

This is an external policy

Data Protection Policy and Privacy Notice

1. Introduction and scope

The Junior and Senior School ("the School", "we") is committed to protecting the personal data of everyone in its community. This document sets out how we collect, use, share, store and protect personal data, and the rights individuals have.

It applies to personal data about:

- pupils, prospective pupils and their parents or guardians (section 7);
- staff, including teachers, administrative and support staff, volunteers and Board members (section 8);
- job applicants (section 9);
- visitors, contractors and suppliers (section 10);
- alumni, donors and supporters (section 11);
- users of the School's website and online services (section 12).

It covers personal data in any format: paper, electronic, images, audio and video. Sections 1 to 6 and 13 to 23 apply to everyone.

2. Who we are and how to contact us

Data controller: The Junior and Senior School, operated by The Junior School (registration no. HE 362), Kyriakou Matsi, Strovolos, Nicosia, Cyprus. The Senior School: tel. +357 22 660156. The Junior School: tel. +357 22 664855.

Data Protection Officer: Constantinos Moullotos, dpo@tjss.ac.cy, tel. +357 22 660156 (Senior School) or +357 22 664855 (Junior School). Anyone may contact the DPO directly about any matter relating to their personal data.

3. Legislation

- Regulation (EU) 2016/679, the General Data Protection Regulation ("GDPR").
- Law 125(I)/2018 on the Protection of Natural Persons with regard to the Processing of Personal Data and the Free Movement of such Data.
- Law 112(I)/2004 on electronic communications, as regards cookies and electronic marketing.

- Applicable employment, social insurance, tax, education and child-protection legislation of the Republic of Cyprus, including Law 91(I)/2014 on preventing and combating the sexual abuse and exploitation of children.

4. Definitions

Term	Meaning
Personal data	Any information relating to an identified or identifiable natural person (Art. 4(1) GDPR).
Special categories of personal data	Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; genetic data; biometric data used to identify a person; data concerning health; data concerning sex life or sexual orientation (Art. 9 GDPR).
Criminal offence data	Data relating to criminal convictions and offences or related security measures (Art. 10 GDPR).
Processing	Any operation performed on personal data, such as collection, recording, organisation, storage, adaptation, retrieval, consultation, use, disclosure, restriction, erasure or destruction (Art. 4(2) GDPR).
Controller	The body that decides why and how personal data is processed. The School is the controller.
Processor	A person or organisation that processes personal data on the School's behalf, such as a software or cloud service provider.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
Data subject	The individual whom the personal data is about.

5. Data protection principles

We process personal data in line with Article 5 GDPR. Personal data is:

1. processed lawfully, fairly and in a transparent manner;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;
3. adequate, relevant and limited to what is necessary;
4. accurate and, where necessary, kept up to date;
5. kept in a form that identifies individuals for no longer than necessary;
6. processed securely, using appropriate technical and organisational measures.

We are responsible for, and must be able to demonstrate, compliance with these principles (accountability, Art. 5(2) GDPR). We do this through this policy, our Record of Processing Activities, data protection impact assessments, contracts with processors, staff training records and a breach log.

6. Roles and responsibilities

- **The Board of Directors** is accountable for the School's compliance with data protection law.
- **The Principal and Headteachers** ensure this policy and the School's data protection procedures are followed day to day.
- **The Data Protection Officer** informs and advises the School and its staff, monitors compliance, advises on data protection impact assessments, and is the contact point for the Commissioner and for data subjects. The DPO performs these tasks independently and reports to the Board.
- **All staff, volunteers and contractors** handle personal data only as their role requires, follow this policy, and report any suspected data breach to the DPO immediately.

Any new system, purpose or use of personal data must be discussed with the DPO before it starts. Where processing is likely to result in a high risk (for example CCTV, biometric systems, new learning platforms or AI tools used with pupil data), a data protection impact assessment is carried out first (Art. 35 GDPR).

7. Pupils and parents

7.1 What we collect

About pupils:

- Identity details: name, date of birth, gender, nationality, ID or passport number, photograph.
- Contact details and home address.
- Academic records: attendance, assessments, internal and external examination results, reports, references.
- Behaviour and pastoral records, including safeguarding and child-protection information.
- Health information: medical conditions, allergies, medication, immunisation records, accident and first-aid records.
- Special educational needs and learning support information.
- Information about religion or ethnicity, where provided for religious education, dietary or pastoral purposes.
- Images, video and live streams of school events (such as assemblies, performances, award ceremonies, graduations and trips) and of pupils' work.
- Online learning data: login details for School platforms, homework, assignments and assessments submitted online.
- Usage data from School IT systems and learning platforms.

