



38

Финансово-стопанска гимназия „Васил Левски“

9300, гр. Добрич, улица „Генерал Гурко“ № 1, п.к. 132

+ 359 58 600 143 – Директор + 359 58 600 144 – Заместник-директор

+ 359 58 600 171 – Главен счетоводител, канцелария

e-mail: fsgdobrich@mail.bg

Web: www.fsgdobrich.org

УТВЪРЖДАВАМ
Минка Господинова



ВЪТРЕШНИ ПРАВИЛА

ЗА МЕРКИТЕ И СРЕДСТВАТА ЗА ОБРАБОТВАНЕ И ЗАЩИТА НА ЛИЧНИ
ДАНИИ

ВЪВ

ФИНАНСОВО-СТОПАНСКА ГИМНАЗИЯ „ВАСИЛ ЛЕВСКИ“

Добрич, 2022 г.

ГЛАВА ПЪРВА Общи положения

Чл. 1.(1) Финансово-стопанска гимназия „Васил Левски“ (училището) е юридическо лице със седалище гр. Добрич, Р България с основен предмет на дейност наука, образование и образователни услуги.

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

Чл. 2. (1) С тези вътрешни правила се уреждат редът и условията за набиране, обработване, актуализация, съхраняване, предоставяне, трансфер и унищожаване на личните данни, както и мерките и средствата за тяхната защита.

(2) Настоящите правила се издават на основание Регламент (ЕС) 2016/679 и Закона за защита на личните данни (ЗЗЛД).

(3) Правилата се утвърждават, допълват, изменят и отменят от Директора на ФСГ „Васил Левски“ - администратор па лични данни.

(4) Администраторът предоставя достъп до обработваните от него лични данни на физическите лица и на трети лица съобразно Регламент (ЕС) 2016/679 на ЕС и ЗЗЛД.

ГЛАВА ВТОРА Цели и обхват на правилата

Чл. 3. Настоящите Правила имат за цел да регламентират:

(1) механизмите за набиране, обработване, актуализация, съхраняване, предоставяне, трансфер и унищожаване на личните данни;

(2) задълженията на Администратора, лицата обработващи лични данни, длъжностното лице по защита на лични данни и тяхната отговорност при неизпълнение на тези задължения;

(3) правилата за разпределение на личните данни и групирането им в регистри и Правилата за работа с личните данни;

(4) необходимите технически и организационни мерки за защита личните данни от неправомерно обработване (случайно или незаконно разрушаване, случайна загуба или промяна, незаконно разкриване или достъп, нерегламентирано изменение или разпространение, както и от всички друг и незаконни форми на обработване на лични данни),

Чл. 4. За целите на настоящите вътрешни правила понятията по-долу имат следното значение:

1. **„Лични данни“** са всяка информация, отнасяща се до физически лица и физическите лица, представляващи юридически училището, както и тази, свързана с неговите служители, които са идентифицирани или чрез която същите могат да бъдат идентифицирани пряко или непряко чрез идентификационен номер или чрез един или повече специфични признаци.

2. **„Обработване на лични данни“** е всяко действие или съвкупност от действия, които училището извършва по отношение наличните данни с автоматични или неавтоматични средства (събиране, записване, организиране, съхраняване, адаптиране или изменение, възстановяване, консултиране, употреба, разкриване чрез предаване, разпространяване, предоставяне, актуализиране или комбиниране, блокиране, заличаване или унищожаване и др.).

3. **„Администратор на лични данни“** е училището, което самостоятелно или чрез възлагане на друго лице обработва лични данни.

4. **„Регистър на лични данни“** е структурирана съвкупност от лични данни, достъпна по определени критерии съобразно вътрешните документи на училището, която може да бъде централизирана и децентрализирана и е разпределена на функционален принцип,

5. **„Съгласие на физическо 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.

Чл. 5.(1) Училището обработва само законно събрани лични данни, необходими за конкретни, точно определени и законни цели. Личните данни, които училището събира и обработва следва да бъдат точни и при необходимост да се актуализират. Личните данни се заличават или коригират, когато се установи, че са неточни или несъответстват на целите, за които се обработват.

(2) Училището поддържа личните данни във вида и формата, които позволяват идентифициране самоличността на физическите лица за срок не по-дълъг от необходимия за изпълнение на целите, за които личните данни се обработват.

(3) Училището спазва принципа за забрана на обработване на специални категории данни съгласно чл. 5, ал. 1 от ЗЗЛД (разкриване на расов или етнически произход, разкриване на политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели, лични данни, които се отнасят до здравето, сексуалния живот или до човешкия геном), като изключения се допускат само в случаите, предвидени в чл. 5, ал. 2 от ЗЗЛД.

Чл. 6. (1) Субектът на личните данни декларира свободно своето съгласие относно обработването на отнасящи се за него лични данни.

(2) Субектът на личните данни има право по всяко време на обработването да поиска блокиране или унищожаване (изтриване) на събрани за него лични данни, в случаите, когато оспорва тяхната точност или обработването им е незаконосъобразно.

Чл. 7. Обработването на личните данни се извършва, когато:

1. Това е необходимо за изпълнение на нормативно установено задължение.

2. Физическото лице, за което се отнасят данните, е дало своето изрично съгласие. Субектът на лични данни и служителите на училището, се идентифицират посредством официален документ за самоличност (лична карта). Документите, които са необходими за извършване на законни действия, задължително се копират, като субектът изписва на копие „Съгласен(а) а съм с копирането" и се подписва върху него..

3. Обработването е необходимо за изпълнение на задължения по договор, по който физическото лице, за което се отнасят данните, е страна, както и действия, предхождащи сключването на договор и предприети по негово искане.

Чл. 8. Всички служители на училището при встъпване в длъжност се задължават да спазват конфиденциалност по отношение на базата данни до които имат достъп, в т.ч. лични данни, както и да не разгласяват данни и информация, станали им известни при и по повод изпълнение на служебните им задължения.

Чл. 9. Училището поддържа вътрешен ред като администратор на лични данни, като осигурява технически и организационни мерки за защита.

Чл. 10. Правилата са задължителни за всички лица, имащи достъп до личните данни, обработвани за нуждите на администратора.

ГЛАВА ТРЕТА Мерки за защита при обработване на личните данни

Чл. 11. (1) 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.

(2) Училището прилага адекватна защита на личните данни, съобразена с нивото на нейното въздействие.

(3) Тя включва:

1. **Физическа защита** - осигурява се чрез набор от приложими технически и организационни

мерки за предотвратяване на нерегламентиран достъп и защита на сградите и помещенията, в които се създават, обработват и съхраняват лични данни.

- Като помещения, в които ще се обработват лични данни, се определят всички помещения, в които с оглед нормалното протичане на учебния и административния процес, се събират, обработват и съхраняват лични данни. Достъпът до тях е физически ограничен само за служители с оглед изпълнение на служебните им задължения, както и лицата, натоварени със служебни ангажменти за поддържането на нормалното функциониране на тези системи. Последните нямат достъп до съхраняваните в електронен вид данни.

Основните приложими *технически мерки за физическа защита са шкафове или картотеки, които могат да се заключават с ключалки (механични или електронни)* за ограничаване достъпа на външни лица и наличие на пожарогасителни средства.

2. Персонална защита

- Задължение на служителите е да се запознаят с нормативната уредба в областта на защитата на лични данни и настоящата инструкция срещу подпис;

- Запознаване и осъзнаване за опасностите за личните данни;

- Забрана за споделяне на критична информация между персонала (например идентификатори, пароли за достъп и т.н.);

- Деклариране на съгласие за поемане на задължение за неразпространение на личните данни.

- Тренировка на персонала за реакция при събития, застрашаващи сигурността на данните, в случай че спецификата на служебните задължения и/или изисква подобно.

3. Документална защита

- Определяне на регистрите, които ще се поддържат на хартиен носител;

- Определяне на условията за обработване на лични данни;

- Регламентиране на достъпа до регистрите;

- Определяне на срокове за съхранение;

- Процедури за унищожаване.

4. Защита на автоматизирани информационни системи и/или мрежи:

- Идентификация и автентификация чрез използване на уникални потребителски акаунти и пароли за всяко лице, осъществяващо достъп до мрежата и ресурсите на училището;

- 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;

- Управление на външни връзки и/или свързване;

- Администриране на достъпа до вътрешната мрежа;

- забрана за пренос на данни от заразени компютри;

- Политиката по създаване и поддържане на резервни копия за възстановяване;

- Личните данни в електронен вид се съхраняват съгласно нормативно определените срокове и съобразно спецификата и нуждите на училището.

3. Криптографска защита

(1) Информацията да бъде направена неразбираема за неавторизирани потребители.

(2) По отношение на лични данни, оценени със степен на въздействие по-висока от „ниско“, се прилагат и мерки, свързани с криптографска защита на данните чрез стандартните криптографски възможности на операционните системи, на системите за управление на бази

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

(3) Забрана за притежание и ползване на хардуерни или софтуерни инструменти от персонала на училището и обучаваните лица, 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.

