени на друг администратор на лични данни съобразно изискванията на Закона за защита на личните данни.

В случаите, когато се налага унищожаване на носител на лични данни, гимназията 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, включително презаписването на електронните средства или физическо унищожаване на носителите. Документите на хартиен носител, съдържащи данни, се унищожават чрез нарязване.

(2) Унищожаване се осъществява от служителя, отговорен за архива на училището.

Чл. 16. (1) Достъп на лица до лични данни се предоставя единствено, ако те имат право на такъв достъп, съгласно действащото законодателство, след подаване на заявление, респективно искане за достъп на информация, и след тяхното легитимиране.

(2) Решението си за предоставяне или отказване достъп до лични данни за съответното лице, гимназията съобщава в 30-дневен от подаване на заявлението, респективно искането.

(3) При необходимост този срок може да бъде удължен с още два месеца, като се взема предвид сложността и броя на исканията. Администраторът информира субекта на данните за всяко такова удължаване в срок от един месец от получаване на искането, като посочва и причините за забавянето. Когато субектът на данни подава искане с електронни средства, по възможност информацията се предоставя с електронни средства, освен ако субектът на данни не е поискал друго.

(4) Информацията може да бъде предоставена под формата на:

1. устна справка;
2. писмена справка;
3. преглед на данните от самото лице;
4. предоставяне на исканата информация на технически и/или електронен носител.

(6) Изключение се допуска единствено за тези органи и/или институции, които извършват това въз основа на изискване на закона (напр. МОН, МВР, съд, прокуратура, НАП, НОИ и др.).

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 помещенията, 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.

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 гимназията включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства.

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. споделяне на критична информация между персонала (например идентификатори, пароли за достъп и т.н.);
5. съгласие за поемане на задължение за неразпространение на личните данни;

(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".

(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.

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. Контрол на достъпа до регистрите: осъществява се от директор и ЗДУД;
5. 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;
6. Правила за размножаване и разпространяване: само в случаите, когато според нормативната уредба е необходимо;
7. 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 гимназията, се унищожават по подходящ и сигурен начин (напр. изгаряне, нарязване, електронно изтриване и други подходящи за целта методи);
8. Процедури за проверка и контрол на обработването.

Чл. 20. (1) Защитата на автоматизираните електронни системи и/или мрежи 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 компютърен кабинет.
4. Политиката по създаване и поддържане на резервни копия за възстановяване регламентира - Основната цел на архивирането е свързана с предотвратяване на загуба на информация, свързана с лични данни, която би затруднила нормалното функциониране на гимназията.
5. Основни електронни носители на информация са: вътрешни твърди дискове, еднократно и/или многократно презаписваеми външни носители (външни твърди дискове, многократно презаписваеми карти, флаш памети 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. Данните, които вече не са необходими за целите на училището и чийто срок за съхранение е изтекъл, се унищожават чрез приложими способ (напр. чрез нарязване, изгаряне или постоянно заличаване от електронните средства).

III. БАЗИСНИ ПРАВИЛА И МЕРКИ ЗА ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ПРИ КОМПЮТЪРНА ОБРАБОТКА

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.

(5) С цел повишаване сигурността на достъпа до информация служителите задължително променят използваните от тях пароли на определен период, като тези пароли се записват на хартиен носител и се съхраняват в касата на директора. В случай на отпадане на основанието за достъп до лични данни правата на съответните лица се преустановяват (вкл. и чрез изтриване на акаунта).

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

(2) При необходимост от ремонт на компютърната техника, предоставянето й на сервизната организация се извършва 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 от ръководителя лице.

(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.

Чл. 24. Служителите, на които е възложено да подписват служебна кореспонденция с универсален електронен подпис (УЕП), нямат право да предоставят издадения им УЕП на трети лица.

IV. ПОДДЪРЖАНИ РЕГИСТРИ И ТЯХНОТО УПРАВЛЕНИЕ

Чл. 25. Поддържаните от Средно училище „Любен Каравелов“ регистри с лични данни са:

1. Ученици
2. Човешки ресурси
3. Родители
4. Пропускателен режим
5. Видеонаблюдение
6. Контрагенти
7. Искания по ЗДОИ
8. Жалби, сигнали, други искания и уведомления за нарушения за сигурността на данните
9. Вътрешен регистър на нарушенията на Регламент (ЕС) 2016/679 и ЗЗЛД

Чл. 26. (1) В регистър „Ученици" се набират и съхраняват лични данни с цел индивидуализиране на физически лица „ученици", обучавани в училището.