About parents and guardians: name, relationship to the pupil, contact details and address; information about custody or court orders affecting contact with the pupil; financial information for fees, payment plans and scholarships or bursaries; correspondence with the School.

7.2 Where we get it

Most information is provided by parents and pupils, for example on application and registration forms. We may also receive information from previous schools, examination boards, doctors and other health professionals, educational psychologists, and public authorities such as the Ministry of Education, Sport and Youth or the Social Welfare Services.

Personal data needed for enrolment and for our legal obligations must be provided under the enrolment contract and the law. Without it, we may be unable to enrol the pupil or provide certain services. Other information, such as consent to publish photos, is optional.

7.3 Why we use it and our legal basis

Purpose	Legal basis (Art. 6 GDPR)	Special category condition (Art. 9 GDPR)
Admission, enrolment and providing education	Contract (6(1)(b))	-
Assessing progress, reports, examination entries and references	Contract (6(1)(b)); legitimate interests (6(1)(f))	-
Pupil welfare, pastoral care and safeguarding	Legal obligation (6(1)(c)); vital interests (6(1)(d))	Substantial public interest (9(2)(g)); vital interests (9(2)(c))
Managing medical needs, allergies and first aid	Legal obligation (6(1)(c)); vital interests (6(1)(d))	Health care (9(2)(h)); vital interests (9(2)(c))
Special educational needs and learning support	Contract (6(1)(b)); legal obligation (6(1)(c))	Explicit consent (9(2)(a)) or substantial public interest (9(2)(g))
Reporting to the Ministry of Education, Sport and Youth and other authorities	Legal obligation (6(1)(c))	Where required, 9(2)(g)
Fees, invoicing and debt recovery	Contract (6(1)(b)); legitimate interests (6(1)(f))	-
School trips, activities and insurance	Contract (6(1)(b))	Explicit consent (9(2)(a)) for health data shared with providers
IT systems, online learning and e-safety monitoring	Contract (6(1)(b)); legitimate interests (6(1)(f))	-
Photos, videos and live streams on the website, social media and promotional material	Consent (6(1)(a))	-

7.4 Pupils' own rights

Personal data about a pupil belongs to the pupil. Parents or guardians with parental responsibility may exercise the pupil's rights on the pupil's behalf. Pupils aged 14 and over are generally considered able to understand and exercise their own rights. When a parent makes a request about such a pupil, we normally take the pupil's views into account and act in the pupil's best interests. Where the School relies on consent for online services offered directly to a pupil under 14, consent is given by a parent or guardian (Art. 8 GDPR and Law 125(I)/2018).

8. Staff

This section applies to employees, teachers, administrative and support staff, peripatetic teachers, volunteers and Board members ("staff").

8.1 What we collect

- Identity and contact details: name, date of birth, ID or passport number, address, telephone, email, photograph, emergency contacts.
- Recruitment information: CV, application form, qualifications, references, right-to-work and residence documents.
- Teaching registration and professional records, including registration with the Ministry of Education, Sport and Youth where required.
- Criminal record certificate and certificate under Law 91(I)/2014 confirming no convictions for sexual offences against children.
- Employment records: contract, job role, working hours, attendance, leave, performance appraisals, training, disciplinary and grievance records.
- Payroll and financial details: salary, bank account, tax identification number, social insurance number, provident or pension fund details.
- Health information: sickness absence, medical certificates, occupational health information and workplace adjustments.
- Use of School IT systems, email and accounts.
- Images and video for staff ID cards, the website and School publications.