(4) Правилата за защита при обработване на лични данни регламентират технически мерки, които:

1. отхвърлят достъпа на неоторизирани лица до оборудването за обработка на данни – контрол на достъпа до оборудване;

2. предотвратяват неоторизираното четене, копиране, промяна или унищожаване на информационни носители – контрол на информационните носители;

3. предотвратяват неоторизираното добавяне, въвеждане, преглеждане, промяна или заличаване на съхранени лични данни – контрол по съхраняването;

4. предотвратяват използването му от неоторизирани лица, използващи комуникационно оборудване за данни - контрол на потребителите;

5. гарантират, че лицата, които са оторизирани да ползват система за автоматизирана обработка на данни, имат достъп само до данните, включени в обхвата на техния достъп – контрол на достъпа до данни;

6. осигуряват възможността за проверка и установяване до кои органи са били или могат да бъдат изпратени или предоставени личните данни чрез използване на комуникационно оборудване за данни – контрол на комуникациите;

7. осигуряват възможност за последваща проверка и установяване какви лични данни са въведени в системите за автоматизирана обработка на данни, кога и от кого са въведени данните - контрол на въвеждане;

8. предотвратяват неоторизирано четене, копиране, промяна или изтриване на лични данни при трансфер на лични данни или превозване на носители на данни – контрол при транспортиране;

9. осигуряване на възможност инсталираните системи да могат да се възстановят в случай на прекъсване на функционирането – възстановяване;

10. осигуряват правилното функциониране на системата, докладване на появата на грешки във функциите (надеждност) и гарантират, че съхранените данни не могат да бъдат повредени чрез неправилно функциониране на системата – интегритет.

Чл. 12. (1) Служителят/ите, обработващи лични данни, вземат мерки за гарантиране на надеждност при обработването, като осъществяват технически и организационни мерки за защита на личните данни.

(2) При автоматичната обработка на лични данни се осъществяват технически мерки за защита срещу:

1. неоторизирано четене, възпроизвеждане, промяна или премахване на носителя на данните;

2. неоторизирано въвеждане, промяна или заличаване на съхранени лични данни;

3. неоторизирано използване на системите за лични данни чрез средства за пренос на данни;

4. неоторизиран достъп до лични данни.

Чл. 13. Базисни правила и мерки за осигуряване на защита на личните данни при компютърна обработка:

(1) Компютърен достъп към файлове, съдържащи лични данни, се осъществява само от длъжностни лица с регламентирани права, единствено от тяхното физическо работно място, от специално определения за целта компютър и след идентификация чрез парола.

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

(3) 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.

(4) При необходимост от ремонт на компютърната техника, предоставянето ѝ на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

(5) В училището се използва единствено софтуер с уредени авторски права. На служебните компютри се използва само софтуер, който е инсталиран от оторизирано лице.

(6) 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.

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

ГЛАВА ЧЕТВЪРТА Оценки на въздействието върху обработваните лични данни

Чл.14. (1) Оценката на въздействието 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.

(2). 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.

Чл.15. При оценката на въздействието администраторът отчита характера на обработваните лични данни, както следва:

1. систематизиране и оценка на лични аспекти, свързани с дадено физическо лице (профилирано), за анализиране или прогнозиране, по-специално на неговото икономическо положение, местоположение, лични предпочитания, надеждност или поведение и др.

2. данни, които разкриват расов или етнически произход, политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели, или данни, които се отнасят до здравето, сексуалния живот или до човешкия геном;

3. лични данни чрез създаване на видеозапис от видео наблюдение на публично достъпни райони;

4. лични данни в широко мащабни регистри на лични данни - данни, чието обработване, съгласно решение на Комисията за защита на личните данни застрашава правата и законните интереси на физическите лица,

Чл. 16, Определят се следните нива на въздействие:

1. **„Исключително високо”** – в случаите, когато неправомерното обработване на лични данни би могло да доведе до възникване на значителни вреди или кражба на само личност на особено голяма група физически лица или трайни здравословни увреждания или смърт на група физически лица:

2. **„Високо“** – в случаите когато неправомерното обработване на лични данни би могло да доведе до възникване на значителни вреди или кражба на самоличност на голяма група физически лица или лица, заемащи висши държавни длъжности, или трайни здравословни увреждания или смърт на отделно физическо лице;

3. **„Средно“** – в случаите, когато неправомерното обработване на лични данни би могло да създаде опасност от засягане на интереси, разкриващи расов или етнически произход, политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели, здравословното състояние, сексуалния живот или човешкия геном на отделно физическо лице или група физически лица;

4. **„Ниско“** - в случаите, когато неправомерното обработване на лични данни би застрашило неприкосновеността на личността и личния живот на отделно физическо лице или група физически лица.

Чл. 17. (1) Администраторът извършва оценка на въздействие за всички поддържани регистри.

(2) Всеки отделен регистър се оценява по критериите поверителност, цялостност и наличност.

(3) Най-високото ниво на въздействие, определено по всеки от критериите по ал. 2 определя нивото на въздействие на съответния регистър.

Чл. 18. В зависимост от нивото на въздействие се определя и съответно ниво на защита.

Чл. 19. (1) Нивата на защита са ниско, средно, високо и изключително високо.

(2) Нивата на защита са, както следва:

1. при ниско ниво на въздействие – ниско ниво на защита;
2. при средно ниво на въздействие – средно ниво на защита;
3. при високо ниво на въздействие – високо ниво на защита;
4. при изключително високо ниво на въздействие – изключително високо ниво на защита.

ГЛАВА ПЕТА Предназначение и видове регистри

Чл. 20. (1) В изпълнение на дейностите си училището о поддържа регистри на лични данни,

(2) Училището поддържа следните регистри:

1. Ученици
2. Родители
3. Персонал
4. Заплати и хонорари
5. Болнични листи
6. Деловодство
7. Пропускателен режим – Външни посетители
7. Видеонаблюдение
8. Контрагенти и партньори
9. Счетоводство
10. Трудови злоупотреки

(3) Подробно описание на регистрите включително категории физически лица, за които се обработват лични данни, групи обработвани данни, източници и средства за събирането им, форма за водене на регистъра, ред за съхраняване и унищожаване на информационни

носителите, служителите, обработващи лични данни, техническите ресурси, прилагани за обработване на данните в електронните регистри и други се съдържа в Приложенията, неразделна част от настоящите Вътрешни правила.

(4) Създаването на нови регистри и извършването на промени се извършва със заповед на Директора на Администратора,

Групи данни и регистъра

Чл. 21. (1) В зависимост от нормативното основание за събирането и предназначението им в регистрите се набират, обработва и съхраняват лични данни относно:

1. физическата идентичност на лицата – имена, ЕГН, номер на документ за самоличност, дата и място на издаването му, адрес, месторождение, телефони за контакт, електронна поща;

2. семейна идентичност на лицата – семейно положение, брой членове на семейството, родствени връзки и др.;

3. образование – вид на образованието, място, номер и дата на издаването на дипломата, допълнителна квалификация и др.;

4. трудова дейност – професионална биография, дни в осигуряване, осигурителен доход, основание за осигуряване, осигурени социални рискове, трудови договори, осигурители и други;

5. медицински данни – здравен статус, медицински диагнози и заключения на медицинската експертиза на временната и трайна неработоспособност;

6. други лични данни – осигурителен доход, трудови възнаграждения, парични обезщетения, статус на липето (осъждено/неосъждено/реабилитирано) и други,

(2) Личните данни в регистри се събират от администратора на лични данни на хартиен или електронен носител.

Чл. 22. Задължения на лицето, отговарящо за водене и съхраняване на данните в регистрите (оправомощеното лице) включват набиране, обработване, актуализация и съхраняване на лични данни.

Чл. 23. (1) В регистър „ученици“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица „ученици“, обучавани в училището след представянето на декларация от родител, настойник или лице носещо родителска отговорност.

(2) Общо описание на регистър „Ученици“

Регистърът съдържа следните категории лични данни:

1. физическата идентичност на лицето: име, ЕГН, адрес, данни от личната карта.
2. месторождение, телефони за връзка;
3. културна идентичност: интереси и хоби;
4. лични данни, които се отнасят до здравето.

Нормативното основание е Закон за предучилищното и училищното образование (ЗПУО) и приложимото законодателство, свързано с предоставянето на образователни услуги.

Определяне на длъжностите, **обработващи** лични данни на регистър „Ученици“ са класните ръководители и завеждащ административна служба (ЗАС) на училището.

Оператор на лични данни на регистър „Ученици“ е целия педагогически персонал. Длъжностните лица – обработващи лични данни и оператори на лични данни предприемат всички организационно-технически мерки за съхраняването и опазването на личните данни.

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.

- Достъп до регистър „Ученици“ имат и държавните органи – МОН, РУО, дирекция „Социално подпомагане“, Държавна агенция за защита на детето (ДАЗД) 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 др., когато са изискали данните по надлежен ред във връзка с изпълнението на техните правомощия.

- Достъп до обработваните лични данни имат и застрахователни дружества – за изпълнение на техните задължения, предвидени в нормативните актове, когато тези данни са поискани по надлежен ред.