(2) Общо описание на регистър „Ученици"

Регистърът съдържа следните категории лични данни:

1. физическата идентичност на лицето: име, ЕГН, адрес, месторождение, телефони за връзка, банкови сметки при необходимост;

2. културна идентичност: интереси и хоби;
3. социална идентичност - образование;
4. семейна идентичност - родствени връзки;
5. лични данни, които се отнасят до здравето.

(3) Технологично описание на регистър „ученици":

Носители на данни:

- На хартиен носител: Данните се набират в писмена (документална) форма и се съхраняват в папки. Папките се подреждат в шкафове, които са разположени в изолирани заключващи се помещения, снабдени със защитна сигнализация. Информацията от хартиените носители за всеки ученик, се записва в Книга за подлежащите на задължително обучение деца до 16-годишна възраст; Регистрационни книги; Личен картон за дневна и самостоятелна форма на обучение в училището със задължителни реквизити съгласно Наредба № 8 от 11.08.2016 г. за информацията и документите за системата на предучилищното и училищното образование, които се съхраняват в същите изолирани помещения и Лични здравно-профилактични карти на учениците, които се съхраняват в заключени шкафове в лекарския кабинет на училището.

- На технически носител: Личните данни се въвеждат в Национална електронна информационна система за предучилищното и училищното образование след регистрация на директора, който определя правата на достът на служителите.

Чрез сключени договори за работа с Модул „Списък-образец“ на платформа АдминПлюс, интегрирана с НЕИСПУО училището изготвя Списък-образец №1, а с платформа “Школо”, също интегрирана с НЕИСПУО, ще се въвеждат данни в електронния дневник на училището.

Модулите отговаря на всички нормативни изисквания и са напълно интегрирани с НЕИСПУО.

- срок на съхранение: съгласно НАРЕДБА № 8 от 11.08.2016 г. за информацията и документите в системата на предучилищното и училищното образование, Приложение 2.

(4) Определяне на длъжностите:

Обработващи лични данни на регистър „Ученици" са: директор, заместник-директори, завеждащ административна служба, педагогически специалисти, главен счетоводител, технически секретар, медицинско лице.

Длъжностните лица - обработващи лични данни предприемат всички организационно- технически мерки за съхраняването и опазването на личните данни.

(5)Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

1. поверителност - ниско ниво;
2. цялостност - ниско ниво;
3. наличност - ниско ниво;
4. общо за регистъра - ниско ниво

(6) Организационни мерки за физическа защита - определени са помещенията, в които ще се обработват лични данни и са разположени комуникационно-информационните системи за обработване на лични данни, като физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения (на база заключващи системи). Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения. 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.

Техническите мерки за физическа защита включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства.

Защитата на електронните данни от неправомерен достъп се осъществява посредством поддържане на антивирусни програми, периодично архивиране на външен носител, както и чрез поддържане на информацията и на хартиен носител.

(7) Средно училище „Любен Каравелов“, предприема превантивни действия при защита на личните данни като съставя план за действие при различните случаи на настъпили форсмажорни събития, а именно:

1. защита при аварии, независещи от Средно училище „Любен Каравелов“ - предприемат се конкретни действия в зависимост от конкретната ситуация;
2. защита от пожари - незабавно гасене със собствени средства /пожарогасители/ и уведомяване на съответните органи;
3. защита от наводнения - предприемат действия по ограничаване на разпространението, както и се изпомпва вода или загребва със собствени подръчни средства.

(8) Достъп до регистър „Ученици" имат и държавните органи - МОН, РУО, дирекция „Социално подпомагане" във връзка с изпълнение на техните задължения, предвидени в съответните законови и подзаконови нормативни актове.

Достъп до обработваните лични данни имат и съответните държавни органи - съд, следствие, прокуратура, ревизиращи органи и други, когато са изискали данните по надлежен ред във връзка с изпълнението на техните правомощия.

(9) Лични данни на учениците се съхраняват до осъществяване на целите, за които се обработват, но не по-късно от периода, предвиден съгласно Номенклатурата на делата със сроковете за тяхното съхранение в Средно училище „Любен Каравелов“

(10) Изготвянето и публикуването на снимков материал за учениците при и по повод изпълнението им на ученическите задължения става само след подписване на декларация от ученика и/или негов родител/настойник.

