

УТВЪРЖДАВАМ:
Д-Р НЕЛИ КИРКОВА-КОСТОВА
ДИРЕКТОР НА 32. СУИЧЕ

ПОЛИТИКА
ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
на 32. Средно училище с изучаване на чужди езици „Св. Климент Охридски“
за учебната 2026/2027 година

*съгласно Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните – GDPR),
Закона за защита на личните данни и приложимото национално законодателство*

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) Настоящата Политика урежда основните принципи, правила и организационни подходи, по които 32. Средно училище с изучаване на чужди езици „Св. Климент Охридски“ обработва и защитава личните данни във връзка с осъществяваната от него образователна, административна, трудова, финансова, проектна и друга законосъобразна дейност.

(2) Политиката се прилага при обработването на лични данни на ученици, родители, настойници, попечители и лица, полагащи грижи, служители, кандидати за работа, контрагенти, посетители, участници в проекти и мобилности и други физически лица, чиито данни се обработват от училището.

(3) Политиката е рамков вътрешен акт. Конкретните дейности по обработване се уреждат и чрез регистър на дейностите по обработване, информационни уведомления по чл. 13 и чл. 14 GDPR, правила, процедури, инструкции, договори с обработващи лични данни и други вътрешни актове.

Чл. 2. Училището обработва лични данни при спазване на Регламент (ЕС) 2016/679, Закона за защита на личните данни, Закона за предучилищното и училищното образование, приложимите подзаконови нормативни актове и другото относимо законодателство.

**II. АДМИНИСТРАТОР НА ЛИЧНИ ДАННИ И ДЛЪЖНОСТНО ЛИЦЕ ПО
ЗАЩИТА НА ДАННИТЕ**

Чл. 3. Администратор на лични данни е 32. Средно училище с изучаване на чужди езици „Св. Климент Охридски“, БУЛСТАТ 000669404, гр. София, бул. „Христо Ботев“ № 63, представлявано от директора.

Официален електронен адрес: kl_ohridski32@school32.com

Чл. 4. (1) В съответствие с чл. 37 GDPR училището определя длъжностно лице по защита на данните (ДЛЗД).

(2) Длъжностно лице по защита на данните: Елена Иванова Златева.

(3) Контакти на ДЛЗД: e-mail: ezlatevaa@abv.bg; тел.: +359 882 030 565.

(4) ДЛЗД изпълнява функциите си независимо, съобразно чл. 38 и чл. 39 GDPR, като консултира администратора и служителите, наблюдава спазването на правилата, участва при оценка на риска и оценка на въздействието и е контактна точка за субектите на данни и надзорния орган.

III. ПРИНЦИПИ НА ОБРАБОТВАНЕ

Чл. 5. При всяко обработване на лични данни училището спазва принципите по чл. 5 GDPR:

- законосъобразност, добросъвестност и прозрачност;
- ограничение на целите – данните се събират за конкретни, изрично указани и легитимни цели;
- свеждане на данните до минимум – обработват се само данни, които са необходими за съответната цел;
- точност и своевременно актуализиране;
- ограничение на съхранението;
- цялостност и поверителност чрез подходящи технически и организационни мерки;
- отчетност – училището носи отговорност и е в състояние да докаже спазването на приложимите изисквания.

IV. КАТЕГОРИИ ЛИЧНИ ДАННИ

Чл. 6. В зависимост от конкретната дейност училището може да обработва следните категории лични данни:

- идентификационни данни – имена, ЕГН/ЛНЧ, дата и място на раждане, гражданство, адрес и други данни, когато се изискват от закона;
- данни за контакт – телефон, електронна поща, адрес за кореспонденция;
- данни, свързани с обучението – клас, паралелка, оценки, отсъствия, резултати от изпити, документи за образование, участие в дейности и мерки за подкрепа за личностно развитие;
- данни за родители, настойници, попечители и лица, полагащи грижи;
- кадрови, трудови, осигурителни, данъчни, финансови и квалификационни данни на служители и кандидати за работа;

- данни, необходими за стипендии, социално подпомагане, проекти, мобилности, екскурзии, състезания, олимпиади и други училищни дейности;
- изображения, аудио- и видеозаписи, когато е налице законосъобразно основание;
- технически данни, свързани с използването на електронни платформи, информационни системи, служебни профили и системи за контрол на достъпа.