- 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 във ФСГ „Васил Левски“.

- След постигане целите по предходната алинея личните данни на учениците се унищожават физически, чрез нарязване или изгаряне, за което се изготвят актови протоколи за унищожаване.

(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 на операторите на лични данни, снабдени със защитна сигнализация. Информацията от хартиените носители за всеки ученик, се записва в подрегистрите както следва:

1. **Книга за подлежащите на задължително обучение деца до 16-годишна възраст** е предназначена за водене на отчет на деца от задължителната училищна възраст и се попълва с данни, събрани за учениците от класните им ръководители и съдържа: имена, ЕГН и др.

Регистърът **се води** от упълномощено лице със заповед на директора.

Данните от регистъра се предоставят доброволно от лицата при записването им. Книгата се съхранява в канцеларията на гимназията.

Право на достъп до данните в регистъра имат:

- Лицата за които се отнасят данните и регистъра, до тяхно изрично искане;
- Директорът, зам.-директорът, ЗАС, класните ръководители при изпълнение на правомощията им по Кодекса на труда и длъжностна характеристика.
- Държавни органи, надлежно легитимирани се със съответни документи - писмени разпореждания на съответния орган, в който се посочва основаниято, имената на лицата, на които е необходимо да се осигури достъп до личните данни.

2. Регистър „Дневници“ е предназначен за вписване на информация за резултатите от учебната дейност на всеки ученик в една паралелка за една учебна година и съдържа имена, адрес, телефони за връзка с родител и личен лекар и оценки. Регистърът се води от класния ръководител и всеки учител, който преподава в класа и се контролира от заместник-директора.

- Данните в регистъра се събират за лицата в процес на обучението им в учебното заведение.
- Дневниците се съхраняват в учителската стая. След приключване на учебната година се предават в архива на училището.

- Право на достъп до данните в регистъра имат:
 - Лицата за които се отнасят данните в регистъра, по тяхно изрично искане;
 - Директорът, заместник-директорът, учителите при изпълнение на правомощията им по длъжностна характеристика.
 - Държавни органи, надлежно легитимирани се със съответни документи – писмени разпореждания на съответния орган, в който се посочва основанието, имената на лицата, на които е необходимо да се осигури достъп до личните данни.
- Регистърът се води в хартиен и електронен вариант, а от учебната 2019/2020 – само в електронен вариант.

3. Регистър „Лични дела“ на учениците е предназначен за вписване на информация за резултатите от учебната дейност на всеки ученик в една паралелка за срока му на обучение в училище и съдържа имена, ЕГН, адрес, издадени документи и оценки. Данните в регистъра се събират за лицата в пропеса на обучението.

Картотеката се съхранява при ЗАС на училището,

Право на достъп до данните в регистъра имат:

- Лицата за които се отнасят данните в регистъра, по тяхно изрично искане;
- Директорът, заместник-директорът, класните ръководители при изпълнение на правомощията им по длъжностна характеристика.
- Държавни органи, надлежно легитимирани се със съответни документи – писмени разпореждания на съответния орган, в който се посочва основанието, имената на лицата, на които е необходимо да се осигури достъп до личните данни.

Данните от регистъра служат за изготвяне на съответните удостоверения за преместване, удостоверения за завършен клас, дипломи за завършено средно образование, свидетелства за професионална квалификация, които остават у приносителя.

Издаването на свидетелство за професионална квалификация, диплома за завършено средно образование, се извършва в електронен вариант и сканирано копие, което се изпраща в МОН, в нарочно създаден регистър „Дипломи“. Копие от документа се съхранява в архива на училището. Регистърът се води от класния ръководител и се контролира от директора.

4. Регистрационна книга за издадените дубликати на документи за завършена степен на образование и за придобита професионална квалификация е предназначена за регистриране дубликати на свидетелства за основно образование, удостоверение за завършен гимназиален етап, дипломи за завършена образователна степен, удостоверения за професионално обучение, свидетелства за професионална квалификация.

За дубликати на свидетелство за основно образование се води обща регистрационна книга.

Книгата се води от длъжностно лице, определено със заповед на директора.

Със заповед на директора се определя мястото за съхранение на книгата до приключването ѝ, след което книгата се съхранява в архива на инструкцията със срок постоянен.

Право на достъп до данните и регистъра имат:

- Лицата за които се отнасят данните в регистъра, по тяхно изрично искане;
- Директорът, заместник-директорът, ЗАС на училището при изпълнение на правомощията им по длъжностна характеристика,
- Държавни органи, надлежно легитимирани се със съответни документи – писмени разпореждания на съответния орган, в който се посочва основанието, имената на лицата, на които е необходимо да се осигури достъп до личните данни.

Данните от регистъра се сканират и се предават по електронен път в регистър „Дипломи“ на МОН.

5. **Регистрационна книга за издадените удостоверения** е предназначена за регистриране на удостоверение за завършен клас.

За регистриране на дубликатите на удостоверения се завежда отделна книга от същия вид.

Книгата се води от длъжностно лице, определено със заповед на директора.

Със заповед на директора се определя мястото на съхранение на книгата до приключването ѝ, след което книгата се съхранява в архива на училището със срок постоянен.

Право на достъп до данните в регистъра имат:

- Лицата за които се отнасят данните в регистъра, по тяхно изрично искане;
- Директорът, заместник-директорът, ЗАС при изпълнение на правомощията им по длъжностна характерно и ка.
- Държавни органи надлежно легатимирани се със съответни документи – писмени разпореждания на съответния орган, в които се посочва основанието, имената на лицата, на които е необходимо да се осигури достъп до личните данни.

Данните от регистъра не могат да бъдат предавани по електронен път,

6. **Регистър Копия на характеристики на ученика за завършена степен на образование.**

Характеристика на ученика за завършена степен на образование се изготвя от класния ръководител за всеки ученик при придобиване на средно образование.

Копие от характеристиката на ученика за завършена степен на образование се съхранява в архива на училището.

Със заповед на директора се определя мястото на съхранение на хартиения носител и отговорните длъжностни лица.

Право на достъп до данните в регистъра имат:

- Лицата за които се отнасят данните в регистъра, по тяхно изрично искане;
- Директорът, заместник-директорите, класните ръководители при изпълнение на правомощията им по длъжностна характеристика.

Данните от регистъра не могат да бъдат предавани по електронен път.

7. **Регистър „Читателска картотека“**

В регистър „Читателска картотека“ се набират, обработват и съхраняват лични данни на ползващи библиотеката лица с оглед на:

1. индивидуализиране на читателите;
2. изпълнение на нормативните изисквания по Наръчника по библиотечна техника;
3. регистриране на библиотечните единици, които получават читателите;
4. Формата на водене на регистъра е на хартиен носител;
5. Данните се предоставят устно, записват се от оператора на лични данни на читателски картони, които се съхраняват в специализирани библиотечни шкафове с чекмеджета.
6. Длъжностните лица от Библиотечно-информационната база - оператори на лични данни предприемат всички организационно-технически мерки за съхраняването и опазването на читателските картони, в това число ограничаване на достъпа до тях на външни лица и служители.
7. Личните картони на читателите не се изнасят извън сградата на администратора.
8. В регистър „Читателска картотека“ се обработват следните групи лични данни:
 - Относно физическата идентичност на лицата: имена, ЕГН, данни от лична карта,

адрес и телефони за връзка;

- -Относно трудовата дейност: длъжност, месторабота.
- -Относно образованието: специалност , клас.
- -Дата на връщане, подпис на читателя при получаване, подпис на библиотекаря при връщане.

9. Сключването на договора с читателя се установява е писмен документ: читателска карта (читателеки картон). Документът се подписва от читателя.

10. На основание Наредбата за запазване на библиотечните фондове, читателите, попълнили тези документи, поемат материална отговорност, чието неизпълнение води до санкциониране или до отнемане правото да ползват услугите на библиотеката временно или за постоянно.

11. На учениците на възраст под 14 г. преди издаване на читателска карта картон се изисква декларация/съгласие от родител. На учениците над 14 г. при регистрация се изисква документ за самоличност: ученическа карта и/или лична карта. На служителите и учителите при регистрация се изисква документ за самоличност - лична карта.

12. В началото на учебната година се прочистват и пренареждат картоните според актуалните списъци на учениците. Отделят се картоните на напуснали и завършили. Пазят се всички картони с невърнати книги – до отчисление. Преглеждат се старите картони и изрядните, запълнени до край. се изпращат в архив за съхранение. Приключеният архив с картони, съдържащ лични данни на читателите, след изтичане на съответния срок на съхранение – 3 г. се унищожава по реда и процедурите на училищния архив.

8. Регистър **Сведение за организацията и дейността в учебното заведение за учебната година – „Списък-образец № 1“** е предназначен да служи за установяване на съответствието на организацията на учебния процес с нормативната уредба в системата на народната просвета. Той обслужва информационно нуждите на МОН, РУО, НИО и финансиращия орган.

