



ОУ "КОЧО ЧЕСТЕМЕНСКИ"

Ул. „Севастопол” №28, гр. Пловдив
school@chestemenski.com
тел. 64-30-58 Директор, 64-30-52 Зам.-директор

УТВЪРДИЛ:П/

/Златка Алдженаби/

**ВЪТРЕШНИ ПРАВИЛА
ЗА РЕДА ЗА ВОДЕНЕ НА РЕГИСТРИ ПО
ЗАКОНА ЗА ЗАЩИТА НА ЛИЧНИТЕ
ДАННИ ЗА УЧЕБНАТА 2026/2027 Г. В
ОУ „КОЧО ЧЕСТЕМЕНСКИ“,
ПЛОВДИВ**

Раздел I ОБЩИ РАЗПОРЕДБИ

Чл. 1.(1) ОУ „ Кочо Честеменски“, Пловдив е юридическо лице със седалище гр. Пловдив, обл. Пловдив, община Пловдив, с основен предмет на дейност образование и образователни услуги.

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

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

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

(3) Правилата се утвърждават, допълват, изменят и отменят от Директора на ОУ „Кочо Честеменски“, Пловдив – администратор на 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.

РАЗДЕЛ II ЦЕЛИ И ОБХВАТ НА ПРАВИЛАТА

Чл. 3.Тези правила имат за цел да регламентират:

- механизмите за набиране, обработване, актуализация, съхраняване, предоставяне, трансфер и унищожаване на личните данни;
- задълженията на Администратора, лицата обработващи лични данни, длъжностното лице по защита на лични данни и тяхната отговорност при неизпълнение на тези задължения;
- необходимите технически и организационни мерки за защита на личните данни на посочените по-горе лица от неправомерно обработване (случайно или незаконно унищожаване, случайна загуба, неправомерен достъп, изменение или разпространение, както и от всички други форми на обработване на лични данни).

Чл. 4. Правилата са задължителни за всички лица имащи достъп до личните данни, обработвани за нуждите на администратора.

РАЗДЕЛ III ПРЕДНАЗНАЧЕНИЕ И ВИДОВЕ РЕГИСТРИ

Чл. 5. Поддържаните регистри в Институцията са:

- Счетоводство
- Човешки ресурси
- Трудови договори
- Видеонаблюдение
- Дарения
- Документи на неназначени служители
- Издадените дипломи за начално и основно образование
- Издадените удостоверения за завършен клас
- Издадените дубликати на удостоверения за завършен клас

- Регистър на Издадените удостоверения за завършена степен на образование
- Приети ученици
- Регистър на Издадените дубликати за завършена степен на образование
- Регистър на Издадените дубликати на документи за завършено образование
- Документи по проекти
- Архив

Целта на регистрите е набиране и съхраняване на лични данни на ОУ „ Кочо Честеменски“, Пловдив

Изпълняване целите на образователно-възпитателния процес;

- Спазване на трудовото законодателство;
- Спазване на Закона за счетоводството;

Чл. 6.(1) Всяка година Директорът издава заповед, с която определя кой да отговаря за всеки отделен регистър.

ФОРМИ НА ВОДЕНЕ НА РЕГИСТЪРА

Чл. 7.(1) Формите биват:

- **Хартиеноносител-** на хартиен носител се съхраняват всички лични данни, които изискват попълването им върху определени бланкови документи и/или формуляри, свързани с изпълнение на изисквания на действащото законодателство или пряко свързани с осъществяването на нормалната дейност на училището;
- **Технически носител/електронен вариант, НЕИСПУО/-**личните данни се съхраняват на твърд диск, на изолиран компютър;

(2)Личните данни се събират само с конкретна цел, пряко свързана с изпълнение на законовите задължения и/или нормалната дейност на училището, а начинът на тяхното съхранение се съобразява със специфичните нужди за обработка.

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

(4)Достъпа до операционната система, съдържаща файлове за обработка на лични данни, има само обработващият лични данни чрез парола за отваряне на тези файлове, както и длъжностното лице по защита на личните данни посредством делегирани му права и задължения от администратора на лични данни.

(5)Документите, съдържащи лични данни, които не подлежат на издаване към Държавен архив, и след изтичане на законовите срокове за тяхното съхранение и не са необходими за нормалното функциониране на училището, се унищожават по подходящ и сигурен начин (напр. изгаряне, електронно изтриване и други подходящи за целта методи).

(6)Документите и преписките, по които работата е приключила, се архивират.

