IVСменно-вечерна гимназия „Отец Паисий“

Утвърждава:

Директор:

Райна Игнатова

Утвърдени със заповед на директора № 411/11.09. 2020 г.

Протокол№13/02.09.2020 г. на ПС

ВЪТРЕШНИ ПРАВИЛА

за учебната 2020/ 2021 година

на IVСменно-вечерна гимназия „Отец Паисий“
за мерките за защита на личните данни съгласно Регламент 2016/679

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) **IVСменно-вечерна гимназия „Отец Паисий“**, наричана по-долу само **IV СВГ**, е юридическо лице, което се състои от всички служители на гимназията и е регистрирана по Закона за регистър БУЛСТАТ с БУЛСТАТ: **000669468**.

(2) **IV СВГ**е със седалище в гр. София и адрес: гр. София, ул. „Дунав“ № 30.

(3) Като юридическо лице, възникнало по силата на закона, **IV СВГ** осъществява чрез своите служители дейностите, предвидени в Закона за училищно и предучилищно образование и други нормативни актове на МОН.

(4) **IV СВГ** обработва лични данни във връзка със своята дейност и самаопределя целите и средствата за обработването им. В този случай **IV СВГ**действа като администратор на лични данни.

(5) В случаите, в които **IV СВГ** обработва лични данни за цели, определени самостоятелно от трето лице или целите са определени съвместно от **IV СВГ** и трето лице, **IV СВГ** има положението или на обработващ лични данни (ако целите са определени от лицето, което е възложило обработването) или на съадминистратор.

Чл. 2.Настоящите Вътрешни правила на **IV СВГ** уреждат организацията на обработване и защитата на лични данни на служителите и учениците в гимназията, както и на всички други групи физически лица, с които **IV СВГ** влиза в отношения при осъществяването на правомощията и дейността си.

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

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

(3) „Регистър с лични данни“ представлява всеки структуриран набор от лични данни, независимо от неговия вид и носител, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип.

Чл. 4.(1) **IV СВГ** е администратор на лични данни по смисъла на чл. 4, т. 7 от Общия регламент относно защитата на данните (ЕС) 2016/679.

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

Чл. 5. (1) 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.

(2) Ако конкретната цел или цели, за които се обработват лични данни от **IV СВГ**, не изискват или вече не изискват идентифициране на субекта на данните, **IV СВГ** не е задължена да поддържа, да се сдобие или да обработи допълнителна информация, за да идентифицира субекта на данните, с единствена цел да докаже изпълнението на изискванията на Регламент 2016/679.

Чл. 6. IV СВГ организира и предприема мерки за защита на личните данни от случайно или незаконно унищожаване, от неправомерен достъп, от изменение или разпространение както и от други незаконни форми на обработване на лични данни. Предприеманите мерки са съобразени със съвременните технологични достижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

Чл. 7. IV СВГ прилага адекватна защита на личните данни, която включва:

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

Чл. 8. (1) Личните данни се събират за конкретни, точно определени цели, които са нормативно определени от Кодекса на труда, Закон за предучилищното и училищно образование, Държавни образователни стандарти, Кодекс на социално осигуряване и

др., обработват се законосъобразно и добросъвестно и не могат да се обработват допълнително по начин, несъвместим с тези цели. По-нататъшното обработване на личните данни за целите на архивирането в обществен интерес, за научни, исторически изследвания или за статистически цели не се счита за несъвместимо с първоначалните цели.

(2) Личните данни се съхраняват на хартиен, технически и/или електронен носител, само за времето, необходимо за изпълнение на правомощия, правни задължения на **IV СВГ** и/или нормалното му функциониране.

(3) Събирането, обработването и съхраняването на лични данни в регистрите на **IV СВГ**се извършва на хартиен, технически и/или електронен носител по централизиран и/или разпределен способ в помещения, съобразно с предвидените мерки за защита и оценката на подходящото ниво на сигурност на съответния регистър.

Чл. 9. Когато не са налице хипотезите на чл. 6, пар. 1, б. „б“ – „ е“ от Регламент 2016/679, физическите лица, чиито лични данни се обработват от **IV СВГ**, подписват Декларация за съгласие *Приложение №2*.

Чл. 10. Администрирането на личните данни в IV СВГ е възложено на следните длъжностни лица:

1. Директорът на училището
2. Главният счетоводител
3. Завеждащ административна служба
4. Ръководител направление ИКТ
5. Класните ръководители на паралелките

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

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

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

(3) Документите на електронен носител се съхраняват на специализирани сървъри, 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 с цел осигуряване на възможност 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.

(4) Достъп до архивираните документи, съдържащи лични данни, имат единствено оторизираните лица на **IV СВГ** съобразно възложените им от закона правомощия.

Чл. 12.(1) С оглед защита на хартиените, техническите и информационните ресурси всички служители са длъжни да спазват правилата за противопожарна безопасност.

(2) Служителите преминават задължителен инструктаж за запознаване с правилата за Противопожарна безопасност най-малко веднъж годишно.

Чл. 13. (1) При регистриране на неправомерен достъп до информационните масиви за лични данни, или при друг инцидент, нарушаващ сигурността на личните данни, служителят, констатирал това нарушение/инцидент, незабавно докладва за това на прекия си ръководител, който от своя страна е длъжен, своевременно да информира

Длъжностното лице по защита на данните за инцидента. Уведомяването за инцидент се извършва писмено, по електронен път или по друг начин, който позвалява да се установи извършването му.

(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) След постигане целта на обработване на личните данни, съдържащи се в поддържаните от IV СВГ регистри, личните данни следва да бъдат унищожени при спазване на процедурите, предвидени в приложимите нормативни актове и в настоящите Вътрешни правила.

(2) В случаите, в които се налага унищожаване на носител на лични данни, IV СВГ прилага необходимите действия за заличаването на личните данни по начин, изключващ възстановяване данните и злоупотреба с тях, като:

1. Личните данни, съхранявани на електронен носител и сървъри, се унищожават чрез трайно изтриване, вкл. презаписването на електронните средства или физическо унищожаване на носителите;

2. Документите на хартиен носител, съдържащи данни, се унищожават чрез нарязване.

(3) Унищожаване се осъществява от служители, упълномощени с изричен писмен акт на Директора на IV СВГи след уведомяване на Длъжностното лице по защита на данните

(4) За извършеното унищожаване на лични данни и носители на лични данни се съставя Протокол, подписан от служителите по ал.3, съгласно образец Приложение №4.

II ПРЕДОСТАВЯНЕ НА ИНФОРМАЦИЯ ЗА ЛИЧНИ ДАННИ

Чл. 15. (1) Достъп на лица до лични данни се предоставя единствено, ако те имат право на такъв достъп, съгласно действащото законодателство, след подаване на заявление, респ. искане за достъп на информация, и след тяхното легитимиране.

(2) Правото на достъп се осъществява с писмено Заявление / *Приложиение № 3/* до администратора на лични данни, което може да бъде отправено на хартиен носител или по електронен път по реда на Закона за електронния документ и елекстронния подпис и съдържа :

- Трите имена на заявителя, адрес, други данни за идентификация на лицето;
- Описание на искането;
- Предпочитана форма за предоставяне на информацията;
- Личен подпис и дата на подаване на заявлението.

(3) Достъп до личните данни имат следните лица :

1. Физическите лица, за които се отнасят данните;
2. Изрично упълномощени с нотариално заверено пълномощно лица по т.1;
3. Трети лица, в случай, че това е предвидено в нормативен акт
4. Обработващият лични данни.

(4) Достапът до лични данни е под формата на :

1. Устна или писмена справка
2. Преглед на данните
3. Предоставяне на копие от обработени данни.

(5) При поискване от физическо лице АЛД предоставя изисканата информация на предпочитан от искателя носител : хартиен носител и / или електронен носител.

(6) Физическото лице има право да поиска по всяко време следното :

1. потвърждение за това, че предоставените от него данни се обработват за целите, за които са предоставени;

2. информация за логиката на всяко автоматизирано обработване на неговите лични данни;

3. заличаване или блокиране на личните му данни, когато обработването им не отговаря на Закона за защита на личните данни.

(6) При смърт на физическото лице правата му на достъп до личните данни, отнасящи се до него се упражняват от неговите законни наследници.

(7) 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 електронен носител.

(8) Администраторът на лични данни разглежда и се произнася по заявлението в срок от четиринадесет дни, като предоставя пълен, частичен достъп или отказ за достъп до изисканите лични данни.

(9) Срокът за отговор от администратовра на лични данни може да бъде удължен до тридесет дни, ако се изисква по-продължително време за събиране и обработване на исканите от заявителя лични данни.

(10) Администраторът на лични данни отказва достъп до лични данни, когато те не съществуват в неговия регистър или когато предоставянето им е забранено със закон.

(11) Третите страни получават достъп до лични данни, обработвани в IV СВГ, при наличие на законово основание за обработването на лични данни (напр. съд, прокуратура, НАП, НОИ, Висш адвокатски съвет, Национално бюро за правна помощ и др.п.).

III. МЕРКИ ПО ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 16. ***Физическата защита*** в IV СВГ се осигурява чрез набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на сградите и помещенията, в които се извършват дейности по обработване на лични данни.

Чл. 17. (1). Основните ***организационни мерки за физическа защита*** в IV СВГ включват:

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

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

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

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

(5) Зони с контролиран достъп са всички помещения на територията на IV СВГ, в които се събират, обработват и съхраняват лични данни.

(6) *Използваните технически средства за физическа защита* на личните данни в IV СВГ са съобразени с действащото законодателство и нивото на въздействие на тези данни. Всички физически зони с хартиени и електронни записи са ограничени само за служители, които трябва да имат достъп с оглед изпълнението на работните им задължения.

(7) Всички записи и документи на хартиен носител, съдържащи лични данни, се съхраняват заключени в кабинети с ограничен достъп само за упълномощен персонал.

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

Чл. 18. (1). Основните ***технически мерки за физическа защита*** в IV СВГ включват:

1. използване на сигнално-охранителна техника;
2. Използване на ключалки и заключващи механизми;
3. шкафове, метални каси,
4. оборудване на помещенията с пожарогасителни средства.

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

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

Чл. 19. (1). Основните ***мерки за персонална защита*** на личните данни, приложими в IV СВГ, са:

1. Задължение на служителите да се запознаят с нормативната уредба в областта на защитата на лични данни
2. Спазване от служителите на настоящите Вътрешни правила и деклариране на съгласие за поемане на задължение за неразпространение на личните данни, което се удостоверява с подпис Декларация по образец – *Приложиние №1*
3. Запознаване и осъзнаване за опасностите за личните данни, обработвани от IV СВГ;
4. Забрана за споделяне на критична информация (идентификатори, пароли за достъп и др.п..)между персонала и всякакви други лица, които са неоторизирани;

Чл. 20. (1). Основните ***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 IV СВГ, сключване на договори, изпълнение на договори, упражняване на предвидени в закона права и установени от закона задължения;
2. *Определяне на условията за обработване на лични данни* - личните данни се събират и обработват само с конкретна цел, пряко свързана с изпълнение на законовите задължения, а начинът на тяхното съхранение се съобразява със специфичните нужди за обработка и физическия носител на данните;
3. *Регламентиране на достъпа до регистритес лични данни* – достъпът до регистрите с лични данни е ограничен и се предоставя само на упълномощените служители;
4. *Определяне на срокове за съхранение* - личните данни се съхраняват не по-дълго отколкото е необходимо, за да се осъществи целта, за която са били събрани или до изтичане на определения в действащото законодателство срок.
5. *Процедури за унищожаване:* Документите, съдържащи лични данни, сроковете за съхранение, на които са изтекли и не са необходими за нормалното функциониране на IV СВГ или за установяването, упражняването или защитата на правни претенции, се унищожават по подходящ и сигурен начин (напр. изгаряне, нарязване, електронно изтриване и други подходящи за целта методи, съобразени с физическия носител на данните).