Към Списък- образец №1 се прилагат:

- документи за статута на училището в случаите, в които е настъпила промяна през предшестващия период;
- прилаганите в училището учебни планове;
- утвърдените учебни програми за преподаваните предмети от раздели В и Г в професионалните училища;
- годишен план на училището;
- дневен режим на институцията.

Данните от Списък-образец № 1 се въвеждат в Национална електронна информационна система за предучилищно и училищно образование - Модул "Институции" и се съгласуват по електронен път.

Право на достъп до данните в регистъра имат:

- Лицата за които се отнасят данните в регистъра, по тяхно изрично искане;
- Директорът, главният счетоводител, ръководител на направление ИКТ, учителите и ЗАС – при изпълнение на правомощията им по Кодекса на труда и длъжностна характеристика.
- Държавни органи надлежно легитимирани се със съответни документи – писмени разпореждания на съответния орган, в които се посочва основанието, имената на лицата, на които е необходимо да се осигури достъп до личните данни.

9. Регистър **„Архив“**

В регистър „Архив“ се съхраняват лични данни:

- На работилите в учебното заведение по трудови правоотношения, на физическите лица, сключили договори с училището на различни основания, както и на други лица, предоставили доброволно личните си данни;

- На учащите се, учителите и служителите в учебното заведение;

1. Предоставените документи се съхраняват в предвидените срокове при изпълнение на нормативните изисквания на Кодекса на труда, Наредба № 8 от 11.08.2016 год, за информацията и документите за системата на предучилищното и училищното образование, Закона за задълженията и договорите, Закона за държавния архив, Номенклатурата за водене и съхранение на делата, Инструкция за документооборота и др.:

2. Събраните данни се използват за служебни цели, свързани с изготвяне на справки, издаване на документи и други статистически и исторически цели.

Формата на водене на регистъра е на хартиен носител, а след внедряване на всички електронни продукти за функциониране на НЕИСПУО, всички документи се съхраняват в електронен и хартиен формат.

3. Данните се съхраняват в писмена (документална) форма и се класират в архивни дела, съответстващи на въведената инструкция за архивиране (деловодна обработка).

4. Делата се подреждат на специални рафове, които са разположени в изолирано помещение със защитна сигнализация.

5. Длъжностните лица предприемат всички организационни мерки за съхраняването и опазването на делата, в това число изолиране на достъпа до тях на външни лица и служители.

6. Делата не се изнасят извън сградата на администратора.

На технически носител: Личните данни се въвеждат в специализирана Информационна система за училищна администрация АдминПро. Базата данни се намира на твърдия диск на изолирани компютри.

Срок на съхранение: съгласно Номенклатурата на делата във ФСГ „Васил Левски“ с определени срокове за съхранение.

10. Регистър за достъп до лични данни

Регистърът представлява книга (тетрадка), в която се номерират и заверяват с подпис и печат отделните страници.

В Регистър за достъп до личните данни има:

а) Графа „Номер и дата“ - заявлението се завежда със съответния номер в зависимост от поредността на неговото постъпване при администратора и датата, на която става това. Всяко заявление се вписва с изходящ номер (започва се от едно, две и т. н., без да се пропускат числа) и дата на извеждането му.

б) Графа „Име и подпис на заявителя“ - имена на подателя на заявлението, който лично полага подпис, за да удостовери това. В Графата има две колони – в първата се изписва името на заявителя, а във втората - той полага своя подпис.

в) Графа „Уведомление“ - посочва се датата на уведомяването и се удостоверява фактът на връчването на информацията. В графата има две колони - в първата колона се вписва датата, на която лицето трябва лично да получи информацията, и лицето се подписва. Във втората колона лицето, получило вече уведомлението и информацията, се подписва и се вписва датата (номера на обратната пощенска разписка).

г) Графа „Отказ“ - посочва се датата на неговото връчване и се удостоверява фактът на самото връчване. В графата има две колони - в първата колона се вписва датата, на която лицето трябва лично да получи информацията и лицето се подписва. Във втората колона лицето, получило вече отказа, се подписва и се вписва датата (номера на обратната пощенска разписка).

Чл.24 (1) В регистър „Родители“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица – родители, настойници и други. Нормативното основание е ЗПУО и приложимото законодателство, свързано с предоставянето на образователни услуги.

При публикуване на снимки на уебсайта и аучилището на деца под 14-год. възраст, следва да бъде получено съгласие от родител или настойник.

(2) Общо описание на регистър „Родители“.

Регистърът съдържа следните групи данни:

- физическата идентичност – име, ЕГН, адрес, телефони за връзка, електронна поща и месторабота;
- икономическа идентичност – финансово състояние;
- социална идентичност – образование, трудова дейност;
- семейна идентичност – семейно положение и родствени връзки.

(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, като са разположени в изолирани заключващи се помещения на операторите на лични данни, снабдени със защитна сигнализация. Информацията от хартиените носители се записва в Книга за подлежащите на задължително обучение деца до 16-годишна възраст: Дневник за VIII - XII клас със задължителни реквизити, които се съхраняват в същите изолирани помещения.

На технически носител: Личните данни се въвеждат в специализирана информационна система за училищна администрация Админ Про. Базата данни се намира на твърдия диск на изолирани компютри,

- срок на съхранение: съгласно Номенклатурата на делата в училището с определени срокове на съхранение.

Информацията се подава и в Националната електронна информационна система за предучилищно и училищно образование, Модул „Характеристики на средата“. В този модул се попълва информацията от работната карта за набиране на информация за образователното ниво и трудовата заетост на членовете на семействата на децата и учениците.

(4) **Определяне на длъжностите:** Обработващи лични данни на регистър „Родители“ са: заместник-директор, класните ръководители, ръководител на направление „ИКТ“ и ЗАС на училището. Оператор на лични данни на регистър „Родители“ е целият педагогически персонал. Длъжностните лица, обработващи лични данни и оператори на 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) Достъп до регистър „Родители“ имат и държавните органи – МОН, РУО, дирекция „Социално подпомагане“ за изпълнение на техните задължения, предвидени в съответните закони и подзаконовни нормативни актове.

Достъп до обработваните лични данни имат и съответните държавни органи – съд, следствие,

прокуратура, ревизиращи органи и др., когато са изискали данните по надлежен ред във връзка с изпълнението на техните правомощия.

(7) 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 училището.

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

Чл. 25 (1) В регистър „Персонал“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица, назначени по трудово правоотношение и/или по граждански договори. 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.

(2) 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, повишаване на квалификацията и др.
4. Установяване на връзка с лицето по телефон, електронна поща, адрес по местоживееене за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудово правоотношение и по граждански договори.
5. Данните в регистъра на хартиен носител се събират, обработват и съхраняват от ЗАС, а данните в регистъра на хартиен и технически носител се обработват и съхраняват от касиер-домакина и главния счетоводител.

6. Личните данни в регистър „Персонал“ се набират при подаване на документи за постъпване на работа по трудово правоотношение,

(3) Регистърът съдържа следните групи данни:

1. физическата идентичност – име, презиме, фамилия, ЕГН, адрес, паспортни данни, месторождение, телефони за връзка, електронна поща и банкови сметки;
2. психологическа идентичност – документи относно психическото здраве, съгласно Наредба № 4 от 24 октомври 2016 г. за определяне заболяванията и отклоненията, които застрашават живота и здравето на децата и учениците;
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 са: Кодексът на труда, Кодексът за социалното осигуряване, Законът за счетоводството, Законът за данъците върху доходите на физическите лица, Наредба № 12 за статута на педагогическите специалисти ... и приложимото законодателство в областта на трудовото право.

Данните се предоставят лично от лицето на основание нормативно задължение.

(4) Източниците, от които се събират данните, са: от физическите лица, за които се отнасят, от публични регистри, както и от външни източници (от съдебни, финансови, осигурителни,

данъчни и други институции в изпълнение на нормативни изисквания).

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

1. поверителност – средно ниво;
2. цялостност – средно ниво;
3. наличност – средно ниво;
4. общо за регистъра – средно ниво.

(6) Технологично описание на регистър „Персонал“

носител на данни:

На хартиен носител: Данните се набират в писмена (документална) форма и се съхраняват в папки (трудова досиета). Папките се подреждат в шкафове, които са разположени в канцеларията – помещение на оператор на лични данни, снабдено със защитна сигнализация.

На технически носител: Личните данни се въвеждат в специализирана счетоводна програма. Базата данни се намира на твърдия диск на изолирани компютри.

Срок на съхранение: съгласно Номенклатурата на делата в училището със срокове на съхранение;

(7) Определяне на длъжностите:

Обработващи лични данни на регистър „Персонал“ са: ЗАС на училището,

Оператор на лични данни на регистър „Персонал“ са счетоводителят, касиерът и ЗАС.

- 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,

(8) Достъп до регистър „Персонал“ имат – НАП, НОИ, Инспекция по труда, служби по трудова медицина, синдикати, застрахователни и осигурителни дружества, здравни заведения, МОН, РУО и др. за изпълнение на техните задължения, предвидени в съответните законови и подзаконовни нормативни актове. Достъп до обработваните лични данни имат и съответните държавни органи – съд, следствие, прокуратура, ревизиращи органи и др., 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 училището.