Чл. 7. Специални категории лични данни, включително данни за здравословно състояние, се обработват само когато е налице приложимо основание по чл. 9 GDPR и при подходящи засилени мерки за защита. Данните за присъди и нарушения се обработват само при условията на чл. 10 GDPR и приложимото национално законодателство.

V. ЦЕЛИ И ПРАВНИ ОСНОВАНИЯ

Чл. 8. Училището обработва лични данни за конкретни цели, включително:

- организиране и провеждане на образователния процес, оценяване, издаване на документи и водене на задължителната училищна документация;
- прием, преместване, записване, движение, обхват и проследяване на обучението на учениците;
- осигуряване на обща и допълнителна подкрепа за личностно развитие;
- изпълнение на задължения, свързани със здравето, безопасността и закрилата на децата и учениците;
- осъществяване на трудови и служебни правоотношения и кадрово администриране;
- изпълнение на счетоводни, финансови, данъчни, осигурителни и архивни задължения;
- организиране на национални и международни програми, Erasmus+ проекти, мобилности, пътувания, състезания и други училищни дейности;
- защита на живота, здравето, сигурността и имуществото;
- осъществяване на официална комуникация с ученици, родители, служители, институции, партньори и доставчици;
- защита на законни права и интереси на училището и изпълнение на задължения към компетентни органи.

Чл. 9. (1) Правното основание се определя за всяка конкретна дейност по обработване и може да бъде едно или повече от основанията по чл. 6 GDPR: законово задължение; задача от обществен интерес или упражняване на официални правомощия; договор или преддоговорни действия; жизненоважни интереси; легитимен интерес, когато е приложим; съгласие, когато то е подходящото основание.

(2) Съгласието не се използва като универсално основание за обработване, което училището е длъжно да извършва по закон или в изпълнение на обществена задача.

(3) Когато обработването се основава на съгласие, то трябва да бъде свободно дадено, конкретно, информирано и недвусмислено и да може да бъде оттеглено толкова

лесно, колкото е било дадено, без това да засяга законосъобразността на обработването преди оттеглянето.

(4) Когато се обработват специални категории лични данни, освен основание по чл. 6 GDPR се определя и приложимото изключение по чл. 9, пар. 2 GDPR.

VI. ЛИЧНИ ДАННИ НА ДЕЦА И УЧЕНИЦИ

Чл. 10. (1) Личните данни на деца и ученици се обработват с повишена грижа, като се отчитат тяхната възраст, най-добрият интерес на детето, необходимостта информацията да бъде ясна и разбираема и повишеният риск от неправомерно публично разпространяване.

(2) Не се публикуват повече лични данни, отколкото са необходими за конкретната цел.

(3) Здравна, социална и друга чувствителна информация за ученик се предоставя само на лица, които имат служебна необходимост и валидно правно основание да я получат.

(4) При упражняване на права от родител или законен представител училището отчита приложимото законодателство, възрастта и зрелостта на детето и правата и интересите на други лица.

VII. СНИМКИ, ВИДЕО, УЧЕНИЧЕСКИ ПРОДУКТИ И ПУБЛИЧНО РАЗПРОСТРАНЕНИЕ

Чл. 11. (1) Преди публикуване на снимки, видеозаписи, ученически продукти или друга информация, позволяваща идентифициране на ученик, училището определя конкретната цел и приложимото правно основание и извършва преценка на необходимостта, пропорционалността, контекста, възрастта на ученика и възможните рискове.

(2) Когато за конкретно публично разпространение е необходимо съгласие, то се изисква отделно и конкретно за ясно посочената цел и канал. Отказът или оттеглянето на съгласие не води до неблагоприятни последици за ученика по отношение на задължителния образователен процес.