(11) След постигане целите по предходната алинея личните данни на учениците се унищожават физически, чрез изгаряне за което се изготвят актови протоколи за унищожаване.

Чл. 27. (1) В регистър „Човешки ресурси" се набират и съхраняват лични данни с цел индивидуализиране на физически лица, назначени по трудово правоотношение и/или и по граждански договори.

(2) Общо описание на регистър „Човешки ресурси"

Регистърът съдържа следните групи данни:

1. физическата идентичност - име, ЕГН, адрес, данни по лична карта, месторождение, телефони за връзка и банкови сметки;
2. психологическа идентичност - документи относно психическото здраве;
3. социална идентичност - образование и трудова дейност;
4. семейна идентичност - семейно положение и родствени връзки;
5. лични данни, които се отнасят до здравето;
6. други - лични данни относно гражданско-правния статус на лицата.

Нормативното основание е Кодексът на труда, Кодексът за социалното осигуряване, Законът за счетоводството, Законът за данъците върху доходите на физическите лица и приложимото законодателство в областта на трудовото право.

Предназначението на събираните данни в регистъра е свързано с:

1. Индивидуализиране на трудовите правоотношения;
2. Изпълнение на нормативните изисквания на свързаното с регистъра приложимо действащо законодателство;
3. Дейностите, свързани със сключване, съществуване, изменение и прекратяване на трудовите правоотношения, изготвяне на договори, допълнителни споразумения, заповеди, документи, удостоверяващи трудовия стаж, доходите от трудови правоотношения и по граждански договори, служебни бележки, справки, удостоверения и др.
4. Установяване на връзка с лицето по телефон, изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудово правоотношение и по граждански договори.

(3) Технологично описание на регистър „Персонал":

Носители на данни:

- На хартиен носител: Данните се набират в писмена (документална) форма и се съхраняват в папки (трудови досиета). Папките се подреждат в шкафове, които са разположени в изолирани заключващи се помещения, снабдени със защитна сигнализация.

- На технически носител: Личните данни се въвеждат в специализиран програмен продукт от счетоводство, касиер-домакин и ЗАС. Базата данни се намира на твърдия диск на изолирани компютри.

- Срок на съхранение: съгласно Закона за счетоводството: ведомости за заплати – 50 години, считано от 1 януари на отчетния период, следващ отчетния период, за който се отнасят;

(4) Определяне на длъжностите:

Обработващи лични данни на регистър „Персонал" са: Директор, заместник-директор, ЗАС, гл.счетоводител, касиер-домакин, технически секретар.

(5) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

4. поверителност - ниско ниво;
5. цялостност - ниско ниво;
6. наличност - ниско ниво;
7. общо за регистъра - ниско ниво.

(6) Организационни мерки за физическа защита - определени са помещенията, в които ще се обработват лични данни и са разположени комуникационно-информационните системи за обработване на лични данни, като физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения (на база заключващи системи). Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения. 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.

Техническите мерки за физическа защита включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства.

Трудовите досиета на персонала не се изнасят извън сградата на училището.

Защитата на електронните данни от неправомерен достъп се осъществява посредством поддържане на антивирусни програми, периодично архивиране на външен носител, както и чрез поддържане на информацията и на хартиен носител.

При изготвяне на ведомости за заплати или щатно разписание на персонала личните данни се въвеждат на твърд диск, на изолиран компютър или на компютър, който е свързан в локална мрежа, но със защитен достъп до личните данни, като използваните софтуерни продукти са адаптирани към специфичните нужди на училището.

При внедряване на нов програмен продукт за обработване на лични данни се 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.

(7) Средно училище „Любен Каравелов“ предприема превантивни действия при защита на личните данни като съставя план за действие при различните случаи на настъпили форсмажорни събития, а именно:

1. защита при аварии, независещи от Средно училище „Любен Каравелов“- предприемат се конкретни действия в зависимост от конкретната ситуация;
2. защита от пожари - незабавно гасене със собствени средства /пожарогасители/ и уведомяване на съответните органи;
3. защита от наводнения - предприемат действия по ограничаване на разпространението, както и се изпомпва вода или загребва със собствени подръчни средства.

(8) Достъп до регистър „Човешки ресурси" имат и държавните органи - НАП, НОИ, МОН, РУО за изпълнение на техните задължения, предвидени в съответните законови и подзаконови нормативни актове.

