ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

DATA PROTECTION POLICY

Wisbech & Peterborough, United Kingdom
Учебна година 2026/2027

Организация: BNU RAINA KNYAGINYA LTD
Company number: 13244864
Data Protection Registration Number: ZB675326

Отговорно лице: Лора Манчева – директор
Email: info@bgschool-wisbech.uk
Телефон: 07450 142437

---

1. ЦЕЛ НА ПОЛИТИКАТА

Българско неделно училище „Райна Княгиня“ обработва лични данни на деца, родители/настойници, служители, кандидати за работа, доброволци, посетители и други лица във връзка със своята образователна и организационна дейност.

Целта на настоящата политика е да определи принципите и правилата, по които Училището събира, използва, съхранява, защитава, споделя и унищожава лични данни.

Училището се ангажира да обработва личните данни законосъобразно, справедливо, прозрачно и сигурно и да обръща специално внимание на защитата на личните данни на децата.

---

2. ПРАВНА РАМКА

Училището обработва лични данни съобразно приложимото законодателство за защита на данните в Обединеното кралство, включително:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- Data (Use and Access) Act 2025, доколкото неговите разпоредби са приложими и в сила;
- Privacy and Electronic Communications Regulations 2003 (PECR), когато са приложими;
- други приложими нормативни изисквания и актуални насоки на Information Commissioner’s Office (ICO).

---

3. ОБХВАТ

Настоящата политика се прилага за всички лични данни, обработвани от Училището, независимо дали се съхраняват:

- електронно;
- на хартиен носител;
- в електронна поща;
- в училищни системи;
- в облачни услуги;
- на разрешени служебни устройства;
- под формата на снимки, видео или аудиозаписи;
- в други допустими формати.

Политиката се прилага за всички служители, учители, помощник-учители, доброволци, външни изпълнители и други лица, които обработват лични данни от името на Училището.

---

4. ОСНОВНИ ОПРЕДЕЛЕНИЯ

Лични данни (Personal Data)

Всяка информация, свързана с идентифицирано или идентифицируемо физическо лице.

Това може да включва например:

- име;
- адрес;
- телефон;
- email;
- дата на раждане;
- снимка или видеозапис;
- информация за посещаемост;
- образователна информация;
- IP адрес или друг online identifier.

Данни от специална категория (Special Category Data)

Лични данни, които се ползват със специална защита, включително информация относно:

- расов или етнически произход;
- религиозни или философски убеждения;
- политически възгледи;
- членство в синдикална организация;

- здравословно състояние;
- генетични данни;
- биометрични данни, когато се използват за уникална идентификация;
- сексуален живот или сексуална ориентация.

Обработване (Processing)

Всяка операция с лични данни, включително събиране, записване, организиране, използване, преглеждане, споделяне, съхраняване, изменение, ограничаване, изтриване или унищожаване.

Data Controller

Организацията, която определя защо и как се обработват личните данни.

За целите на настоящата политика Data Controller е:

BNU RAINA KNYAGINYA LTD

Data Processor

Външно лице или организация, която обработва лични данни от името на Data Controller.

Data Subject

Физическото лице, за което се отнасят личните данни.

---

5. ПРИНЦИПИ ЗА ЗАЩИТА НА ДАННИТЕ

Училището прилага принципите на UK GDPR.

Личните данни трябва да бъдат:

5.1. Lawfulness, fairness and transparency

Обработвани законосъобразно, справедливо и прозрачно.

5.2. Purpose limitation

Събирани за конкретни, изрични и легитимни цели и да не се използват несъвместимо с тези цели.

5.3. Data minimisation

Адекватни, относими и ограничени до необходимото.

5.4. Accuracy

Точни и при необходимост актуализирани.

5.5. Storage limitation

Съхранявани не по-дълго от необходимото, освен когато има законова или друга обоснована причина за по-дълго съхранение.

5.6. Integrity and confidentiality

Обработвани по начин, осигуряващ подходяща сигурност и защита срещу неразрешен достъп, загуба, унищожаване или повреждане.

5.7. Accountability

Училището носи отговорност за спазването на тези принципи и трябва да може да демонстрира съответствието си с тях.

---

6. КАКВИ ЛИЧНИ ДАННИ ОБРАБОТВА УЧИЛИЩЕТО

В зависимост от конкретната цел Училището може да обработва:

За ученици:

- имена;
- дата на раждане;
- адрес и контактна информация;
- информация за родители/настойници;
- emergency contacts;
- посещаемост;
- клас и учебна информация;
- оценки, напредък и образователни записи;
- информация за предходно обучение;
- здравна информация, алергии и медицински потребности;
- SEND или друга информация, необходима за подходяща подкрепа;
- safeguarding информация;
- снимки и видеозаписи;
- информация, необходима за издаване на училищни документи и отчетност пред МОН.