(7) Трайното съхраняване на документи, съдържащи лични данни, се извършва на хартиен носител в помещение, определено за архив, за срокове, съобразени с действащото законодателство. Помещението, определено за архив, е оборудвано с пожарогасител и задължително се заключва като документите се съхраняват в заключващи се метални шкафове

(8)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

ГРУПИ ДАННИ В РЕГИСТЪРА

Чл. 8. (1) В зависимост от нормативното основание за събирането и предназначението им в регистрите се набират, обработва и съхраняват лични данни относно:

- физическата идентичност на лицата – имена, ЕГН, номер на документ за самоличност, дата и място на издаването му, адрес, месторождение, телефони за контакт, имейли и др;
- семейна идентичност на лицата – семейно положение, брой членове на семейството, родствени връзки и др.;

- образование – вид на образованието, място, номер и дата на издаването на дипломата, допълнителна квалификация и др.;
- трудова дейност – професионална биография, дни в осигуряване, осигурителен доход, основание за осигуряване, осигурени социални рискове, трудови договори, осигурители и други;
- медицински данни – здравен статус, медицински диагнози и заключения на медицинската експертиза на временната и трайна неработоспособност;
- други лични данни – осигурителен доход, трудови възнаграждения, парични обезщетения, статус на лицето (осъждано/неосъждано/реабилитирано) и други.

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

ЗАДЪЛЖЕНИЯ НА ЛИЦЕТО И СЛУЖИТЕЛИТЕ, ОТГОВАРЯЩИ ЗА ВОДЕНЕ И СЪХРАНЯВАНЕ НА ДАННИТЕ В РЕГИСТРИТЕ

Чл. 9.(1)Задълженията на лицето, което отговаря за водене и съхраняване на данните в регистъра (оправомощеното лице) включват набиране, обработване, актуализация и съхраняване на лични данни.Негова е отговорността да информира и съветва администратора или обработващия лични данни и служителите, които извършват обработване, за техните задължения по силата на Общия регламент за защита на данните и на други разпоредби за защитата на данни на равнище Съюз или национално законодателство;

(2)Служителите на училището имат следните отговорности:

- да обработват лични данни законосъобразно, добросъвестно и прозрачно;
- 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;
- при необходимост да актуализират регистрите на личните данни;

- да заличават или коригират личните данни, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;
- да поддържат личните данни във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват;
- да не разгласяват лични данни, до които са получили достъп при и по повод изпълнение на задълженията си;
- незабавно да уведомяват администратора на лични данни в случай, че установят изтичане на лични данни, независимо дали при извършване на своята работа или при друго лице, което обработва лични данни.

(3) За неспазването на разпоредбите на Настоящите вътрешни правила служителите носят административна отговорност.

ПЕРИОДИЧНО АРХИВИРАНЕ

Чл. 10. Архивиране на личните данни на технически носител се извършва периодично на всяка 1 година от обработващия лични данни с оглед запазване на информацията за съответните лица в актуален вид.

КОНТРОЛ ПРИ ОБРАБОТВАНЕ НА ЛИЧНИТЕ ДАННИ

Чл. 11. Контролът върху дейностите по обработка на лични данни се осъществява от Директора на образователната институция - администратор на лични данни.

АКТУАЛИЗАЦИЯ НА ЛИЧНИ ДАННИ

Чл. 12. (1) Актуализация на лични данни представлява допълнение или изменение на съществуваща информация в дружеството. Актуализация на лични данни се извършва:

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

- при установена грешка при обработката на личните данни от страна на обработващия лични данни;

(2) 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.

РАЗДЕЛ IV

ДОСТЪП ДО ЛИЧНИ ДАННИ ОСИГУРЯВАНЕ НА ДОСТЪП НА ЛИЦАТА ДО ЛИЧНИТЕ ИМ ДАННИ

Чл. 13. (1) Всяко физическо лице, както и служителите в ОУ „ Кочо Честеменски“, Пловдив 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 него.

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

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

(5) Достъп на лица до лични данни се предоставя единствено, ако те имат право на такъв достъп, съгласно действащото законодателство, след подаване на молба в администрацията на училището.

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

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

Чл. 14.(1) Молбата по чл. 12 съдържа:

- трите имена, ЕГН/ЛНЧ/, адрес за контакт и телефон на заявителя;
- описание на искането;
- предпочитана форма за предоставяне на достъп до личните данни;
- 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) Директорът или администраторът разглеждат заявлението за достъп и се произнасят по него в 14-дневен срок.
- (4) 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.
- (5) Директорът или администраторът вземат решение за предоставянето на пълен или частичен достъп на заявителя или мотивират отказ за предоставяне на достъп.
- (6) Директорът или администраторът писмено уведомяват заявителя за решението си. Уведомяването е лично срещу подпис или по пощата с обратна разписка.

Чл. 15. Право на достъп до данните в поддържаните от администратора регистри на лични данни имат служителите в ОУ „ Кочо Честеменски“, Пловдив; 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. 16. Служителите в ОУ „ Кочо Честеменски“, Пловдив 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.

РАЗДЕЛ V ЛИЦАТА ПО ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 17. (1) За обезпечаване на адекватна защита на регистрите с лични данни администраторът може да определи лице/лица по защита на личните данни.