Достъп до обработваните лични данни имат и съответните държавни органи - съд, следствие, прокуратура, ревизиращи органи и други, когато са изискали данните по надлежен ред във връзка с изпълнението на техните правомощия.

(9) Лични данни се съхраняват до осъществяване на целите, за които се обработват, но не по-късно от периода, предвиден съгласно Номенклатурата на делата със сроковете за тяхното съхранение в Средно училище „Любен Каравелов“.

(10) След постигане целите по предходната алинея личните данни се унищожават физически, чрез изгаряне за което се изготвят актови протоколи за унищожаване.

Чл. 28. (1) В регистър „Родители" се набират и съхраняват лични данни с цел индивидуализиране на физически лица, родители, настойници и други категории, свързани с тях лица.

(2) Общо описание на регистър „Родители"

Регистърът съдържа следните групи данни:

1. физическата идентичност - име, адрес, телефони за връзка и месторабота;
2. социална идентичност - образование, трудова дейност;
3. семейна идентичност - семейно положение и родствени връзки.

Нормативното основание е ЗНП и ЗПУО и приложимото законодателство, свързано с предоставянето на образователни услуги.

(3) Технологично описание на регистър „Родители":

Носители на данни:

- На хартиен носител: Данните се набират в писмена (документална) форма и се съхраняват в папки. Папките се подреждат в шкафове, които са разположени в изолирани заключващи се помещения, снабдени със защитна сигнализация.

- На технически носител: Личните данни се въвеждат в НЕИСПУО.

- Срок на съхранение: съгласно НАРЕДБА № 8 от 11.08.2016 г. за информацията и документите в системата на предучилищното и училищното образование, Приложение 2 и до края на съответната учебна година за Декларациите за стипендии и приложените към тях документи. Анкетните карти се съхраняват до момента, в който ученикът напусне гимназията (завърши средно образование или се премести да учи в друго училище);

(4) Определяне на длъжностите:

Обработващи лични данни на регистър „Родители" са: директор, заместник-директори, педагогически специалисти, главен счетоводител, ЗАС, технически секретар, медицинско лице.

Длъжностните лица, обработващи лични данни, предприемат всички организационно-технически мерки за съхраняването и опазването на личните данни.

(5) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

1. поверителност - ниско ниво;
2. цялостност - ниско ниво;
3. наличност - ниско ниво;
4. общо за регистъра - ниско ниво.

(5) Организационни мерки за физическа защита - определени са помещенията, в които ще се обработват лични данни и са разположени комуникационно-информационните системи за обработване на лични данни, като физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения (на база заключващи системи). Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения. 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.

Техническите мерки за физическа защита включват използване на ключалки, шкафове, метални каси, както и оборудване на помещенията с пожарогасителни средства.

Защитата на електронните данни от неправомерен достъп се осъществява посредством поддържане на антивирусни програми, периодично архивиране на външен носител, както и чрез поддържане на информацията и на хартиен носител.

(6) Средно училище „Любен Каравелов“ предприема превантивни действия при защита на личните данни като съставя план за действие при различните случаи на настъпили форсмажорни събития, а именно:

1. защита при аварии, независещи от Средно училище „Любен Каравелов“ предприемат се конкретни действия в зависимост от конкретната ситуация;
2. защита от пожари - незабавно гасене със собствени средства (пожарогасители) и уведомяване на съответните органи;
3. защита от наводнения - предприемат действия по ограничаване на разпространението, както и се изпомпва вода или загребва със собствени подръчни средства.

(7) Достъп до регистър „Родители" имат и държавните органи - МОН, РУО, дирекция „Социално подпомагане" за изпълнение на техните задължения, предвидени в съответните законови и подзаконови нормативни актове.

Достъп до обработваните лични данни имат и съответните държавни органи - съд, следствие, прокуратура, ревизиращи органи и други, когато са изискали данните по надлежен ред във връзка с изпълнението на техните правомощия.

(8) Лични данни се съхраняват до осъществяване на целите, за които се обработват, но не по-късно от периода, предвиден съгласно Номенклатурата на делата със сроковете за тяхното съхранение в Средно училище „Любен Каравелов“

(9) След постигане целите по предходната алинея личните данни се унищожават физически, чрез нарязване за което се изготвят актови протоколи за унищожаване.

Чл. 29. (1) В регистър „Пропускателен режим" се набират и съхраняват лични данни с цел индивидуализиране на физически лица, съгласно Закона за частната охранителна дейност. Категориите физически лица, за които се обработват лични данни, са посетителите в сградата на училището.