(3) Участието в екскурзия, проект, състезание, олимпиада, мобилност или друго мероприятие не означава само по себе си съгласие за неограничено публикуване на снимки или други лични данни.

(4) При публикуване на училищния сайт, официални социални канали или други публични пространства се прилага принципът за минимизиране на данните и се избягва ненужно комбиниране на изображение с пълни идентифициращи данни.

VIII. ВИДЕОНАБЛЮДЕНИЕ

Чл. 12. (1) Видеонаблюдение може да се извършва за конкретни и предварително определени цели, свързани със сигурността, защитата на живота и здравето, опазването на имуществото и установяването на инциденти, при спазване на принципите на необходимост и пропорционалност.

(2) Зоните под видеонаблюдение се обозначават с подходяща информация. Достъп до записите имат само оправомощени лица.

(3) Записите се съхраняват за ограничен срок, определен съобразно целта, приложимите правила и оценката на риска, освен когато конкретен запис е необходим за проверка, производство или защита на правни претенции.

(4) Предоставяне на видеозаписи се допуска само след проверка на правното основание и при защита на правата и свободите на трети лица.

(5) Видеонаблюдението не се използва рутинно за оценяване на учебни резултати или за постоянен контрол на трудовото изпълнение.

(6) Подробният ред за видеонаблюдението се урежда с отделни правила на училището.

IX. ЕЛЕКТРОННИ СИСТЕМИ, ОБЛАЧНИ УСЛУГИ И ИЗКУСТВЕН ИНТЕЛЕКТ

Чл. 13. (1) За служебни цели се използват одобрени от училището информационни системи, електронни платформи и комуникационни канали.

(2) Преди въвеждането на нова облачна услуга, платформа или цифров инструмент се оценяват ролята на страните, видовете данни, целите, сигурността, местоположението на данните, сроковете за съхранение, договорните гаранции и евентуалното предаване на данни извън Европейското икономическо пространство.

(3) Лични, чувствителни, поверителни или служебни данни не се въвеждат в публични системи с изкуствен интелект, освен ако конкретната услуга е изрично одобрена за такава употреба и са изпълнени приложимите изисквания за защита на данните, сигурност и договорни гаранции.

(4) При използване на изкуствен интелект в административни или педагогически процеси се спазват принципите на минимизация на данните, прозрачност, сигурност и човешки контрол.

(5) Не се допуска вземане на решение със значими правни или сходни последици за лице единствено чрез автоматизирано обработване, освен в допустимите от закона случаи и при осигурени подходящи гаранции.

Х. ПРОЕКТИ, ERASMUS+ И МЕЖДУНАРОДНИ МОБИЛНОСТИ

Чл. 14. (1) При участие в национални и международни проекти, включително Erasmus+, училището обработва само данните, необходими за подготовката, кандидатстването, организацията, изпълнението, отчитането, безопасността на участниците и изпълнението на договорните и нормативните изисквания.

(2) Данни се предоставят на приемащи организации, партньори, транспортни и настаняващи доставчици, застрахователи, компетентни органи и други получатели само в необходимия за конкретната дейност обем и при наличие на правно основание.

(3) Когато получател или доставчик се намира извън Европейското икономическо пространство, се проверява дали предаването е допустимо съгласно глава V GDPR и дали са налице приложимите гаранции.

(4) Медицинска или друга чувствителна информация за участник се предоставя само когато е необходима за безопасността, здравната грижа или изпълнението на конкретна дейност и при наличие на приложимо правно основание.

ХІ. ПОЛУЧАТЕЛИ И ОБРАБОТВАЩИ ЛИЧНИ ДАННИ

Чл. 15. Лични данни могат да се предоставят само при наличие на правно основание и в необходимия обем, включително на:

- Министерството на образованието и науката, регионалните управления на образованието и други компетентни образователни органи;
- НАП, НОИ, НЗОК, общински и държавни органи в рамките на техните правомощия;
- органи на МВР, прокуратура, съд, органи за закрила на детето и други компетентни органи, когато законът го изисква или допуска;
- банки, застрахователи, доставчици на услуги и други договорни партньори при наличие на правно основание;
- партньорски и приемащи организации по проекти и мобилности – само в необходимия за конкретната дейност обем.