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

Чл. 25 Регистър „Трудови злополуки“. Администраторът е длъжен да води книга за регистриране на актовете за трудова злополука.

Регистърът съдържа следните данни:

- Номер и дата на декларацията;
- Входящи номера на декларацията в НАП;
- Трите имена на пострадалия и ЕГН;
- Място и време на злополуката;
- Номер и дата на разпореждането на НАП за приемането или неприемането на злополуката;

- Последници от злополука.

Носители на данни:

На хартиен носител: Данните се набират в писмена (документална) форма и се съхраняват в папки (трудова досиета).

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.

Регистърът на трудовите злополуки се съхранява в кабинета на ЗАС.

Достъп до данните на лицето, претърпяло трудова злополука имат: счетоводителят и директорът,

Чл. 26 (1) Регистър „**Заплати и хонорари**“ съдържа следните данни – име, ЕГН, номер на лична карта, адрес, банкова сметка, данъчна служба по местоживееене, месечен доход.

При изготвяне на ведомости за заплати или щатно разписание на персонала, се използва програмен продукт „Кодар“, личните данни се въвеждат на твърдия 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. Обработващи лични данни на регистър „Заплати и хонорари“ са: счетоводителя и касиера на училището.

Срок на съхранение: съгласно Номенклатурата на делата в училището със срокове на съхранение.

(2) При внедряване на нов програмен продукт за обработване на лични данни се съставя нарочна комисия по тестване и проверка възможностите на продукта с оглед спазване изискванията па Закона за защита на личните данни и осигуряване максималната им защита от неправилен достъп, загубване, повреждане или унищожаване.

Чл. 27. Регистър „Деловодство“ - Организация и ред за деловодно обработване

(1) Всички постъпили документи – писма от РУО, МОН, Община и др. институции, молби, жалби, сигнали, предложения, запитвания, постъпили в училище по пощата и/или по електронната поща се регистрират в деловодната система на училището от ЗАС.

(2) В деловодната система на ФСГ „Васил Левски“ се въвежда информацията относно: кореспондента, кореспондентски индекс и дата; описание на съдържанието на документа, адресат, тип на документа, регистрационен индекс и дата (даден от системата).

(3) На всяко от исканията се поставя самостоятелен регистрационен индекс и се образува самостоятелна преписка. При регистрация на документи, но които има вече образувана преписка, се записва регистрационният индекс на първоначалната преписка и датата на регистриране на новообразуваната преписка.

Чл. 28. (1) След регистрацията, документите се предават в оригинал на директора на училището в деня на постъпването им или най-късно до 12:00 часа на следващия работен ден. Предаването и приемането на регистрираните документи се удостоверява с подпис на длъжностните лица, като се посочва датата и часа на получаване.

(2) Оригиналите на резолираните от директора искания се съхраняват в деловодството, като в деловодната система се въвеждат:

1. резолюцията на директора ;
2. текст на резолюцията;

3, адресат на резолюцията;

4, срок за изпълнение, ако е определен такъв.

(3) Копие от резолюцията от директора документ се предава на посоченият в него изпълнител в деня на резолюцията или най-късно до 12:00 часа на следващия работен ден.

(4) Посочените в резолюцията изпълнители приемат срещу подпис и дата само документи, които предварително са регистрирани в деловодната система.

(5) Документи, по които трябва да работят повече изпълнители, ако това е указано с резолюцията или в самия документ, се размножават в необходимия брой екземпляри от деловодството и се предават за изпълнение едновременно. Първият изпълнител, посочен в резолюцията, е отговорен за обобщаването и изготвянето на изходящия документ при строго съблюдаване на защита на личните данни, ако се предоставят такива.

Чл. 29. (1) Всички изходящи документи се съставят задължително върху бланка на училището съобразно регламентираният срок и в съответствие с Правилата за организацията на документооборота и деловодната дейност.

(2) Един екземпляр от изходящия документ (със съгласувателните подписи), заедно с приложенията към него се оставя за съхранение в деловодството и се класира към съответната преписка.

Чл. 30. За всички нерегламентирани с настоящите правила въпроси относно реда и организацията на деловодната обработка се прилагат разпоредбите на Правилата за организацията на документооборота и деловодната дейност в училището. Право на достъп до данните в регистър „Деловодство“ имат:

- ❖ Лицата, за които се отнасят данните в регистъра, по тяхно изрично искане;
- ❖ Директорът, заместник-директорът, счетоводителят и ЗАС на училището при изпълнение на правомощията им по Кодекса на труда и др.
- ❖ Обработващите и операторите на лични данни – ЗАС на училището;
- ❖ Данните от регистъра не се предават на трети лица;
- ❖ Физическата защита на личните данни от регистъра е организирана, като данните се обработват и съхраняват в заключващи се помещения и строг контрол на достъпа до тях.

Чл. 31. (1) В регистър „Видеонаблюдение“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица, съгласно Закона за частната охранителна дейност. Записите с видеозаписи се съхраняват на отделни устройства (DVR), монтирани в дирекцията.

(2) Данните в регистъра се предоставят доброволно от лицата при влизането им в сградата на ФСГ „Васил Левски“. На входовете на сградата и в сградата са поставени предупредителни табели, че обектът се намира под постоянно видеонаблюдение. Данните от този регистър се съхраняват до 30 дни.

(3) Физическата защита на личните данни се осъществява от директора.

(4) Общо описание на регистър „Видеонаблюдение“: Категориите физически лица, за които се обработват лични данни, са посетители, ученици, преподаватели и служители в сградите на гимназията.

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

(5) Технологично описание на регистър „Видеонаблюдение“:

Регистърът се попълва с данни от автоматично денонощно видеонаблюдение (видеозапис) за движението на служителите, учениците и посетителите в сградата на училището.

(6) Определяне на длъжностите:

Оператори на лични данни на регистър „Видеонаблюдение“ са: директор и зам.-директор УД.

(7) 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.

(8) 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.

(9) 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.

(10) Лични данни се съхраняват в паметта на дивира за срок от 30 дни. При необходимост записи те могат да бъдат свалени на външен носител.

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

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

(13) На входовете на сградата и по коридорите се поставят информационни табели за уведомяване на гражданите, че при влизане и излизане от сградата подлежат на проверка съгласно чл. 30, ал. 131. 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.

(14) Право на достъп до данните в регистър „Видеонаблюдение“ имат:

1. Лицата, за които се отнасят данните в регистъра по тяхно изрично искане;
2. Директорът, заместник-директорът, педагогическият съветник - при изпълнение на правомощията им длъжностна характеристика;
3. Длъжностното лице, което поддържа регистър „Видеонаблюдение“ трябва да следи за изправността на използваната апаратура;
4. Обработващите и операторите на лични данни;
5. Държавни органи, надлежно легитимирани се със съответни документи – писмени разпореждания на съответния орган, в които се посочва основанието, имената на лицата, на които е необходимо да се осигури достъп до личните данни.
 - Данните от регистъра не могат да бъдат предавани по електронен път.
 - Длъжностното лице, което поддържа регистър „Видеонаблюдение“ трябва да следи за изправността на ползваната апаратура.
 - Защитата на регистъра се осъществява посредством помещения с контролиран достъп, които са защитени от случайно проникване в тях.

Чл. 32. Регистър „Пропускателен режим – Външни посетители“ съдържа трите имена на посетителите на училището.

(1) Данните се набират в писмена форма в дневник, с цел индивидуализиране на физически лица, съгласно Закона за частната охранителна дейност.

(2) Определяне на длъжностите:

Обработващ лични данни на регистър „Пропускателен режим“ е охрана/хигиенисти.

Оператор на лични данни на регистър „Пропускателен. Режим“ е зам.-директорът.

(3) Категориите физически лица, за които се обработват лични данни, са посетителите в сградата на училището.

(4) Регистърът съдържа следните групи данни: физическата идентичност на лицето: имена, номер на лична карта, дата и място на издаване, ЕГН (първите 6 цифри), местоживеене, адрес и др.

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

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

(7) 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.

(8) На входовете на сградата се поставят информационни табла за уведомяване на гражданите, че при влизане и излизане от сградата подлежат на проверка съгласно чл. 30, ал. 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.

(9) Данните, съхранявани в регистър „Посетители“ се предоставят на :

- Физически лица, за които се отнасят даните;
- на лица, ако е предвидено в нормативен акт;
- на лица, обработващи личните данни.

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

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

След приключване на дневника, същият се унищожава физически, чрез изгаряне или нарязване.

Чл. 33. (1) В регистър „**Контрагенти и партньори**“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица и персонализиране на юридическите лица, фирми, имащи партньорски взаимоотношения с училището. Нормативното основание е Законът за задълженията и договорите. Законът за обществените поръчки и други приложими закони.

(2) Регистърът съдържа следните групи данни:

1. физическата идентичност на лицето: имена, номер на лична карта, дата и място на издаване, ЕГН, месторождение, адрес, електронна поща, телефони за връзка и др.