(2) Общо описание на регистър „Пропускателен режим"

Регистърът съдържа следните групи данни - физическата идентичност: име по лична карта.

(3) Технологично описание на регистър „Пропускателен режим": Данните се набират в писмена форма в дневник.

(4) Определяне на длъжностите:

Обработващ лични данни на регистър „Пропускателен режим" е портиерът.

(5) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

1. поверителност - ниско ниво;
2. цялостност - ниско ниво;
3. наличност - ниско ниво;
4. общо за регистъра - ниско ниво.

(6) Организационни мерки за физическа защита - определено е помещение, в което се съхраняват личните данни, като физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения.

(7) Действия за защита при аварии, произшествия и бедствия: длъжностното лице изнася дневника при евакуация.

(8) Достъп до регистър „Пропускателен режим": Категориите лица, на които личните данни могат да бъдат разкривани са физическите лица, за които се отнасят данните, и на лица, ако е предвидено в нормативен акт.

(9) Лични данни се съхраняват до осъществяване на целите, за които се обработват (до приключване на дневника).

(10) След приключване на дневника, същият се унищожава физически, чрез изгаряне.

(11) Източниците, от които се събират данните, са: от физическите лица.

(12) Данните в регистъра се предоставят доброволно от лицата при влизането им в сградата на училището.

(13) На входовете на сградата се поставят информационни табла за уведомяване на гражданите за пропускателния режим в сградата и проверка съгласно чл. 24, ал. 1 от Закона за частната охранителна дейност (ЗЧОД), както и за използването на технически средства за наблюдение и контрол, съгласно чл. 24, ал. 2 от ЗЧОД.

Чл. 30. (1) В регистър „Видеонаблюдение" се набират и съхраняват лични данни с цел индивидуализиране на физически лица, съгласно Закона за частната охранителна дейност.

(3) Общо описание на регистър „Видеонаблюдение":

Категориите физически лица, за които се обработват лични данни, са посетители, ученици, преподаватели и служители в сградите на училището.

Регистърът съдържа следните групи данни - физическата идентичност на лицето - видеообраз.

(4) Технологично описание на регистър „Видеонаблюдение": Регистърът се попълва с данни от автоматично денонощно видеонаблюдение (видеообраз) за движението на учениците, служителите и посетителите в сградата на училището.

(5) Определяне на длъжностите:

Обработващи личните данни на регистър „Видеонаблюдение" са директор, заместник-директори, учители ИКТ.

(6) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

1. поверителност - ниско ниво;
2. цялостност - ниско ниво;
3. наличност - ниско ниво;
4. общо за регистъра - ниско ниво.

(6) Организационни мерки за физическа защита - определени са помещенията, в които ще се обработват лични данни, като физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения.

(7) Категориите лица, на които личните данни могат да бъдат разкривани са физическите лица, за които се отнасят данните, и на лица, ако е предвидено в нормативен акт.

(8) Лични данни се съхраняват в паметта на дивиара за срок от 15 до 30 дни. При необходимост записите могат да бъдат свалени на външен носител.

(9) След постигане целите по предходната алинея личните данни се унищожават физически, чрез изтриване.

(10) Данните в регистъра се предоставят доброволно от лицата при подхода и влизането им в сградата на училището.

Чл. 31. (1) В регистър „Контрагенти" се набират и съхраняват лични данни на физически лица за изпълнение на договорите, които сключва по реда на ЗЗД, ЗОП, ТЗ и други нормативни актове.

Регистърът съдържа следните групи данни - физическата идентичност на лицето - име, ЕГН, адрес, данни по лична карта, месторождение, телефони за връзка и банкови сметки;

(2)Технологично описание на регистър „Контрагенти": Регистърът се попълва с данни от лицата със сключени договори.

(3)Определяне на длъжностите:

Обработващи личните данни на регистър „Контрагенти" са директор, заместник-директори, ЗАС, главен счетоводител, касиер домакин, технически секретар.

(4)Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

1. поверителност - ниско ниво;

2. цялостност - ниско ниво;

3. наличност - ниско ниво;

4. общо за регистъра - ниско ниво.

(5) Организационни мерки за физическа защита - определени са помещенията, в които ще се обработват лични данни, като физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения.

(6) Категориите лица, на които личните данни могат да бъдат разкривани са физическите лица, за които се отнасят данните, и на лица, ако е предвидено в нормативен акт.