За родители/настойници:

- име;
- адрес;
- телефон;
- email;
- информация за parental responsibility, когато е необходимо;
- информация относно плащания;
- комуникация с Училището.

За персонал и доброволци:

- идентификационни и контактни данни;
- образование и квалификации;
- employment records;
- right to work information;
- DBS и safeguarding suitability информация;
- payroll и payment information;
- attendance и working records;
- training records;
- друга информация, необходима за трудовото или договорното правоотношение.

---

7. ЗАКОННИ ОСНОВАНИЯ ЗА ОБРАБОТВАНЕ

Училището определя подходящо lawful basis за всяка дейност по обработване.

В зависимост от конкретната цел това може да бъде:

1. **Consent** – съгласие;
2. **Contract** – необходимо за изпълнение на договор или предприемане на действия преди сключване на договор;
3. **Legal obligation** – необходимо за изпълнение на законово задължение;
4. **Vital interests** – необходимо за защита на живота или жизненоважните интереси на дадено лице;
5. **Public task** – когато е приложимо и има необходимото правно основание;
6. **Legitimate interests** – когато обработването е необходимо за легитимен интерес и правата и интересите на лицето не го надделяват.

Училището **не приема автоматично, че за всяко обработване на данни на дете е необходимо родителско consent**.

За всяка конкретна дейност се определя подходящото законово основание.

---

8. SPECIAL CATEGORY DATA

Когато Училището обработва special category data, трябва да има както подходящо lawful basis по UK GDPR, така и приложимо допълнително условие за обработване на тези данни.

Това може да включва например обработване на здравна информация, необходима за защита и безопасност на детето.

Когато законодателството изисква допълнителна документация или Appropriate Policy Document, Училището осигурява такава.

---

9. ЛИЧНИ ДАННИ НА ДЕЦА

Данните на децата изискват особено внимание и защита.

Училището:

- поставя интересите, безопасността и личната неприкосновеност на децата в центъра на решенията относно техните данни;
- събира само информация, която е необходима за определена цел;
- ограничава достъпа до информацията;
- предоставя ясна информация за начина, по който данните се използват;
- отчита възрастта, зрелостта и способността на детето да разбира информацията;
- прилага data protection by design and by default;
- предприема допълнителни предпазни мерки при по-чувствителни категории информация.

Когато е подходящо, информацията относно поверителността се предоставя и по начин, който е разбираем за самите деца.

---

10. PRIVACY NOTICES

Училището предоставя подходящи Privacy Notices на лицата, чиито данни обработва.

Поддържат се отделни или подходящо разграничени Privacy Notices за:

- ученици и родители/настойници;
- служители и кандидати за работа;
- доброволци, когато е необходимо;
- посетители и други категории лица, когато е приложимо.

Privacy Notice обяснява, наред с другото:

- кой е Data Controller;
- каква информация се събира;

- защо се използва;
- lawful basis;
- с кого може да бъде споделяна;
- колко време се съхранява;
- какви права има лицето;
- как може да се свърже с Училището;
- как може да подаде complaint до ICO.

---

11. DATA PROTECTION BY DESIGN AND DEFAULT

Защитата на личните данни се разглежда още при планирането на нови:

- системи;
- формуляри;
- приложения;
- онлайн услуги;
- процедури;
- проекти;
- договори;
- начини за събиране или споделяне на информация.

По подразбиране се събират и използват само данните, които са необходими за съответната цел.

Особено внимание се обръща на нови дейности, включващи данни на деца.

---

12. DATA PROTECTION IMPACT ASSESSMENT – DPIA

Преди започване на нова обработваща дейност Училището оценява дали тя може да доведе до висок риск за правата и свободите на лицата.

Когато обработването е вероятно да доведе до висок риск, се извършва **Data Protection Impact Assessment (DPIA)**.

DPIA може да бъде необходима например при:

- въвеждане на нова технология;
- систематично наблюдение;
- обработване на особено чувствителна информация;
- обработване, което може да създаде висок риск за деца;

- други високорискови дейности.

DPIA се извършва преди започване на съответната дейност.

---

13. СИГУРНОСТ НА ДАННИТЕ

Училището прилага подходящи технически и организационни мерки за защита на личните данни.