2. обрачолалие: вил на образованието, място, номер тт дата на издаване на дипломата - данните си необходими съгласно действащото законодателство та доказване на наличие на квалификация по търгове и други специфични взаимоотношения. Предоставят се от лицата на основание нормативно задължение във всички слу чай, когато е необходимо.

(3) 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.

(4) Източниците, от които се събират данните, са; от физическите и или юридическите лица, за които се отнасят, от публични регистри, от интернет.

(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.

Чл.34 „Счетоводни регистри“

(1) Счетоводната отчетност на ФСГ „Васил Левски“ се осъществява при спазване на задължителните основни принципи, определени в чл. 4, ал. 1 от Закона за счетоводството.

(2) Форма на счетоводство

1. Във ФСГ „Васил Левски“ се прилага двустранно счетоводно записване, като счетоводната информация се обработва автоматизирано с програмен продукт „СКИПТЪР“. Счетоводните регистри за аналитично и синтетично отчитане се съставят под формата на постоянни информационни масиви.

2. Регистрите се приключват в края на всеки месец и задължително към 31 декември на отчетния период.

3. За да се осъществи контрол върху правилността на систематичните (синтетични и аналитични) записвания по счетоводни регистри, се съставя оборотна ведомост.

4. В края на всеки отчетен период се извършва контрол за взаимовръзка и равнение на приходите и разходите на начислена и касова основа.

5. Счетоводните документи в училището се дешифрират като хартиени и магнитни носители на счетоводна информация за регистриране на стопанските операции.

6. Счетоводните документи, съобразно съдържанието се в тях информация, се класифицират като първични, вторични и регистри. Формата (образецът) на счетоводните документи, план-графикът на документооборота и съхранението на счетоводните документи са регламентирани с „Правилник за документооборота“.

(3) .Обработващи лични данни на регистър „Счетоводство“ са: счетоводителят и касиерът на училището.

(4) .Срок на съхранение: съгласно Номенклатурата на делата в училището със срокове на съхранение.

(5) .Данните, съхранявани в регистър „Счетоводство“ се предоставят на :

- физически лица, за които се отнасят данните;
- на лица, ако е предвидено в нормативен акт;
- на лица, обработващи личните данни;
- на одитора.

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

След приключване на финансовата година документите се предават в архива на училището.

(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.

Чл. 34а. (1) В регистър „ДАРЕНИЯ“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица и персонализиране на юридическите лица, фирми, извършили общи или целеви дарения на училището. Нормативното основание е Закон за задълженията и договорите, Наредба № 8/11.08.2016 г. за информацията и документите за системата на предучилищното и училищното образование и други приложими закони.

(2) Регистърът съдържа следните групи данни:

1. идентификация на дарителя – физическо или юридическо лице, вид и стойност на дарението.

(3) 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.

(4) Източниците, от които се събират данните, са: от физическите и/или юридическите лица, за които се отнасят.

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

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

Чл. 35. Периодично архивиране

(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 помещения, определени за архив, за срокове, съобразени с действащото законодателство. Помещенията, определени за архив, са оборудвани с пожарогасители и задължително се заключват.

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

(4) Документите на електронен носител се съхраняват на специализирани компютърни системи и/или външни носители на информация. Архивиране на личните данни на технически носител се извършва периодично от обработващия/оператора на лични данни с оглед запазване на информацията за съответните лица в актуален вид и възможността ѝ 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.

Чл. 36. С оглед защита на хартиените, техническите и информационните ресурси всички служители са длъжни да спазват правилата за противопожарна безопасност.

Чл. 37. (1) Оторизирани служители трябва да извършват периодични проверки за състоянието и целостта на личните данни, съдържащи се в обработваните от училището регистри и изготвят съответни доклади не по-малко от веднъж годишно.

(2) Тези доклади трябва да включват преценка на необходимостта за обработка на личните данни и унищожаване или прехвърляне на личните данни съгласно чл. 25 от Закона за защита на личните данни.

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

съдържащи данни, се унищожават чрез нарязване.

(4) Унищожаването се осъществява от служители, упълномощени с изричен писмен акт на директора на училището.

(5) Контролът върху дейностите по обработка на лични данни и правилното им архивиране се осъществява да от зам.-директора.

Актуализации на лични данни

Чл. 38. (1) Актуализация на лични данни представлява допълнение или изменение на съществуваща информация в гимназията.

Актуализация на лични данни се извършва:

1. по искане на лицето, за което се отнасят личните данни, когато то е установило, че е налице грешка или непълнота в тях, и удостовери това с документ;

2. по инициатива на обработващия лични данни – при наличие на документ, даващ основание за актуализация;

3. при установена грешка при обработката на личните данни от страна на администратора.

4. При актуализация на лични данни в досието на съответното лице се отразяват регистрационния номер на документа, източник на данните за актуализацията, дата на актуализацията. Актуализацията се извършва от лицето, обработващо личните данни.

ГЛАВА ШЕСТА Достъп до лични данни

Осигуряване на достъп на лицата до лични данни

Чл. 39. (1). Всяко физическо лице, както и служителите във ФСГ „Васил Левски“ има право на достъп до отнасящите се до него лични данни, обработвани от администратора.

(2) В случаите, когато при осъществяване правото на достъп на физическото лице могат да се разкрият лични данни и за трето лице, администраторът предоставя на съответното физическо лице достъп само за частта от данните, отнасяща се за него.

(3) При упражняване на правото си на достъп физическото лице има право по всяко време да поиска от администратора на лични данни:

1. потвърждение за това, дали отнасящи се до него данни се обработват, информация за целите на това обработване, за категориите данни и за получателите или категориите получатели, на които данните се разкриват;

2. съобщение до него в разбираема форма, съдържащо личните му данни, които се обработват, както и всяка налична информация за техния източник.

(4) При смърт на физическото лице право на достъп до личните му данни имат неговите наследници.

Чл.40. (1) Правото на достъп се осъществява с писмена молба до администратора на лични данни.

(2) Молбата може да бъде отправена и по електронен път по реда на Закона за електронния документ и електронния подпис.

(3) Молбата по ал. 1 се отправя лично от физическото лице или от изрично упълномощено от него лице чрез нотариално заверено пълномощно.

Чл. 41. (1) Молбата по чл. 40 съдържа:

1. трите имена, ЕГН/ЛНЧ/, адрес за контакт и телефон на заявителя;
2. описание на искането;

3. предпочитана форма за предоставяне на достъп до личните данни;
4. подпис, дата на подаване на заявлението и адрес за кореспонденция.

(2) При подаване на молба от упълномощено лице към същото се прилага и нотариално завереното пълномощно.

(3) При приемане на молбата, техническо лице извършва регистрацията на същата в деловодната система на администратора.

Чл. 42. (1) Физическото лице може да поиска копие на обработваните лични данни на предпочитан носител или предоставянето им по електронен път, освен в случаите, когато това е забранено от закон.

(2) Администраторът на лични данни е длъжен да се съобрази с предпочитаната от молителя форма на предоставяне на информацията по чл. 41, ал. 1, т. 3.

(3) Администраторът на лични данни предоставя исканата информация във форма, различна от заявената, когато:

1. за исканата форма няма техническа възможност;
2. исканата форма е свързана с необосновано увеличаване на разходите по предоставянето.

Чл. 43. (1) Администраторът на лични данни или изрично оправомощено от него лице разглежда молбата по чл. 41 и се произнася в 14-дневен срок от неговото постъпване.

(2) Срокът по ал. 1 може да бъде удължен от администратора до 30 дни в случаите, когато обективно се изисква по-дълъг срок за събирането на всички искани данни и това сериозно затруднява дейността на администратора.

(3) С решението си администраторът предоставя пълна или частична информация на заявителя или мотивирано отказва предоставянето ѝ.

Чл. 44. Право на достъп до данните в поддържаните от администратора регистри на лични данни имат служителите във ФСГ „Васил Левски“ – администратори на базите данни, служителите на които е възложено приемането и обработването на лични данни върху хартиен и електронен носител (обработващите лични данни), както и служителите, за които служебните им функции налагат такъв достъп.

Чл. 45. Служителите във ФСГ „Васил Левски“ – с оторизиран достъп до лични данни са длъжни да обработват същите законосъобразно и добросъвестно, съобразно целите, за които се събират и да не ги обработват допълнително по начин, несъвместим с тези цели, както и да ги поддържат във вид, който им позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които се обработват.

Достъп на трети лица до регистрите съдържащи лични данни

Чл. 46 (1) Достъп до обработваните от администратора лични данни имат лицата, за които същия произтича от законово или договорно основание, както и органи на надзора или на съдебната власт (Комисия за финансов надзор, съд, прокуратура, следствени органи и др.). Достъпът на тези органи до личните данни на лицата е правомерен.

(2) Не се изисква съгласие на лицето, ако обработването на неговите лични данни се извършва само от или под контрола на компетентен държавен орган за лични данни, свързани с извършване на престъпления, на административни нарушения и на непозволени увреждания. На такива лица се осигурява достъп до личните данни, като при необходимост им се осигуряват съответни условия за работа в помещение на училището.