Чл. 32. (1) В регистър „Искания по ЗДОИ" се набират и съхраняват лични данни на физически лица искащи информация по реда на ЗДОИ

Регистърът съдържа следните групи данни - физическата идентичност на лицето - име, ЕГН, адрес, данни по лична карта, месторождение, телефони за връзка;

(2) Технологично описание на регистър „Искания по ЗДОИ": Регистърът се попълва с данни от лицата подали заявления.

(3) Определяне на длъжностите:

Обработващи личните данни на регистър „Искания по ЗДОИ" са директор, заместник-директори, ЗАС, главен счетоводител, касиер домакин.

(4)Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

1. поверителност - ниско ниво;

2. цялостност - ниско ниво;

3. наличност - ниско ниво;

4. общо за регистъра - ниско ниво.

(5) Организационни мерки за физическа защита - определени са помещенията, в които ще се обработват лични данни, като физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения.

(6) Категориите лица, на които личните данни могат да бъдат разкривани са физическите лица, за които се отнасят данните, и на лица, ако е предвидено в нормативен акт.

Чл. 33. (1) В регистър „Жалби, сигнали и други искания и уведомления за нарушения за сигурността на данните" се набират и съхраняват лични данни на физически лица искащи информация по реда на ЗДОИ

Регистърът съдържа следните групи данни - физическата идентичност на лицето - име, ЕГН, адрес, данни по лична карта, месторождение, телефони за връзка.

(2)Технологично описание на регистър „Жалби, сигнали и други искания и уведомления за нарушения за сигурността на данните": Регистърът се попълва с данни от лицата подали жалби, сигнали и други искания.

(3)Определяне на длъжностите:

Обработващи личните данни на регистър „Жалби, сигнали и други искания и уведомления за нарушения за сигурността на данните" са директор, заместник-директори, ЗАС, главен счетоводител, касиер домакин, технически секретар.

(4) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

1. поверителност - ниско ниво;

2. цялостност - ниско ниво;

3. наличност - ниско ниво;

4. общо за регистъра - ниско ниво.

(5) Организационни мерки за физическа защита - определени са помещенията, в които ще се обработват лични данни, като физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения.

(6) Категориите лица, на които личните данни могат да бъдат разкривани са физическите лица, за които се отнасят данните, и на лица, ако е предвидено в нормативен акт.

Чл. 34. (1) В регистър „Вътрешен регистър на нарушения на Регламент (ЕС) 2016/679 и ЗЗЛД" се набират и съхраняват лични данни на физически лица и при извършване на нарушения на сигурнастта на информацията. Регистърът съдържа данни които са били установени при нарушението;

(2)Технологично описание на регистър „Жалби, сигнали и други искания и уведомления за нарушения за сигурността на данните": Регистърът се попълва с данни от лицата подали жалби, сигнали и други искания.

(3)Определяне на длъжностите:

Обработващи личните данни на регистър „Жалби, сигнали и други искания и уведомления за нарушения за сигурността на данните" са директор, заместник-директори, завеждащ административна служба, главен счетоводител, касиер домакин, технически секретар.

(4)Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

- поверителност - ниско ниво;
- цялостност - ниско ниво;
- наличност - ниско ниво;
- общо за регистъра – ниско ниво.

(5) Организационни мерки за физическа защита - определени са помещенията, в които ще се обработват лични данни, като физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения.

(6) Категориите лица, на които личните данни могат да бъдат разкривани са физическите лица, за които се отнасят данните, и на лица, ако е предвидено в нормативен акт.

V. ПРАВА И ЗАДЪЛЖЕНИЯ НА ЛИЦАТА, ОБРАБОТВАЩИ ЛИЧНИ ДАННИ

Чл. 35. Лицата, обработващи лични данни в Средно училище „Любен Каравелов“: директор, заместник-директори, всички педагогически специалисти, главен счетоводител, касиер-домакин, завеждащ административна служба, технически секретар, медицинско лице, портиер.

Чл. 36.(1) Служителите на училището са длъжни:

- да обработват лични данни законосъобразно и добросъвестно;
- 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;
- да актуализират регистрите на личните данни (при необходимост);
- да заличават или коригират личните данни, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;
- 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.
- да не разгласяват лични данни, до които са получили достъп при и по повод изпълнение на задълженията си.

Чл. 37. (1) За неспазването на разпоредбите на настоящата инструкция служителите носят административна отговорност.

(2) 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.