8.2 Why we use it and our legal basis

Purpose	Legal basis (Art. 6 GDPR)	Special category / criminal data condition
Managing the employment relationship	Contract (6(1)(b))	-
Payroll, tax and social insurance	Contract (6(1)(b)); legal obligation (6(1)(c))	-
Safer recruitment and checks for working with children	Legal obligation (6(1)(c))	Authorised by law (Art. 10 GDPR; Law 91(I)/2014)

Purpose	Legal basis (Art. 6 GDPR)	Special category / criminal data condition
Sickness absence, health and safety at work	Legal obligation (6(1)(c))	Employment law obligations (9(2)(b)); occupational medicine (9(2)(h))
Performance management, training and professional development	Contract (6(1)(b)); legitimate interests (6(1)(f))	-
Disciplinary, grievance and legal claims	Contract (6(1)(b)); legitimate interests (6(1)(f))	Legal claims (9(2)(f)), where relevant
IT security and acceptable-use monitoring	Legitimate interests (6(1)(f))	-
Reporting to the Ministry and other authorities	Legal obligation (6(1)(c))	-
Photos on the website and promotional material	Legitimate interests (6(1)(f))	-

Any monitoring of staff use of School IT systems is proportionate, limited to what is necessary for security and compliance, and explained to staff in advance in the School's IT and acceptable-use rules.

9. Job applicants

We collect the information in your application, CV and covering letter, interview notes, references, qualifications and, for successful candidates, the checks described in section 8. We use it to assess your suitability for the role, on the basis of steps taken before entering into a contract (Art. 6(1)(b)) and our legal obligation to carry out safer-recruitment checks (Art. 6(1)(c)).

We contact referees only with your knowledge. If your application is unsuccessful, we keep your data only as long as needed to complete the recruitment process and deal with any related queries or legal claims, unless you agree that we keep it longer for future vacancies.

10. Visitors, contractors and CCTV

When you visit the School, we record your name, organisation, the person you are visiting, and your arrival and departure times. For contractors and suppliers, we also hold business contact details, contract and payment information, and any checks needed for work near pupils. We do this to keep pupils and staff safe and to manage our premises and contracts (legitimate interests, Art. 6(1)(f); contract, Art. 6(1)(b); and legal obligation where checks are required by law).

10.1 CCTV

The School does not currently operate CCTV. If CCTV is installed in the future, it will be used to protect the safety of pupils, staff and visitors and to protect property (legitimate interests, Art.

6(1)(f)), following a data protection impact assessment. Signs will be displayed where cameras operate. Cameras will not cover toilets, changing rooms or other private areas, and will not record sound. Footage will be kept for 30 days unless needed to investigate an incident, and access will be limited to authorised staff. This document will be updated before any cameras operate.

11. Alumni, donors and supporters

We keep contact details and basic school history of former pupils, and the details of donors and supporters, to keep in touch, share news and events, and support fundraising and alumni activities. We do this on the basis of legitimate interests (Art. 6(1)(f)) or, for electronic marketing where the law requires it, consent (Art. 6(1)(a)). You can unsubscribe or ask us to stop contacting you at any time.

12. Website and online services

Our website uses cookies. Essential cookies are used to make the website work. Analytics or other non-essential cookies are used only with your consent, which you can change at any time. Details are shown in the cookie banner on our website. Information submitted through online forms is used only for the purpose stated on the form.

13. Who we share personal data with

We share personal data only where the law allows and only the data needed. Recipients may include:

- the Ministry of Education, Sport and Youth, the Tax Department, the Social Insurance Services and other public authorities, where the law requires;
- Social Welfare Services, the Police or health services, where needed to protect a child or another person;
- examination boards (e.g. Cambridge, Pearson Edexcel and other awarding bodies), universities and other schools;
- doctors, school nurses and emergency services;
- banks, JCC Payment Systems (card payments), payroll providers, provident or pension funds and insurers;
- travel companies and activity providers for school trips;
- our service providers (processors), such as iSAMS (school management system) and Microsoft 365, who act only on our instructions under a written contract (Art. 28 GDPR);
- our professional advisers (lawyers, auditors) and debt collectors, where necessary.

We do not sell personal data.

14. Transfers outside the European Economic Area

Some recipients or service providers may be outside the EEA, for example examination boards and universities in the United Kingdom and other countries, and cloud service providers. We transfer personal data outside the EEA only where:

- the European Commission has decided the country ensures an adequate level of protection (Art. 45 GDPR); or
- appropriate safeguards are in place, such as the European Commission's Standard Contractual Clauses (Art. 46 GDPR); or
- a specific exception applies, for example the transfer is necessary for a university application you have requested (Art. 49 GDPR).

You can request details of the safeguards used by contacting the DPO.

15. How long we keep personal data

We keep personal data only for as long as necessary for the purposes for which it was collected, and to meet our legal, regulatory, tax, accounting and reporting obligations.

When deciding how long to keep personal data, we consider the purpose of the processing, the amount, nature and sensitivity of the data, the potential risk from unauthorised use or disclosure, and any legal requirements that apply.