Те могат да включват:

- password protection;
- подходящи access controls;
- ограничаване на достъпа до лица, които действително се нуждаят от информацията;
- сигурно съхранение на хартиени документи;
- подходяща защита на електронни устройства;
- сигурно изпращане на чувствителна информация;
- редовно преглеждане на достъпа;
- обучение и инструкции за персонала;
- сигурно унищожаване на информация.

Служителите не трябва да предоставят лични данни на неоторизирани лица.

---

14. ИЗПОЛЗВАНЕ НА ЛИЧНИ УСТРОЙСТВА

Когато служител е упълномощен да използва лично устройство за училищна дейност, той трябва да предприеме разумни мерки за защита на информацията.

Чувствителни лични данни и safeguarding информация не трябва да се съхраняват ненужно на лични устройства.

Информацията трябва да бъде прехвърлена или съхранявана в одобрена от Училището система възможно най-скоро, когато това е приложимо.

---

15. EMAIL И ЕЛЕКТРОННА КОМУНИКАЦИЯ

При изпращане на лични данни по email или чрез друга електронна комуникация персоналът трябва:

- да проверява правилно получателя;
- да изпраща само необходимата информация;
- да използва BCC при групова комуникация, когато получателите не трябва да виждат email адресите на останалите;
- да не изпраща чувствителна информация чрез неподходящ или несигурен канал;
- да спазва правилата на Училището за safeguarding и confidentiality.

---

16. СНИМКИ И ВИДЕОЗАПИСИ

Снимките, видеозаписите и аудиозаписите на идентифицируеми лица представляват лични данни.

Училището определя подходящо lawful basis за конкретното им използване и когато обработването се основава на consent, това съгласие трябва да бъде валидно и да може да бъде оттеглено.

Снимки и видеозаписи могат да бъдат използвани само за определени и предварително установени цели, например:

- документиране на училищна дейност;
- училищни публикации;
- website;
- social media;
- информационни и promotional materials;

когато съществува подходящо правно основание.

Персоналът не трябва да публикува снимки или видеозаписи на ученици в личните си social media accounts във връзка с работата си в Училището без изрично разрешение.

---

17. SAFEGUARDING И СПОДЕЛЯНЕ НА ИНФОРМАЦИЯ

Data protection law не трябва да се използва като причина да не бъде споделена информация, когато споделянето е необходимо и законосъобразно за safeguarding или защита на дете.

Safeguarding информацията се споделя:

- само когато има подходяща причина;

- само с подходящите лица или организации;
- само в необходимия обем;
- по сигурен начин;
- при подходящо документиране на решението.

Safeguarding records се съхраняват с ограничен достъп.

---

18. СПОДЕЛЯНЕ НА ДАННИ С ТРЕТИ СТРАНИ

Училището може да споделя лични данни, когато това е необходимо и законосъобразно, например с:

- Министерството на образованието и науката на Република България;
- компетентни UK authorities;
- safeguarding agencies;
- emergency services;
- професионални консултанти;
- payroll/accounting providers;
- IT и cloud service providers;
- застрахователи;
- други доставчици или организации, когато това е необходимо за дейността на Училището.

Преди споделяне се преценяват необходимостта, законовото основание, обемът на информацията и подходящите мерки за сигурност.

---

19. DATA PROCESSORS И ДОГОВОРИ

Когато външна организация обработва лични данни от името на Училището, се извършва подходяща проверка на доставчика.

Когато законът го изисква, отношенията се уреждат чрез договор или друго подходящо споразумение за обработване на данни.

Училището следва да се увери, че Data Processor прилага подходящи мерки за защита на информацията.

---

20. МЕЖДУНАРОДНО ПРЕДАВАНЕ НА ДАННИ

Когато лични данни се предават извън Обединеното кралство, Училището проверява дали съществува подходящ правен механизъм и необходимите safeguards.

Това се отнася и до използването на cloud или други online services, при които данните могат да бъдат обработвани извън UK.

---

21. СЪХРАНЕНИЕ И УНИЩОЖАВАНЕ

Личните данни не се съхраняват по-дълго от необходимото.

Периодът на съхранение зависи от:

- целта на обработването;
- приложимите законови изисквания;
- изискванията на МОН;
- safeguarding необходимостта;
- договорни и финансови задължения;
- необходимостта от защита или установяване на правни претенции.

Когато информацията вече не е необходима, тя се унищожава или изтрива по сигурен начин.