(3) Правомерен е и достъпът на ревизиращите държавни органи, надлежно легитимирани се със съответни документи – писмени разпореждания на съответния орган, в които се посочва основанието, имената на лицата, като за целите на дейността им е необходимо да им се осигури достъп до кадровите досиета на персонала или клиентите.

(4) Решението си за предоставяне или отказване достъп до лични данни за съответното лице администраторът съобщава на третите лица в 30-дневен срок от подаване на молбата, респ. искането.

ГЛАВА СЕДМА Видове защита на лични данни

Лицата по защита на личните данни

Чл. 47. (1) За обезпечаване на адекватна защита на регистрите с лични данни администраторът определя лице/лица по защита на личните данни.

(2) Лицето/лицата по защита на личните данни има следните правомощия:

1. осигурява организация по водене на регистрите и мерки за гарантиране на адекватна защита;

2. следи за спазването на конкретните мерки за защита и контрол на достъпа съобразно спецификата на водените регистри;

3. осъществява контрол по спазване на изискванията по защита на регистрите;

4. специфицира техническите ресурси, прилагани за обработване на личните данни;

5. подпомага установяването на обстоятелства, свързани с нарушаване на защитата на регистрите;

6. в случай на установяване на нарушение на сигурността на личните данни, лицето по защита на личните данни уведомява в спешен порядък администратора на лични данни. Настъпилото събитие поражда задължение за администратора на лични данни в рамките на 72 часа от установяване на нарушението незабавно да уведоми КЗЛД за нарушаване сигурността на личните данни в училище.

7. поддържа връзка с Комисията за защита на личните данни (КЗЛД) относно предприетите мерки и средства за защита на регистрите;

8. контролира спазването на правата на потребителите във връзка с регистрите и програмно-техническите ресурси за тяхната обработка;

9. периодично информира персонала по въпросите на защитата на личните данни.

10. следи за спазване на организационните процедури за обработване на личните данни и провежда периодичен контрол за спазване на изискванията по защита на данните и при открити нередности взема мерки за тяхното отстраняване.

Чл. 48. (1) Всяко лице, желаещо да внесе документ съдържащ лични данни предоставя същия в деловодството на ФСГ „Васил Левски“. Лицето приемащо документа е задължено да запознае вносителя на документите с правата му на субект на лични данни, както и с Вътрешните правила за тяхната обработка. Преди приемането му вносителят попълва съответна Декларация по образец, предоставена му от лицето приемащо документите за деклариране на предоставените лични данни и основанието, на което те се предоставят и ще се ползват. Лицето, приемащо документите има право да изиска от субекта на лични данни документа, доказващ истинността на предоставените лични данни, а при наличие на предвидена в закона възможност, да снима копие от този документ и да го приложи към декларацията.

(2) Внесените документи с лични данни се докладват на Директора, който ги разпределя на лицата обработващи съответните лични данни.

(3) Лицата, обработващи личните данни са задължени да предоставят личните данни в съответствие с разпореждането на Директора на Администратора,

(4) Лични данни се предоставят на трети лица само чрез Директора на Администратора.

(5) При предоставяне на личните данни за ползване от трети лица, те попълват

декларация за задължението си да обработват личните данни съгласно Регламент 2016/679 и ЗЗЛД.

ГЛАВА ОСМА Процедури за докладване и управление при инциденти

Чл.49.(1) При възникване и установяване на инцидент и/или нерегламентиран достъп, свързан с нарушаване защитата или загуба на лични данни, незабавно се докладва на лицето по защита на личните данни във ФСГ „Васил Левски“.

За инцидентите се води регистър, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада.

(2) След анализ от лицето по защита на личните данни, в регистъра се записват последствията от инцидента и мерките, които са предприети за отстраняването им.

(3) В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на лицето по защита на личните данни, като това се отразява в регистър по архивиране и възстановяване на данни.

(4) В случаите на компрометиране на парола, тя се подменя с нова, като събитието се отбелязва в регистъра.

Действия за защита при аварии, произшествия и бедствия

Чл. 50. Училището 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 Училището - 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 се действия по ограничаване на разпространението, както и да се изпомпва вода или загребва със собствени подръчни средства.

ОТГОВОРНОСТ

Чл. 51. За неизпълнение на задълженията, вменени на съответните оправомощени лица по тези Правила, по ЗЗЛД и по Регламент (ЕС) 2016/679, се налагат дисциплинарни наказания по КТ, а когато неизпълнението на съответното задължение е констатирано и установено от надлежен орган – предвиденото в ЗЗЛД административно наказание по Наказателния кодекс, ако такава отговорност се предвижда по закон.

Чл. 52. (1) За вреди, причинени в резултат на незаконосъобразно обработване на лични данни от служители във ФСГ „Васил Левски“, засегнатите лица могат да търсят отговорност от виновните лица по реда на общото гражданско законодателство или наказателна отговорност, ако извършеното представлява престъпление.

(2) Ако в резултат на незаконосъобразно обработване на лични данни, включително незаконното им разкриване или разпространение, са причинени щети на администратора на лични данни на виновните лица се търси имуществена отговорност по Кодекса на труда.

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 ФСГ „Васил Левски“ (училище).
- **„Анонимни данни“** са лични данни, приведени във форма, която не позволява те да бъдат свързани със съответното физическо лице, за което се отнасят.
- **„Високо ниво на въздействие“** е неправомерното обработване на лични данни, което би могло да доведе до възникване на значителни вреди или кражба на самоличност на голяма група физически лица или лица, заемащи висши държавни длъжности, или трайни здравословни увреждания или смърт на отделно физическо лице.
- **„Външни мрежи“** са всички мрежи, вкл. и безжични мрежи, интернет, интернет връзки, мрежови връзки с трети страни, мрежови сегменти на хостинг системи на трети страни, които не са под административния контрол на училището.
- **„Вътрешни мрежи“** са всички локални жични мрежи и/или телекомуникационни връзки тип „точка - точка“, които се намират под контрола и администрацията на училището.
- **„Група физически лица“** е съвкупност от физически лица, чийто брой надхвърля 2.
- **„Длъжностно лице“** е служител, на когото е възложено да упражнява ръководство на процес в училището, в неговите структурни и/или функционални единици, както и служител, който изпълнява работа на специалист във функционалните и обслужващите звена на училището.
- **„Документална защита на лични данни“** е система от организационни мерки при обработването на лични данни на хартиен носител.
- **„Защита на автоматизирани информационни системи и/или мрежи“** е система от технически и организационни мерки за защита от незаконни форми на обработване на личните данни.
- **„Исключително високо ниво на въздействие“** е неправомерното обработване на лични данни, което би могло да доведе до възникване на значителни вреди или кражба на самоличност на особено голяма група физически лица или трайни здравословни увреждания или смърт на група физически лица.
- **„Инцидент“** е непредвидимо обстоятелство, което би могло да засегне сигурността на личните данни.
- **„Криптографска защита на лични данни“** е система от технически и организационни мерки, които се прилагат с цел защита на личните данни от нерегламентиран достъп при предаване, разпространяване или предоставяне.
- **„Лице по защита на личните данни“** е физическо лице, притежаващо необходимата компетентност, което е упълномощено или назначено от администратора със съответен писмен акт, в който са уредени правата и задълженията му във връзка с осигуряване на необходимите технически и организационни мерки за защита на личните данни при тяхното обработване.
- **„Наличност“** е изискване за осигуряване непрекъсната възможност за обработване на личните данни на оторизираните лица и за изпълнение на функциите на системата за обработване или бързото им възстановяване.

- **„Ниво на защита“** е степен на организация на обработката на личните данни в зависимост от рисковете и вида им.
- **„Ниско ниво на въздействие“** е неправомерното обработване на лични данни, което би застрашило неприкосновеността на личността и личния живот на отделно физическо лице или група физически лица.
- **„Носител на лични данни“** е физически обект, на който могат да се запишат данни или могат да се възстановят от същия.
- **„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 физическо или юридическо лице, държавен орган или орган на местно самоуправление, който обработва лични данни от името на администратора на лични данни.
- **„Оператор на лични данни“** е всяко лице, което по указание и под ръководството на администратора има достъп до лични данни и упражнява ограничени функции по тяхната обработка съобразно нормативните актове, регламентиращи дейността на училището.
- **„Оторизирано лице“** е лице, което по силата на естеството на преките си служебни задължения и/или изричното оторизиране от Ръководството на училището, има право за достъп до определена категория 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.
- **„Персонална защита на лични данни“** е система от организационни мерки спрямо физическите лица, които обработват лични данни по указание на администратора.
- **„Поверителност“** е изискване за неразкриване на личните данни на неоторизирани лица в процеса на тяхното обработване.
- **„Получател“** е физическо или юридическо лице, орган на държавна власт или на местно самоуправление, на когото се разкриват лични данни, независимо дали е трето лице или не. Органите, които могат да получават данни в рамките на конкретно проучване, не се смятат за получатели.
- **„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.
- **„Резервни копия за възстановяване“** са копия на данните, съхранявани на носител, чрез които може да се осъществи възстановяването.
- **„Специфични признаци“** са признаци, свързани с физическа, физиологична, генетична, психическа, психологическа, икономическа, културна, социална или друга идентичност на лицето.
- **„Средно ниво на въздействие“** е неправомерното обработване на лични данни, което би могло да създаде опасност от засягане на интереси, разкриващи расов или етнически произход, политически, религиозни или философски убеждения, членство в политически

партии или организации, сдружения с религиозни, философски, политически или синдикални цели, здравословното състояние, сексуалния живот или човешкия геном на отделно физическо лице или група физически лица.