In general, data relating to registration, education, examinations and graduation is kept while the pupil is enrolled at the School and is then archived for a longer period, so that we can confirm a pupil's attendance and results in the future. Staff records are kept for the duration of employment and for a period afterwards as required by employment, tax and social insurance law. Some data may be kept for longer where this is required for legal, regulatory or technical reasons, or for the establishment, exercise or defence of legal claims.

When personal data is no longer needed, it is securely deleted or anonymised. For details of the retention period that applies to specific personal data, please contact the DPO at dpo@tjss.ac.cy.

16. How we keep personal data secure

- Access to personal data is limited to people who need it for their role.
- School accounts are protected by strong passwords and multi-factor authentication where the system supports it.
- Laptops, mobile devices and removable media holding personal data are encrypted.
- Paper records are kept in locked storage and are not left on desks, staffroom tables or noticeboards.
- Personal data is taken off site only when necessary, with the minimum data needed, and kept secure in transit.
- Staff using personal devices for school work must follow the School's IT and acceptable-use rules and use only School-approved apps and accounts. Personal data is not shared through personal email or messaging apps.

- Records no longer needed are destroyed securely: paper is cross-cut shredded, and electronic files are securely deleted or overwritten. Any external disposal company works under a written contract and provides a certificate of destruction.
- The School has an internal information security policy, which all staff must follow, and assesses the effectiveness of its security measures regularly.
- All staff receive data protection training at induction and refresher training every year.

17. Your rights

You have the right to:

- **access** the personal data we hold about you and receive a copy;
- **rectification** of inaccurate or incomplete data;
- **erasure** of data in certain circumstances;
- **restriction** of processing in certain circumstances;
- **data portability** for data you provided, processed by consent or contract and by automated means;
- **object** to processing based on legitimate interests, and to direct marketing at any time;
- **withdraw consent** at any time, where processing is based on consent, without affecting processing carried out before withdrawal;
- **lodge a complaint** with the Commissioner for Personal Data Protection (section 22).

Some rights are subject to legal limits, including restrictions under Article 23 GDPR and Article 11 of Law 125(I)/2018. We do not make decisions about anyone based solely on automated processing, including profiling.

18. How to make a request

You can make a request by contacting the DPO at dpo@tjss.ac.cy, by post to the School, or in person. Staff may also contact the DPO by internal email. Requests received by any member of staff are passed to the DPO immediately. We may ask for proof of identity before responding.

We will respond without undue delay and within **one month** of receiving the request. We may extend this by up to two further months where requests are complex or numerous, and we will tell you if we do. Requests are free of charge unless they are manifestly unfounded or excessive. We may withhold information where disclosure could cause serious harm to a person or put a child at risk.

19. Personal data breaches

1. Anyone who discovers or suspects a breach reports it immediately to the DPO.
2. The DPO and the Principal contain the breach and assess the risk to the individuals affected.
3. Unless the breach is unlikely to result in a risk, the School notifies the Commissioner for Personal Data Protection within 72 hours of becoming aware of it (Art. 33 GDPR).

4. If the breach is likely to result in a high risk, the individuals affected (or the parents of affected pupils) are informed without undue delay (Art. 34 GDPR).
5. Every breach is recorded in the breach log, with its facts, effects and remedial action.

20. Monitoring and review

The Principal, the Headteachers and the Data Protection Officer, Constantinos Moullotos, are responsible for monitoring this policy. The DPO reports on compliance to the Board at least once a year. This policy is reviewed at least once a year, and sooner if the law or our practices change significantly. The latest version is published on the School's website.

21. Links with other policies

This policy should be read with the School's other relevant policies, including its Safeguarding and Child Protection Policy and Complaints Policy.

22. Complaints

If you have a concern about how we handle personal data, please contact the DPO first so that we can try to resolve it. Complaints may also be raised under the School's Complaints Policy.

You also have the right to complain to the supervisory authority:

Office of the Commissioner for Personal Data Protection

1 Iasonos Street, 1082 Nicosia, Cyprus · P.O. Box 23378, 1682 Nicosia, Cyprus

Tel. +357 22818456 · commissioner@dataprotection.gov.cy · www.dataprotection.gov.cy

23. Contacts

For any questions about this policy or your personal data, please contact our Data Protection Officer, Constantinos Moullotos, at dpo@tjss.ac.cy.

END