Чл. 16. Когато външно лице или организация обработва лични данни от името на училището, отношенията се уреждат с договор или друг правен акт съобразно чл. 28 GDPR, включващ необходимите гаранции за поверителност, сигурност, съдействие и прекратяване на обработването.

ХІІ. СРОКОВЕ ЗА СЪХРАНЕНИЕ

Чл. 17. (1) Личните данни се съхраняват само толкова дълго, колкото е необходимо за конкретната цел, или за срока, предвиден в приложимото образователно, трудово, счетоводно, данъчно, осигурително, архивно и друго законодателство.

(2) Не се прилага един универсален срок за всички категории лични данни. Конкретните срокове се определят според вида на документа, целта, правното основание и приложимите правила за архивиране.

(3) Документите с дългосрочна или постоянна стойност се съхраняват и архивират съгласно приложимите нормативни изисквания.

(4) След отпадане на основанието и изтичане на приложимия срок данните се унищожават, заличават или анонимизират по начин, който предотвратява неправомерното им възстановяване.

XIII. ПРАВА НА СУБЕКТИТЕ НА ДАННИ

Чл. 18. При условията и ограниченията на GDPR физическите лица имат право на:

- информация относно обработването на личните им данни;
- достъп до собствените им лични данни;
- коригиране на неточни или непълни данни;
- изтриване, когато са налице законовите предпоставки;
- ограничаване на обработването;
- възражение срещу обработването в приложимите случаи;
- преносимост на данните, когато това право е приложимо;
- оттегляне на съгласие, когато обработването се основава на съгласие;
- да не бъдат обект на решение, основаващо се единствено на автоматизирано обработване, когато са налице предпоставките по чл. 22 GDPR;
- жалба до Комисията за защита на личните данни и съдебна защита.

Чл. 19. (1) Исканията за упражняване на права се подават до училището или до ДЛЗД по начин, позволяващ идентифициране на искането и заявителя.

(2) Исканията се разглеждат без ненужно забавяне и по правило в срок до един месец, освен когато GDPR допуска удължаване.

(3) Правата не са абсолютни и могат да бъдат ограничени, когато това е предвидено в закона или когато упражняването им би засегнало правата и свободите на други лица.

(4) Правото на изтриване не води до заличаване на данни, които училището е длъжно да съхранява по закон.

XIV. ПРОЗРАЧНОСТ И ИНФОРМАЦИОННИ УВЕДОМЛЕНИЯ

Чл. 20. (1) Училището предоставя на субектите на данни необходимата информация за конкретното обработване съобразно чл. 13 и чл. 14 GDPR.

(2) Настоящата Политика не замества конкретните информационни уведомления за ученици и родители, служители, кандидати за работа, посетители, участници в проекти, лица под видеонаблюдение и други категории субекти.

(3) Информацията се предоставя в кратка, прозрачна, разбираема и леснодостъпна форма, като при информация, предназначена за деца, се използва ясен и подходящ за възрастта език.

XV. СИГУРНОСТ НА ЛИЧНИТЕ ДАННИ

Чл. 21. (1) Училището прилага подходящи технически и организационни мерки съобразно риска, естеството, обхвата, контекста и целите на обработването.

- контрол на физическия и логическия достъп;
- индивидуални потребителски профили и управление на права;
- защита на служебните устройства и информационните системи;
- мерки за архивиране, резервни копия и възстановяване, когато са приложими;
- защита от зловреден софтуер и своевременно актуализиране;
- контрол върху хартиени документи и архиви;
- правила за сигурна електронна комуникация и предаване на данни;
- псевдонимизация и криптиране, когато са подходящи спрямо риска;
- обучение и инструктаж на служителите;
- периодичен преглед на ефективността на мерките.