VI.МЕРКИ ЗА ЗАЩИТА НА АВТОМАТИЗИРАНИ ИНФОРМАЦИОННИ СИСТЕМИ И КРИПТОГРАФСКА ЗАЩИТА

Чл. 38. (1) Достъп до операционната система, съдържаща файлове с лични данни, имат само лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп. Достъпът се осъществява чрез парола.

(2) Електронните бази данни са защитени посредством логически средства за защита, като антивирусна програма, която се обновява автоматично, защитни стени (firewalls) и др.

(3) Архивиране на личните данни на технически носител се извършва периодично с оглед съхранение на информацията.

Чл. 39. (1) Защитата на електронните данни от неправомерен достъп, повреждане, изгубване или унищожаване, извършени умишлено от лице или в случай на технически неизправности, аварии, произшествия, бедствия и др., се осигурява посредством:

- въвеждане на пароли за компютрите, чрез които се предоставя достъп до личните данни, и файловете, които съдържат лични данни;
- антивирусни програми, проверки за нелегално инсталиран софтуер;
- периодични проверки на целостта на базата данни и актуализиране на системната информация, поддържане на системата за достъп до данните;
- периодично архивиране на данните на технически носители, поддържане на информацията на хартиен носител (архивни копия).

(2) Лицето, отговорно за личните данни, докладва периодично на ръководството на дружеството предприетите мерки за гарантиране нивото на сигурност при обработване на лични данни.

VII.ПРАВО НА ДОСТЪП, КОРЕКЦИЯ, ИЗТРИВАНЕ И ОГРАНИЧАВАНЕ ИЗПОЛЗВАНЕТО НА ЛИЧНИТЕ ДАННИ

Чл.40 Права на достъп във връзка с личните данни:

1. Достъп до информация: това право Ви дава възможност да получите копие на личните данни, които съхраняваме за Вас, и да проверите дали имаме законово основание за тяхната обработка.
2. Коригиране: това право Ви дава възможност да изискате от нас да коригираме всяка непълна или неточна информация за Вас.
3. Изтриване: това право Ви дава възможност да изискате от нас да изтрием или премахнем Ваши лични данни, когато нямаме валидна причина да продължим обработката им. Също така имате правото да изискате данните Ви да се изтрият или премахнат, когато сте упражнили правото си да възразите срещу тяхната обработка.
4. Възражение срещу обработка: в случаите, които ние разчитаме на легитимните си интереси като основание за обработка, Вие можете да възразите срещу тази обработка.
5. Ограничаване на обработката: това право Ви дава възможност да изискате от нас временно да преустановим обработването на Вашите лични данни, ако например желаете да установим точността на данните или причините за тяхното обработване.
6. Преносимост на данните: това право е ограничено до случаите, когато данните са ни предоставени от Вас за целите на договор и Ви дава възможност да изискате от нас да предоставим съхраняваните в електронна форма Ваши данни на трето лице.
7. Право да оттеглите съгласието си

Чл. 41. Субектът на данни има правото да поиска чрез писмено заявление от администратора администратора да предприе действия по предходният член.

Чл. 42 . Когато администраторът е направил личните данни обществено достояние и е задължен да изтрие личните данни, той, като отчита наличната технология и разходите по изпълнението, предприема разумни стъпки, включително технически мерки, за да уведоми администраторите, обработващи личните данни, че субектът на данните е

поискал изтриване от тези администратори на всички връзки, копия или реплики на тези лични данни.

Чл. 43. Изтриването на личните данни се прилага, доколкото обработването е необходимо:

а) за упражняване на правото на свобода на изразяването и правото на информация;

б) за спазване на правно задължение, което изисква обработване, предвидено в правото на Съюза или правото на държавата членка, което се прилага спрямо администратора или за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора;

в) по причини от обществен интерес в областта на общественото здраве в съответствие с член 9, параграф 2, букви з) и и), както и член 9, параграф 3 от РЕГЛАМЕНТ (ЕС) 2016/679 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА;

г) за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели съгласно член 89, параграф 1, доколкото съществува вероятност правото, установено в параграф 1, да направи невъзможно или сериозно да затрудни постигането на целите на това обработване; или

д) за установяването, упражняването или защитата на правни претенции.

Преходни и заключителни разпоредби:

§ 1. По смисъла на настоящата инструкция:

• „Лични данни“ са всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко чрез идентификационен номер или чрез един или повече специфични признаци.