Училището поддържа или прилага подходящ **Retention Schedule**, когато е необходимо.

---

22. DATA BREACH

Personal data breach може да включва:

- загубен документ или устройство;
- изпращане на информация на грешен получател;
- неоторизиран достъп;
- загуба или изтриване на информация;
- cyber incident;
- неправомерно разкриване;
- кражба на информация.

Всеки служител трябва **незабавно** да съобщи за действителен или предполагаем data breach на директора.

Училището документира и оценява инцидента.

Когато нарушението е вероятно да доведе до риск за правата и свободите на физическите лица, Училището уведомява ICO без ненужно забавяне и, когато е приложимо, в рамките на 72 часа от узнаването.

Когато нарушението е вероятно да доведе до висок риск за засегнатите лица, те се уведомяват без ненужно забавяне, когато законът го изисква.

---

23. ПРАВА НА ЛИЦАТА

В зависимост от обстоятелствата и приложимите изключения лицата могат да имат право:

1. да бъдат информирани как се използват техните данни;
2. на достъп до личните си данни;
3. на коригиране на неточни данни;
4. на изтриване;
5. на ограничаване на обработването;
6. на data portability;
7. на възражение срещу определено обработване;
8. на права във връзка с определени автоматизирани решения.

Тези права не са абсолютни и приложимостта им зависи от конкретното обработване и законовото основание.

---

24. ПРАВА НА ДЕЦАТА

Правата върху личните данни принадлежат и на самото дете.

Когато родител или настойник упражнява право от името на дете, Училището взема предвид:

- възрастта и зрелостта на детето;
- способността му да разбира съответното решение;
- parental responsibility;
- естеството на информацията;
- confidentiality;
- safeguarding considerations;
- най-добрия интерес на детето.

Safeguarding информация не се предоставя автоматично на родител само поради наличието на parental responsibility, когато това може да изложи детето или друго лице

на риск или когато съществува друго законово основание за ограничаване на предоставянето.

---

25. SUBJECT ACCESS REQUESTS

Искане за достъп до лични данни (Subject Access Request – SAR) може да бъде направено писмено или устно.

Искането трябва незабавно да бъде насочено към директора.

Преди предоставяне на информация Училището може да предприеме разумни действия за удостоверяване самоличността на заявителя и неговото право да получи съответната информация.

Исканията се разглеждат в сроковете, определени от приложимото законодателство.

---

26. ОБУЧЕНИЕ И ОТГОВОРНОСТ НА ПЕРСОНАЛА

Всички лица, които обработват лични данни от името на Училището, трябва да:

- познават тази политика;
- спазват confidentiality;
- използват информацията само за разрешени цели;
- пазят passwords и устройствата си;
- съобщават незабавно за data breaches;
- участват в подходящо обучение и актуализация на знанията си.

Нарушаването на изискванията за защита на данните от служител може да бъде разглеждано съгласно приложимите employment и disciplinary procedures.

---

27. ОТГОВОРНОСТ

Общата отговорност за прилагането на настоящата политика се носи от:

BNU RAINA KNYAGINYA LTD

Ежедневната организационна отговорност е на:

Лора Манчева – директор

Не се определя отделен Data Protection Officer (DPO), освен ако Училището установи, че това е законово необходимо или реши доброволно да назначи такъв.

Всички служители носят отговорност за правилното обработване на личните данни, до които имат достъп.

---

28. INFORMATION COMMISSIONER'S OFFICE

Лице, което има concern относно обработването на личните му данни, следва първо да се свърже с Училището, за да може въпросът да бъде разгледан.

То има и право да подаде complaint до:

Information Commissioner's Office (ICO)

Актуалните начини за контакт и подаване на complaint се публикуват от ICO.

---

29. КОНТАКТ

За въпроси, искания или concerns относно личните данни:

Лора Манчева
Director
БНУ „Райна Княгиня“ / BNU RAINA KNYAGINYA LTD

Email: info@bgschool-wisbech.uk
Телефон: 07450 142437

---

30. ПРЕГЛЕД НА ПОЛИТИКАТА

Настоящата политика се преглежда най-малко веднъж годишно и по-рано при:

- промяна в законодателството;
- нови ICO guidance;
- значителна промяна в начина на обработване на лични данни;
- въвеждане на нова система или технология;
- значим data breach;
- промяна в структурата или дейността на Училището.

Версия: 2026/2027

ОДОБРЕНИЕ

Лора Манчева
Director
BNU RAINA KNYAGINYA LTD

Дата: 6/9/2026 год.