(2) Служителите обработват лични данни само в рамките на предоставените им служебни правомощия и спазват задължение за поверителност.

XVI. НАРУШЕНИЯ НА СИГУРНОСТТА

Чл. 22. (1) Всеки служител е длъжен незабавно да съобщи на директора и ДЛЗД за загуба, неправомерно разкриване, изпращане до грешен получател, неоторизиран достъп, изгубено устройство, зловреден софтуер или друг инцидент, свързан с лични данни.

(2) Училището документира и оценява всеки инцидент и предприема мерки за ограничаване на последиците.

(3) Когато нарушението на сигурността може да породи риск за правата и свободите на физическите лица, Комисията за защита на личните данни се уведомява без ненужно забавяне и, когато е възможно, не по-късно от 72 часа след узнаването, освен ако са налице предпоставките да не се извършва уведомяване.

(4) Когато нарушението може да породи висок риск за правата и свободите на физическите лица, засегнатите лица се уведомяват без ненужно забавяне, освен в предвидените от GDPR случаи.

XVII. РЕГИСТЪР НА ДЕЙНОСТИТЕ, ОЦЕНКА НА РИСКА И ЗАЩИТА НА ДАННИТЕ ПО ПРОЕКТИРАНЕ

Чл. 23. Училището поддържа необходимата документация за дейностите по обработване, включително регистър по чл. 30 GDPR, когато това е приложимо, и периодично преглежда целите, основанията, категориите данни, получателите, сроковете за съхранение и мерките за сигурност.

Чл. 24. Преди въвеждане на нов процес, технология или система се прилагат принципите за защита на данните на етапа на проектирането и по подразбиране по чл. 25 GDPR.

Чл. 25. Когато предвиденото обработване, по-специално чрез нови технологии, е вероятно да породи висок риск за правата и свободите на физическите лица, училището извършва оценка на въздействието върху защитата на данните (DPIA) при условията на чл. 35 GDPR и се консултира с ДЛЗД.

XVIII. ЗАДЪЛЖЕНИЯ НА СЛУЖИТЕЛИТЕ

Чл. 26. Служителите на училището са длъжни:

- да обработват лични данни само в рамките на служебните си правомощия и за определените цели;
- да не разкриват лични данни на неупълномощени лица;
- да използват одобрените официални канали за комуникация и информационни системи;
- да не копират, прехвърлят или съхраняват лични данни на лични устройства или в нерегламентирани услуги без разрешение;
- да прилагат принципа за минимизиране на данните при изпращане на съобщения, списъци, справки и документи;
- да съобщават незабавно за установен инцидент или съмнение за нарушение;
- да участват в обучения и инструктажи по защита на личните данни и информационна сигурност.

XIX. КОНТРОЛ, ПРЕГЛЕД И АКТУАЛИЗАЦИЯ

Чл. 27. (1) Контролът по изпълнението на настоящата Политика се осъществява от директора в рамките на неговите правомощия, със съдействието и независимите консултативни функции на ДЛЗД.

(2) Политиката се преглежда най-малко веднъж годишно и при съществена промяна на нормативната уредба, училищните процеси, използваните технологии, категориите обработвани данни или оценката на риска.

(3) Установените несъответствия се отстраняват своевременно, а свързаните вътрешни актове, уведомления, декларации и образци се актуализират съгласувано.

XX. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Настоящата Политика отменя предходните общи политики за защита на личните данни на 32. СУИЧЕ в частта, в която им противоречат.

§ 2. Подробните правила за видеонаблюдение, реагиране при нарушения на сигурността, упражняване правата на субектите, управление на достъпа, работа с обработващи лични данни, архивиране и други специфични процеси се уреждат с отделни вътрешни актове.

§ 3. Настоящата Политика се публикува на официалния интернет сайт на училището в подходяща за публичен достъп версия.

§ 4. Политиката влиза в сила от датата на утвърждаването ѝ от директора.