• Администратор“ е физическо или юридическо лице, както и орган на държавната власт или на местното самоуправление, който сам или съвместно с друг определя целите и средствата за обработване на личните данни.

• „Администратор на лични данни" е Природо-математическа гимназия „Иван Вазов“- Димитровград (гимназията).

• „Ниво на защита" е степен на организация на обработката на личните данни в зависимост от рисковете и вида им.

• „Обработване на лични данни" е всяко действие или съвкупност от действия, които могат да се извършват по отношение на личните данни с автоматични или други средства, като събиране, записване, организиране, съхраняване, адаптиране или изменение, възстановяване, консултиране, употреба, разкриване чрез предаване, разпространяване, предоставяне, актуализиране или комбиниране, блокиране, заличаване или унищожаване.

• „Обработващ лични данни" е лице, което обработва лични данни от името на администратора на лични данни.

• „Оценка на въздействие" е процес за определяне нивата на въздействие върху конкретно физическо лице или група физически лица, в зависимост от характера на обработваните лични данни и броя на засегнатите физически лица при нарушаване на поверителността, цялостността или наличността на личните данни.

• „Поверителност е изискване за неразкриване на личните данни на неоторизирани лица в процеса на тяхното обработване.

• „Предоставяне на лични данни" са действия по цялостно или частично пренасяне на лични данни от един администратор към друг или към трето лице на територията на страната или извън нея.

• „Регистър на лични данни" е всяка структурирана съвкупност от лични данни, достъпна по определени критерии, централизирана, децентрализирана или разпределена на функционален или географски принцип.

• „Съгласие на физическото лице" е всяко свободно изразено, конкретно и информирано волеизявление, с което физическото лице, за което се отнасят личните данни, недвусмислено се съгласява, те да бъдат обработвани.

• „Трето лице" е физическо или юридическо лице, орган на държавна власт или на

местно самоуправление, различен от физическото лице, за което се отнасят данните, от администратора на лични данни, от обработващия лични данни и от лицата, които под прякото ръководство на администратора или обработващия имат право да обработват лични данни.

§2. Всички служители на училището са длъжни срещу подпис да се запознаят с правилата и да ги спадват.

§3. Правилата се издават на основание чл. 23, ал. 4 от Закона за защита на личните данни, както и на Регламент (ЕС) 2016/679 на Европейския съюз.

§4. За всички неуредени в настоящите правила въпроси са приложими разпоредбите на Закона за защита на личните данни и действащото приложимо законодателство на Р България.

§5. Настоящите Вътрешни правила са утвърдени със Заповед №РД 13-856 от 14.09.2024 г.

ПРИЛОЖЕНИЕ № 1

Оценка на нивото на въздействие на регистър

Име на регистъра	НИВО НА ВЪЗДЕЙСТВИЕ			
	поверителност	цялостност	наличност	общо за регистъра

ПРИЛОЖЕНИЕ №2

ДЕКЛАРАЦИЯ

Долуподписаният/ата ……...

ЕГН: ……., Лична карта № ……..……..……..,

издадена от ……..…….. на ……..… г.

ДЕКЛАРИРАМ:

Съгласен/а съм Средно училище „Любен Каравелов“ гр. Димитровград, да обработва личните ми данни, съгласно изискванията на 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 на достъп и на коригиране на събраните данни;
- получателите или категориите получатели, на които могат да бъдат разкрити данните.

Дата: **ДЕКЛАРАТОР: ……**

гр. Димитровград

ПРИЛОЖЕНИЕ № 3

ДО ДИРЕКТОРА НА
СРЕДНО УЧИЛИЩЕ „ЛЮБЕН КАРАВЕЛОВ“
ДИМИТРОВГРАД

ЗАЯВЛЕНИЕ

за предоставяне на лични данни

От ……...
(име, презиме, фамилия)

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

Упълномощено лице:…….....
(име, презиме, фамилия)

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

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

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

Уважаема .....,

Във връзка с .....
(посочват се обстоятелствата, във връзка с които се иска информацията)

и на основание чл. 29, ал.1 от Закона за защита на личните данни (ЗЗЛД) с настоящото заявление се обръщам към Вас с оглед получаване на лични данни относно:

1. .....

2. .....

Предпочитам формата на предоставената информация да бъде във вид на ……
(на дискета , CD , копие ,факс , електронна поща и др.)

Адрес за кореспонденция :

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

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

Дата: ..... С уважение: ….....