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

- осигурява организация по водене на регистрите и мерки за гарантиране на адекватна защита;
- следи за спазването на конкретните мерки за защита и контрол на достъпа съобразно спецификата на водените регистри;
- осъществява контрол по спазване на изискванията по защита на регистрите;
- 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 ОУ „Кочо Честеменски“, Пловдив .
- поддържа връзка с Комисията за защита на личните данни (КЗЛД) относно предприетите мерки и средства за защита на регистрите;
- контролира спазването на правата на потребителите във връзка с регистрите и програмнотехническите ресурси за тяхната обработка;
- периодично информира персонала по въпросите на защитата на личните данни;
- 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. 18. (1) С цел недопускането на неправомерен достъп, както и всички други незаконни форми на обработване на личните данни, администраторът организира и предприема мерки, съобразени със съвременните технологични постижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

(2) Видове защита:

- Физическа защита на личните данни представлява система от технически и организационни мерки за предотвратяване на нерегламентиран достъп до сгради, помещения и съоръжения, в които се обработват лични данни.
- Персонална защита представлява система от организационни мерки спрямо физическите лица, които обработват лични данни по указание на администратора.
- Документална защита представлява система от организационни мерки при обработването на лични данни на хартиен носител.
- Защита на автоматизираните информационни системи и/или мрежи представлява система от технически и организационни мерки за защита от незаконни форми на обработване на личните данни.
- Псевдонимизация чрез употребата на технически и организационни мерки

МЕРКИ ПО ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 19. (1) В училището включва набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп до системите и/или мрежите, в които се създават, обработват и съхраняват лични данни.

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

- Идентификация чрез използване на пароли за лицата, които имат достъп до мрежата и ресурсите на училището. Прилагането на тази мярка е с цел да се регламентират нива на достъп, съобразен с принципа „Необходимост да знае”;

- 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;
- Защитата от вируси, включва използването на стандартни конфигурации за всяка компютърна и/или мрежова платформа, като системният, а при възможност и приложният, софтуер се контролира, инсталира и поддържа от ръководител направление ИКТ.
- Политиката по създаване и поддържане на резервни копия за възстановяване има за цел предотвратяване на загуба на информация, свързана с лични данни, която би затруднила нормалното функциониране на училището.
- Основни електронни носители на информация са: вътрешни твърди дискове, еднократно и/или многократно презаписваеми външни носители (външни твърди дискове, многократно презаписваеми карти, памети ленти и други носители на информация, еднократно записваеми носители и др.)
- Персоналната защита на данните е част от цялостната охрана на училището.
- Личните данни в електронен вид се съхраняват съгласно нормативно определените срокове и съобразно спецификата и нуждите на училището.
- Данните, които вече не са необходими за целите на училището и чиито срок за съхранение е изтекъл, се унищожават чрез приложим способ (напр. чрез нарязване с шредер, постоянно заличаване от електронните средства).
- Предотвратяване на неоторизирано четене, копиране, промяна или изтриване на лични данни при трансфер на лични данни или превозване на носители на данни – контрол при транспортиране;

(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).

РАЗДЕЛ VI

ПРОЦЕДУРИ ЗА ДОКЛАДВАНЕ ПРИ ИНЦИДЕНТИ

Чл. 20. (1) При възникване и установяване на инцидент и/или нерегламентиран достъп, свързан с нарушаване защитата или загуба на лични данни, незабавно се докладва на Директора на образователната институция - администратор на лични данни;

(2) 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.

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

(4) 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.

(5) В случаите на компрометиране на парола, тя се подменя с нова, като събитието се отразява в регистъра за инциденти.

Чл. 21. (1) Всеки служител, който отговаря за обработването на личните данни носи отговорност 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 българското законодателство, а когато неизпълнението на съответното задължение е констатирано и установено от надлежен орган – предвиденото в ЗЗЛД административно наказание, ако такава отговорност се предвижда по закон.

Чл. 22. (1) За вреди, причинени в резултат на незаконосъобразно обработване на лични данни от служители в ОУ „Кочо Честеменски“, Пловдив ;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 или Закона за държавния служител.

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

1. Всички педагогически специалисти и служители в ОУ „ Кочо Честеменски“, Пловдив са длъжни срещу подпис да се запознаят с настоящите вътрешните правила за защита на личните данни и да ги спазват.
2. Вътрешните правила се издават на основание чл. 23, ал. 4 от Закона за защита на личните данни и Регламент (ЕС) 2016/679.
3. За всички неуредени в настоящите вътрешни правила въпроси са приложими разпоредбите на Регламент (ЕС) 2016/679, Закона за защита на личните данни и действащото приложимо законодателство на Република България.
4. Вътрешните правила се утвърждават със Заповед на Директора на ОУ „ Кочо Честеменски“, Пловдив и се гласуват на Общо събрание на колектива на ОУ „ Кочо Честеменски“, Пловдив
5. Комисията ще провежда заседания само при необходимост при постъпване на сигнали, получаване на инструкции от МОН, РУО или други институции.

ПОЯСНЕНИЯ СПОРЕД РЕГЛАМЕНТ НА (ЕС) 2016/679, чл. 4, пар. 1 и 2

1. **„Лични данни“ са:** 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, поспециално 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. **„Субект на лични данни“ е:** идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано.
3. **„Обработване“ е:** всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, поддръждане или комбиниране, ограничаване, изтриване или унищожаване.