Чл. 21. (1)***Защитата на автоматизираните информационни системи и/или мрежи***в IV СВГ 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, включват:

1. Идентификация и автентификация чрез използване на уникални потребителски акаунти и пароли за всяко лице, осъществяващо достъп до мрежата и ресурсите на IV СВГ. С цел повишаване сигурността на достъпа до информация служителите задължително променят използваните от тях пароли на определен от IV СВГ период, не по-дълъг от 9 месеца. В случай на отпадане на основанието за достъп до лични данни правата на съответните лица се преустановяват (вкл. и чрез изтриване на акаунта).

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

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

- Дефиниране на обхвата на вътрешните мрежи: Като *вътрешни мрежи* се разглеждат всички локални жични мрежи и/или телекомуникационни връзки тип „точка – точка“, които се намират под контрола и администрацията на IV СВГ. 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 IV СВГ.
- Регламентиране на достъпа до вътрешната мрежа: Достъп до вътрешната мрежа имат единствено служители на IV СВГ. Достъпът до мрежата и обработваните лични данни се предоставя с оглед изпълнение на техните преки служебни задължения. 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 IV СВГ, вкл. и чрез използване на защитни стени и други адекватни мерки и инструменти.

4 *Защитата от зловреден софтуер* включва:

- използването на стандартни конфигурации за всяка компютърна и/или мрежова платформа, като системният, а при възможност и приложният, софтуер се контролира, инсталира и поддържа от ръководител на направление „Информационни и комуникационни технологии“ в IV СВГ. Забранено е инсталирането на софтуерни продукти без изричното одобрение на ИТ специалиста на IV СВГ.
- използване на вградената функционалност на операционната система и/или хардуера, които се настройват единствено от ръководител на направление „Информационни и комуникационни технологии“ в IV СВГ. Всяка промяна и/или деактивация на системите за защита от неоторизирани лица е забранена.
- активиране на автоматична защита и сканиране за зловреден софтуер и обновяване на антивирусни дефиниции. Забранено е потребителите да отказват автоматични софтуерни процеси, които актуализират вирусните дефиниции.
- забрана за пренос на данни от заразени компютри. При съмнение или установяване на заразяване на компютърна система работещият с нея е задължен да уведоми ръководител на направление „Информационни и комуникационни технологии“ в IV СВГ 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.

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

- Основната цел на архивирането е свързана с предотвратяване на загуба на информация, свързана с лични данни, която би затруднила нормалното функциониране на IV СВГ.
- Начина на архивиране: информацията следва да бъде архивирана по подходящ способ и на носител, извън конкретния физически компютър, и да позволява пълното възстановяване на данните, в случай на погиване на техния основен носител.

- Отговорност за архивиране има лицето, обработващо личните данни.
- Срокът на архивиране следва да е съобразен с действащото законодателство.
- Съхраняването на архива следва да бъде в друго физическо помещение. Всички архиви, съдържащи поверителна и/или служебна информация, трябва да се съхраняват с физически контрол на достъпа

6 Основни *електронни носители на информация са*: вътрешни твърди дискове (част от компютърна и/или сторидж система), 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.)

7 *Персоналната защита на данните* е част от цялостната охрана на IV СВГ.

8 *Личните данни в електронен вид се съхраняват* съгласно нормативно определените срокове и съобразно спецификата и нуждите на IV СВГ.

9 Данните, които вече не са необходими за целите на IV СВГ и чийто срок за съхранение е изтекъл, се *унищожават чрез приложим способ* (напр. чрез нарязване, изгаряне или постоянно заличаване от електронните средства).

10 Мерките, свързани с текущото *поддържане и експлоатация* на информационните системи и ресурси на IV СВГ, включват:

1. Оценка на сигурността, включваща периодични тестове и оценки на уязвимостта на мрежите и системите 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.
2. Забрана за притежание и ползване на хардуерни или софтуерни инструменти от персонала на IV СВГ, 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 опериращ компютър. За неоторизирано използване на подобни инструменти служителят се наказва дисциплинарно, а ако нарушението е не само дисциплинарно или представлява престъпление – и по предвидения за санкциониране на това нарушение/престъпление ред.

Чл. 22. Мерките, свързани със създаване на *физическа среда (обкръжение),* включват физически контрол на достъпа (сигнално-охранителна техника, ключалки, метални решетки и други приложими способи), създаване на подходяща работна среда, вкл. чрез поддържане на подходяща температура и нива на влажност, както и пожароизвестителна система. Те са насочени към осигуряване на среда за нормално функциониране, за защита на ИТ оборудването от неоторизиран достъп и контрол на риска от повреда и унищожаване.

Чл. 23. (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 ѝ на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

Чл. 24. (1) В IV СВГ се използва единствено софтуер с уредени авторски права. Инсталирането и/или използването на всякакъв друг тип софтуер с неуредени авторски права е забранено.

(2) На служебните компютри се използва само софтуер, който е инсталиран от ръководител на направление „Информационни и комуникационни технологии“ в IV СВГ лице. Забранено е самоволното инсталиране на всякакъв друг вид софтуер.

(3) При внедряване на нов програмен продукт за обработване на лични данни се тестват и проверяват възможностите на продукта с оглед спазване изискванията на Регламент 2016/679, Закона за защита на личните даннии осигуряване максималната защита на данните от неправомерен достъп, загубване, повреждане или унищожаване.

Чл. 25. Служителите, на които е възложено да подписват служебна кореспонденция с квалифициран електронен подпис (КЕП), нямат право да предоставят издадения им КЕП на трети лица, респ. да споделят своя PIN с трети лица.

IV. ПОДДЪРЖАНИ РЕГИСТРИ С ЛИЧНИ ДАННИ И ТЯХНОТО УПРАВЛЕНИЕ

Чл. 26. Поддържаните от IV СВГ регистри с лични данни са:

1. Служителите във връзка с трудовоправните отношения,
2. Учениците във връзка с документите им за завършен клас или етап на образование
3. Доставчици на услуги
4. Видеонаблюдение

1. *Регистър „Служители“,* за водене и съхраняване на регистрите на педагогическия и непедагогически персонал, в който се вписват следните видове лични данни:
   - *Физическа идентичност:* имена, ЕГН, паспортни данни, адрес, телефон, електронен адрес, и др.п.
   - *Социална идентичност:* информация за образование, документ за придобито образование, професионална квалификация, за придобита педагогическа правоспособност, за владеене на чужди езици, трудов стаж, включително педагогически стаж, предшестващ вписването в регистъра и др.п.;
   - *Лични данни относно съдебното минало:* свидетелство за съдимост;
   - *Данни за здравословно състояние:* медицинско свидетелство от психодиспансер, болнични листове, решения на ТЕЛК/НЕЛК и др.п.
   - Личните трудови досиета се обработват и съхраняват в отделни хронологично оформени папки от завеждащ административна служба в канцелария при мерки за сигурност и защита.
   - Личните трудови досиета съдържат конфиденциална информация , която не може да бъде разгласявана без изричното съгласие на служителя.
   - Личните данни , организирани и съхранявани на електронен носител се въвеждат, обработват и съхраняват на отделен компютър за всяко длъжностно лице , защитен с парола за достъп само за обработващия данните и при използване само на лицензиран софтуер и услугите на лицензирани доставчици на софуерни услуги .
2. *Регистър „Ученици“,* в който се вписват следните видове лични данни:
   - *Физическа идентичност* – имена, паспортни данни (ЕГН, номер на лична карта, дата и място на издаване, адрес, телефон за връзка и други необходими за идентифициране на субекта на данни);
   - *Социална идентичност* – данни относно образование и допълнителна квалификация, трудова дейност и професионална биография;

- *Икономическа идентичност* – информация за номер на банкова сметка, данни относно имотното и финансово състояние на лицето, участието и/или притежаването на дялове или ценни книжа на дружества и други, изискуеми с оглед преценка на изискванията за съвместимост за съответната длъжност;

- Дневниците и личните картони на учениците се обработват от класните ръководители, съхраняват на хартиен носител в канцеларията на зам. директора, а след тяхното приключване в архива на училището при спазване правила за ситгурност и срокове съгласно Номенклатура на делата и срокове за тяхното съхранение. Дневниците на паралелките и личните картони на учениците съдържат лични данни, които са конфиденциални и не могат да бъдат разпространявани на трети лица.
- Главна класна книга, Книга за резултатите от проведени изпити с ученици от самостоятелна и индивидуална форма на обучение, Книги за регистриране завършен клас или етап на образование съдържат лични данни за учениците и се попълват от длъжностни лица, определени със заповед на директора. Те се съхраняват в канцеларията.
- Длъжностните лица, отговорни за обработването на лични данни на учениците нямат право да изнасят поверените им документи извън училище , както и да разпространяват поверената им информация.

3. *Регистър „Доставчици на услуги“*, в който се вписват следните видове лични данни:

- *Физическа идентичност* – имена, паспортни данни (ЕГН, номер на лична карта, дата и място на издаване, адрес, телефон за връзка и други необходими за идентифициране на субекта на данни);
- *Икономическа идентичност* – обща банкова информация, информация за номер на банкова сметка и др.;
- *Лични данни относно съдебното минало на лицето* (свидетелство за съдимост в зависимост от вида на преддоговорните отношения);
- Документите се съхраняват в канцеларията или дирекцията.

4. *Регистър „Видеонаблюдение",* в който 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 посетители, ученици, преподаватели и служители в сградата на училището и подстъпите към нея. Регистърът съдържа следните групи данни - физическата идентичност на лицето – видеообраз
- Регистърът „Видеонаблюдение „ се попълва с данни от автоматично денонощно видеонаблюдение (видеообрази) при движение в служители, ученици и външни лица сградата на училището .
- Оператори на лични данни на регистър „Видеонаблюдение" са директор и ръководител направление „Информационни технологии“. Архивирани данни от видеонаблюдение са записи от проведени годишни изпити на самостоятелна и задочна форма на обучение и Държавни зрелостни изпити, които се съхраняват в дирекцията за определения от заповед на Министъра на МОН срок.
- 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.

- 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.
- Лични данни се съхраняват в паметта на дивиара за срок до 30 дни. При необходимост записите могат да бъдат свалени на външен носител. Позволява се съхраняване на данни извън 30 дневния срок, когато това е указано в нормативен акт или разпоредено от надлежен орган.
- След постигане целите по предходната алинея личните данни се унищожават физически, чрез изтриване.
- Данните в регистъра се предоставят доброволно от лицата при подхода и влизането им в сградата на училището.
- На входа на сградата и на видни места в коридорите се поставят информационни табла за уведомяване на гражданите, че при влизане и излизане от сградата подлежат на проверка съгласно чл. 30, ал. 1, т. 1, буква „а" и „б" от ЗЧОД и за използването на технически средства за наблюдение и контрол съгласно чл. 30, ал. 2 и ал. 4 от ЗЧОД.

V. ПРАВА И ЗАДЪЛЖЕНИЯ НА ЛИЦАТА, ОБРАБОТВАЩИ ЛИЧНИ ДАННИ

Чл. 27. (1) Длъжностно лице по защита на данните се определя от Ръководството на IV СВГ.

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

1. осигурява организацията по водене на регистрите, съгласно предвидените мерки за гарантиране на адекватна защита;
2. следи за спазването на конкретните мерки за защита и контрол на достъпа съобразно спецификата на водените регистри с лични данни;
3. осъществява контрол по спазване на изискванията за защита на регистрите съобразно действащото законодателство и настоящите вътрешни правила;
4. поддържа връзка с Комисията за защита на личните данни относно предприетите мерки и средства за защита на регистрите и подадените заявления за предоставяне на лични данни;
5. контролира спазването на правата на потребителите във връзка с регистрите и програмно-техническите ресурси за тяхната обработка;
6. специфицира техническите ресурси, прилагани за обработка на личните данни;
7. следи за спазване на организационната процедура за обработване на личните данни, включваща време, място и ред при обработване, чрез регистрация на всички извършени действия с регистрите в компютърната среда;
8. определя ред за съхраняване и унищожаване на информационни носители;
9. определя ред при задаване, използване и промяна на пароли, както и действията в случай на узнаване на парола и/или криптографски ключ;
10. определя правила за провеждане на редовна профилактика на компютърните и комуникационните средства, включваща и проверка за вируси, за нелегално инсталиран софтуер, на целостта на базата данни, както и архивиране на данни, актуализиране на системната информация и др.;

11. провежда периодичен контрол за спазване на изискванията по защита на данните и при открити нередности взема мерки за тяхното отстраняване;

Чл 28. Служителите на IV СВГ са длъжни:

1. да обработват лични данни законосъобразно и добросъвестно;
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 при необходимост регистрите на личните данни;
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.

Чл. 29. (1) За неспазването на разпоредбите на настоящите Вътрешни правила служителите носят дисциплинарна отговорност.

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

VI. ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

Чл. 30. Всички служители на IV СВГ са длъжни да се запознаят с настоящите Вътрешни правила и да ги спазват ежедневно при изпълняване на заемната от тях длъжност и възложената им работа.

Чл. 31.(1) За всички неуредени в настоящитеВътрешни правила въпроси, са приложими разпоредбите на Общия регламент относно защитата на данните (ЕС) 2016/679, приложимото право на Европейския съюз изаконодателството на Република България относно защитата на личните данни,.

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

- **Приложение № 1** – Декларация за конфиденциалност и спазване на Вътрешните правила от длъжностните лица в IV СВГ
- **Приложение № 2** – Декларация за съгласие за обработка на лични данни /от служители, ученици, трети лица/
- **Приложение № 3 –** Заявление за предоставяне на лични данни
- **Приложение № 4 –** Протокол за унищожаване на лични данни;

Настоящите вътрешни правила са приети с решение на ПС с Протокол №15 от 02.09.2019 г..

Приложение № 1

IV Сменно-вечерна гимназия „Отец Паисий”

Д Е К Л А Р А Ц И Я

Долуподписаният/та .....
ЕГН:.....

Д Е К Л А Р И Р А М

Запознат съм с Вътрешните правила на IV Сменно-вечерна гимназия „Отец Паисий“ за мерките за защита на личните данни, съгласно Регламент 2016/679.

Познавам правилата за сигурност при обработването на лични данни и с прилаганите от IV Сменно-вечерна гимназия „Отец Паисий“ мерки за физическа, персонална, документална защита на личните данни и защитата на автоматизирани информационни системи и мрежи по отношение на регистрите с лични данни, до които имам достъп при осъществяване на трудовата ми функция.

Като администратор на лични данни в качеството си на ..... имам задължение да приемем, обработвам и съхранявам лични данни законосъобразно и добросъвестно. Като администратор на лични данни нямам право да разпространявам информация за лични данни, станали ми известни при изпълнение на служебните ми задължения.

Нося отговорност за опазване на документи, съдържащи лични данни на служители и/или ученици. За неспазване на разпоредбите на ЗЗЛД нося административна отговорност.

Декларатор :
Име и фамилия / подпис

Приложение 2

ДЕКЛАРАЦИЯ

За съгласие за обработка на лични данни

Долуподписаният/ата .....
ЕГН.....Лична карта №.....издадена на..... от.....

Известно ми е, че IV Сменно-вечерна гимназия „Отец Паисий“, град София е администратор на лични данни.

Декларирам, че предоставям доброволно и свободно личните си данни и давам съгласието си същите да бъдат обработвани и съхранявани от IV Сменно-вечернагимназия „Отец Паисий““, град София за дейности , свързани със сключване, изменение и прекратяване на трудовите правоотношения, съставяне на договори, допълнителни споразумения, заповеди, документи, удостоверяващи трудов стаж, доходи от трудови правоотношения и по граждански договори, служебни бележки, справки, удостоверения и установяване на връзка с мен за коренспонденция.

Известно ми е , че във всеки един момент имам право на достъп до личните ми данни, както и да ги коригирам, посредством заявление, отправено към администратора в писмена форма или по електронен път по реда на Закона за електронния подпис и електронния документ.

Запознат/а съм, че мога да осъществявам посочените права по реда на чл. 28а-чл. 34а от ЗЗЛД. Запознат съм с всички данни съгласно чл. 19 от ЗЗЛД

Декларатор : .....
Име фамилия подпис

Приложение 2

ДЕКЛАРАЦИЯ

За съгласие за обработка на лични данни

Долуподписаният/ата .....
ЕГН.....

Известно ми е, че IV Сменно-вечерна гимназия „Отец Паисий“, град София е администратор на лични данни.

Декларирам, че предоставям доброволно и свободно личните си данни и давам съгласието си същите да бъдат обработвани и съхранявани от IV Сменно-вечерна гимназия „Отец Паисий“, град София за дейности, свързани с обучението ми в училището - водене на задължителна документация, издаване на документи за завършен клас/ етап на образование.

Известно ми е, че във всеки един момент имам право на достъп до личните ми данни, както и да ги коригирам, посредствам заявление, отправено към администратора в писмена форма или по електронен път по реда на Закона за електронния подпис и електронния документ.

Запознат/а съм, че мога да осъществявам посочените права по реда на чл. 28а-чл. 34а от ЗЗЛД. Запознат/а съм с всички данни съгласно чл. 19 от ЗЗЛД

Декларатор : .....

Име фамилия подпис

Приложение 3

ДО
Директора на
IV Сменно-вечерна гимназия „Отец Паисий”

З А Я В Л Е Н И Е
за предоставяне на лични данни

От .....
/трите имена на заявителя/
Трите имена на упълномощено лице .....
Адрес за кореспондеция....., Тел. за връзка.....

Г-н, г-жо Директор,

Във връзка с ..... желая : /посочва се причината/

На основание чл. 29. , ал. 1 от ЗЗЛД желая да получа данни относно :

1. .....
2. .....
3. .....
4.

Предпочитам предоставената информация да бъде на: хартиен носител, електронен носител, електронна поща /

Личен подпис
Дата

Приложение 4

IV Сменно-вечерна гимназия „Отец Паисий”

ПРОТОКОЛ

за унищожаване на лични данни

Днес ....., подписаният/ата ……., служител на длъжност: …….., упълномощен(а) на основание чл. 20, ал. 1, т. 5 от Вътрешните правила на IV СВГ за мерките за защита на личните данни със Заповед на директора на IV СВГ от …….., да извърша унищожаване на лични данни и носители на лични данни с изтекъл срок за съхранение, част от Регистър с лични данни „……“, съставих настоящия протокол за унищожаването на лични данни с изтекъл срок за съхранение, включително и резервни копия от тях, както следва:

1. Данни съхранявани на магнитни носители за многократен запис, чрез **трайно изтриване, вкл. презаписването на носителите**.

2. Данни съхранявани на хартиен носител, чрез: **нарязване.**

3. Данни съхранявани на оптични носители за еднократен запис, чрез **физическо унищожаване на носителите:**

Унищожените данни:

Не са обработвани чрез облачни услуги.

Служител: ……..

/……/