- **„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.

- **„Физическа защита на лични данни“** е система от технически и организационни мерки за предотвратяване на нерегламентиран достъп до сгради, помещения и съоръжения, в които се обработват лични данни.

- **„Цялостност“** е изискване, данните да не могат да бъдат променени/подменени по неоторизиран начин в процеса на тяхното обработване и изискване да не се дава възможност за изменение и за неразрешени манипулации на функциите по обработване на данните.

§2. Всички учители, служители и работници са длъжни срещу подпис да се запознаят с Правилата и да ги спазват.

§3. Правилата се издават на основание чл. 23, ал. 4 от Закона за защита на личните данни и чл. 6, §1, чл. 9, §2 и чл. 10 от Регламент (ЕС) 2016/679 – Общ регламент относно защита на данните GDPR.

§4. За всички неуредени в настоящите правила въпроси са приложими разпоредбите на Закона за защита на личните данни, Регламент (ЕС) 2016/679 – Общ регламент относно защита на данните GDPR, действащото приложимо законодателство на Р България и разпоредданията на Директора на образователната институция – администратор на лични данни.

§5. Настоящите правила са утвърдени със Заповед № РД-04-.../.....2022 г. на директора на ФСГ „Васил Левски“ гр. Добрич.

ДЕКЛАРАЦИЯ

От _____

(имената на лицето)

декларирам , че съм информиран/а относно следните обстоятелства:

- 1) Всички предоставени от мен в настоящата декларация данни са лични данни по смисъла на ЗЗЛД и като такива попадат *под специален режим на защита*;
- 2) По силата на ЗЗЛД имам право на достъп до тези документи, в които се съдържат моите лични данни, и *при спазване вътрешните правила на работодателя*;
- 3) По силата на ЗЗЛД имам право да искам извършване на корекция в моите лични данни и *при спазване вътрешните правила на работодателя*;
- 4) ФСГ „Васил Левски“ гр. Добрич в лицето на Директора ѝ като работодател поема задължение да обработва, използва и съхранява личните ми данни само и единствено във връзка с реализиране на правата и задълженията по трудовото правоотношение;
- 5) ФСГ „Васил Левски“ гр. Добрич в лицето на Директора ѝ като работодател поема задължение да обработва, използва и съхранява личните ми данни, като гарантира опазването им в тайна от други работници и служители или от трети лица.
- 6) ФСГ „Васил Левски“ гр. Добрич в лицето на Директора ѝ като работодател поема задължение да не предоставя личните ми данни на трети лица, освен в случаите, когато това е необходимо, за да бъдат защитени моите права и реализирани моите задължения по трудовото правоотношение (Давам съгласието си ФСГ „Васил Левски“ гр. Добрич в лицето на Директора ѝ да предоставя личните ми данни на различни институции за целите на различни дейности и други служебни нужди).
- 7) Заявявам, че *изцяло доброволно сега и за в бъдеще предоставям* личните си данни, за да бъдат използвани за реализиране на моите права по трудово правоотношение с ФСГ „Васил Левски“ гр. Добрич, разрешавам на Директора ѝ да ги предоставя на държавни органи и институции или на трети лица, за да реализира посочените по-горе мои права и при пълно спазване на ЗЗЛД.

Дата:

Декларатор:

До Директора
на ФСГ „Васил Левски“
гр. Добрич

ЗАЯВЛЕНИЕ

Относно: достъп до лични данни

От.....
(Име, презиме и фамилия)

ЕГН:....., л. к. №....., издадена на.....,
от....., адрес.....,
телефон за контакт....., е-поща.....

Моля, на основание чл. 26 и чл. 29 от Закона за защита на лични данни, да ми бъде предоставена информация относно личните ми данни, съхранявани във ФСГ „Васил Левски“ гр. Добрич.

Желая да получа исканата от мен информация в следната форма:

- преглед на информация;
- устна справка;
- писмена справка;
- копия на технически носител;
- по електронен път.

Дата:

гр. Добрич

Декларатор:

(.....)

ФИНАНСОВО-СТОПАНСКА ГИМНАЗИЯ "ВАСИЛ ЛЕВСКИ" - ДОБРИЧ

ДЕКЛАРАЦИЯ-СЪГЛАСИЕ

за доброволно предоставяне на лични данни във връзка с чл. 4, ал. 1, т. 2 от Закона за защита на личните данни (ЗЗЛД)

От ЕГН
(трите имена на родителя/настойника)
лична карта №, издадена от МВР – гр., на г.
родител на ЕГН.....
(трите имена на детето)
ученик/чка в клас на ФСГ "Васил Левски" - гр. Добрич за учебната 20...../20.....г.

ДЕКЛАРИРАМ,

че доброволно и лично предоставям и давам своето съгласие администраторът на лични данни и служителите, обработващи лични данни във ФСГ „Васил Левски” – гр. Добрич, да обработват личните ни данни, както и личните данни на сина/дъщеря ни по ЗЗЛД за служебно ползване, за осъществяване на учебно-възпитателния процес в училище, както и за изпълнение на Наредба № 8/11.08.2016 за информацията и документите за системата на предучилищното и училищното образование, както и при издаване на служебна бележка/удостоверение, копие на документ, съдържащ личните данни на сина/дъщеря ни, при направено заявление от наша страна и др.

Запознат/и съм/сме:

- че личните данни ще бъдат обработвани от тук посочения администратор на лични данни, а именно: ФСГ „Васил Левски“ и използвани от ФСГ „Васил Левски“, включително видеонаблюдение и видеозаснемане, на територията на Република България;
- че обработването ще се извършва чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване при спазване на принципите за законосъобразност, добросъвестност и прозрачност;
- че личните данни ще се съхраняват в хартиен и електронен вариант, според законите изисквания за защита на данните;
- че имам право да получа информация за съхраняваните лични данни, мои и на детето ми, по всяко време, че имам право на достъп до личните данни и че по всяко време мога да поискам тяхното коригиране;
- че имам право на възражения и жалби във връзка с обработването и съхраняването на личните данни пред Комисия за защита на личните данни, която е надзорен орган в Република България;
- с целта и средствата на обработване на личните ни данни;
- с доброволния характер на предоставянето на данните и последиците от отказа за предоставянето им;
- с получателите или категориите получатели, на които могат да бъдат разкрити данните.

Давам съгласието си личните данни на детето ми, предоставени на ФСГ „Васил Левски“, да бъдат обработени за:

- Водене на документация в гимназията;
- Предоставяне на справки към външни институции от системата на образованието (МОН, РУО, Община Добрич и др.);
- Публикуване на снимки в сайта и фейсбук страницата на гимназията.

Декларирам, че

- съм информиран/а за условията за даване на съгласие по чл.7, ал.1 от Регламент 2016/679;
- настоящото съгласие давам в резултат на свободна воля;
- уведомен/а съм, че личните данни на детето ми ще бъдат съхранявани само и единствено в срока определен по Закона за архивиране;
- ще уведомявам администратора на лични данни за всяка промяна в личните данни на детето.

Декларатор:

Данни за книгата за подлежащите на задължително обучение

1. Трите имена на на ученика/чката.....
2. ЕГН на ученика/чката
3. Месторождение (град, село, община, област).....
4. Адрес (град, село, община, област, ж.к., ул., №, бл., вх., ет., ап.)
5. Записан/а във ФСГ "Васил Левски", на20..... г. в VIII ... клас, идва от училище –, гр./с.
6. Трите имена на родителя/настойника
7. ЕГН на родителя, телефонemail
8. Адрес (град, село, община, област, ж.к., ул., №, бл., вх., ет., ап.)
9. Личен лекар, адрес/тел.

Уведомен съм, че данните ще бъдат вписани Книгата за подлежащи на задължително обучение деца и ученици до 16-годишна възраст и няма да бъдат разпространявани на трети лица.

Не съм предоставял копие от акт за раждане на ученика.

Не съм предоставял копие от лична карта.

Посочените от мен данни в настоящата декларация са сверени от длъжностното лице, което приема документите.

Декларирам, че доброволно съм предоставил и ще предоставям в бъдеще лични данни по ЗЗЛД за мен, съпругата/съпруга ми и нашето дете за осъществяване на неговото обучение, възпитание, както и във връзка с правата и задълженията на учебното заведение за изпълнение на Наредба № 8/11.08.2016 г. за информацията и документите за системата на предучилищното и училищното образование.

Декларатор: