Data Protection Policy

This policy applies to the whole school including Boarding and Early Years. The current version of any policy, procedure, protocol or guideline is the version held on the TASIS England website. It is the responsibility of all staff to ensure that they are following the current version.

Information Sharing Category	PUBLIC
TASIS England Document reference (Org, Doc, version, date)	TASIS_DataProtectionPolicy_V16.4_01092026
Version	16.4
Date published	01 September 2026
Date ratified by Head of School	01 September 2026
Review/Update date	01 September 2027
Responsible area	Director of Inclusion, Wellbeing and Compliance

Agreed by:

Head of School	**Chair of the Board**
Bryan Nixon	David King
01 September 2026	01 September 2026

1. Related Policies

This policy refers to other TASIS England policies within the text and the following should be read/referred to in conjunction with this policy:

- Safeguarding Children Child Protection Policy
- Online Safety Policy
- Faculty and Staff Code of Conduct
- Confidentiality and Information Sharing Policy
- Complaints Procedures
- Records Retention Policy
- Data Protection Complaints Procedure

These policies can be accessed via the school website.

2. Governance

This policy is one of several information sharing and information management policies and protocols approved by the Proprietorial Board of Directors (Board of Directors). This policy is reviewed annually (see section 4 - Roles and Responsibilities below). All Senior Leaders are responsible to the Board of Directors for ensuring compliance with this policy.

The school maintains a Record of Processing Activities (RoPA) and reviews it alongside the retention schedule. All faculty and staff complete induction and annual refresher training on data protection, cyber security and handling personal data.

3. Scope

This policy applies to all members of TASIS England faculty, staff, Board of Directors, contractors, agents and representatives, volunteers and temporary staff working for or on behalf of the school.

This policy applies to all personal data created or held by the school in whatever format (e.g., paper, electronic, email, microfiche, film) and however it is stored, (for example ICT system/database, shared drive filing structure, workbooks, email, filing cabinet, shelving and personal filing drawers).

4. Roles and Responsibilities

- TASIS England Board of Directors: The Proprietorial Board of Directors has overall responsibility for ensuring that TASIS England complies with all relevant data protection obligations.
- The Data Protection Officer (DPO): The DPO is responsible for reviewing this policy, monitoring the school's compliance with UK GDPR, acting as the point of contact for any data protection issues, and operating the school's data protection complaints process under section 164A of the Data Protection Act 2018, including maintaining the data protection complaints log and reporting complaint volumes and outcomes to the Board of Directors.
- Director of Inclusion, Wellbeing and Compliance: Is the senior manager responsible for ensuring that the policy is reviewed annually, and that data protection is embedded into school processes.

5. What is Personal Data?

'Personal Data' shall mean any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity.

Examples of Personal Data can be seen in the relevant Privacy Statement at Appendix 1 (for Parents and Students), Appendix 2 (for Staff & Faculty) or Appendix 3 (for Visitors to The School).

6. Use of Personal Data

The school is an international co-educational day and boarding school, for children in the age range 3 to 18 years.

a. The school is committed to safeguarding and promoting the welfare of students and expects all staff and volunteers to share this commitment. It is our aim that all students fulfil their potential.
b. The school processes personal data including names, addresses and contact telephone numbers, both in electronic and paper form, in line with the conditions described within the UK General Data Protection Regulation (UK GDPR) as tailored by the Data Protection Act 2018 (DPA) in order to:

- Provide education and pastoral care for day and boarding students and their parents, delivered by school faculty and staff.
- Provide academic, examination and career references for day and boarding students and staff.
- Fulfil its contractual or other legal and regulatory obligations towards current day and boarding students (both past and prospective) all faculty and staff, parents, board of directors and others.
- Protect the vital interests of all students and all faculty and staff employed by the school.

Lawful Basis

All processing described in this section is carried out under one or more lawful bases in Article 6 UK GDPR (and, where relevant, special-category conditions in Article 9). The specific lawful bases for students/parents, staff, and visitors are set out in the Privacy Notices at Appendices 1–3 and will be documented in the School's Record of Processing Activities (RoPA). Where we rely on consent (e.g., certain marketing or publication of identifiable images), consent is recorded and may be withdrawn at any time.

7. Purpose

The school is registered with the Information Commissioner's Office (ICO) as a Data Controller under the UK GDPR. This policy is intended to operate in accordance with UK GDPR relevant guidance and good practice, paying particular regard to the 6 Data Protection Principles set out in the UK GDPR and summarized as follows:

Personal data shall be:

a. Processed lawfully, fairly and in a transparent manner in relation to the data subject.
b. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

c. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization').
d. Accurate and, where necessary, kept up to date.
e. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
f. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Data protection by design and default: We embed privacy into our planning and day-to-day operations. Before introducing new systems, processes or technologies that involve personal data, we consider privacy risks early, ensure only the minimum necessary data is processed, restrict access on a need-to-know basis, and configure systems to the most privacy-protective settings by default. Where appropriate, we complete a Data Protection Impact Assessment (DPIA) and implement its recommended controls.

The school must maintain the trust and confidence of the whole school community and others with whom the school comes into contact. In all circumstances the welfare of students comes first, but the school is mindful of other legal requirements, such as duties owed to visitors, parents, faculty, staff and public authorities.

The school aims never to:

- Hold or use inaccurate or misleading data.
- Keep more data, more categories of data, or keep data for longer than is reasonably required in order to fulfil the 'purpose' of this policy.
- Disclose personal data to others except in accordance with this policy.
- Use personal data to make any automated decision which affects a student, member of staff or parent. The Data (Use and Access) Act 2025 reformed the rules on automated decision-making (new sections 50A–50D of the Data Protection Act 2018); the school does not make solely automated decisions producing legal or similarly significant effects about any individual, and any future proposal to do so would require a Data Protection Impact Assessment, meaningful human review and the approval of the Data Protection Officer.
- Sell or transfer any part of its database/s for the purposes of direct marketing.

8. Data Protection Impact Assessments (DPIA)

TASIS England will carry out Data Protection Impact Assessments (DPIA) for any new or substantially changed projects or processes involving the processing of personal data that are likely to result in a high risk to the rights and freedoms of individuals.

The DPIA process will be overseen by the Data Protection Officer, and the results will be reported to the Board of Directors. The DPIA process will ensure that risks are identified and mitigated where possible.

9. Record of Processing Activities (RoPA)

The School maintains an Article 30 UK GDPR *Record of Processing Activities* covering all systems and processes in which personal data is handled. The DPO owns the RoPA and ensures it is updated at least annually and whenever processing changes (e.g., new systems, new data uses, new transfers). The RoPA includes controller details; purposes of processing; categories of data subjects and personal data; categories of recipients; international transfers and safeguards; envisaged

retention periods; and a general description of technical and organisational security measures (Article 32). The RoPA is available to the ICO on request.

10. Access to Data

- The Board of Directors of the school is responsible for Data Control at the school.
- A request for data held by the school about the individual making the request is termed a 'Data Subject Access Request' (SAR), see Appendix 4 of this policy for more information.
- Individuals are Data Subjects and have legal rights over the information that is processed about them by the Data Controller. This is true for all individuals, including children (students).
- Any reasonable request by a student, (if known to be of an age that they can make such a request) parent or member of faculty or staff for access to personal data held about their child by the school may be made in writing, using the form provided at Appendix 4 of this policy.
- We may need to verify identity before responding to a SAR.
- Where a request is unclear, we may seek clarification and pause the response clock until clarification is received. Identity checks are reasonable and proportionate, and formal identification is not requested where the individual and their authority are already reliably known. In responding, the school carries out a reasonable and proportionate search for the information requested, in line with the Data Protection Act 2018 as amended by the Data (Use and Access) Act 2025.
- We do not normally charge a fee; a reasonable fee may apply where a request is manifestly unfounded or excessive, or for extra copies (UK GDPR Article 12).
- It does not follow that, just because a child can make a SAR, they also understand what providing consent to sharing their personal data with others means. This will be reviewed on a case-by-case basis.
- Parents making a SAR on behalf of a child should be advised that the child might be deemed to be of an age whereby their consent should be sought. If so, the consent and express permission of the child will be sought prior to any release of information or data.
- Where required, consent to collect and process personal data will be sought at the point of collection and recorded.
- The separate 15-school-day response regime and fee for 'educational records' under the Education (Pupil Information) (England) Regulations 2005 applies to maintained schools and does not apply to TASIS England as an independent school. All SARs, including those covering curricular and educational records, are handled under the standard UK GDPR regime described below.
- The one-month time limit for responding as required by the UK GDPR applies to all SARs; days are elapsed calendar days, not school days.
- The one-month period for a response starts from the day the request is received (whether it is a working day or not) until the corresponding calendar date in the next month. Therefore, if the SAR was received on 19 September 2024, the data controller should respond by 19 October 2024.
- The one-month period can be extended by a further two months if the request is complex or a number of requests have been made by the data subject. If this is the case the school will inform the requestor of this within 1 month and explain the reasons why an extension is necessary.

The school shall not be required to disclose data which is exempt or partially exempt from disclosure. For instance:

- Where applicable, when disclosure of particular data would be likely to cause serious harm to the health of the person requesting disclosure or to someone else.
- Examination scripts within a specific timeframe of the examination.

- Employment references made by the school which remain in the control of the school.
- Planning information relating to staff, if it may be deemed to damage school business to disclose it.
- When the data is held for national security reasons.
- It identifies third party individuals.
- If it is in the public interest.

The school may also withhold medical data if it is held under the professional jurisdiction of the school Doctor/Medical Officer. In those circumstances, the parent, student or member of faculty or staff (as appropriate) may be required to contact the school Doctor/Medical Officer directly in order to arrange access to this data.

For more information, please see the ICO's current guidance on the right of access and subject access requests.

11. Data Protection Complaints

The Data (Use and Access) Act 2025 inserts a new section 164A into the Data Protection Act 2018. From 19 June 2026, any individual who considers that the school has infringed the UK GDPR in connection with the processing of their personal data has the right to make a data protection complaint directly to the school as data controller. The school treats this internal route as the first step: individuals are asked to raise a data protection complaint with the school before escalating to the Information Commissioner's Office (ICO).

How to make a data protection complaint:
You may make a data protection complaint to the school by any of the following means:

- Online: complete the school's data protection complaints form here.
- Email: the Data Protection Officer, David Harris, at dharris@tasisengland.org.
- Post: Data Protection Officer, TASIS England, Coldharbour Lane, Thorpe, Surrey TW20 8TE.
  A complaint may concern any aspect of how the school has collected, used, shared, stored or otherwise processed your personal data.

How the school handles data protection complaints
Acknowledgement - we acknowledge receipt within 30 days. The 30-day period begins on the day after the complaint is received, including where it is received on a weekend or public holiday.
Investigation - we begin enquiring into the complaint without undue delay and carry out an investigation that is reasonable and proportionate to the nature and complexity of the issues raised and their impact on the individual.
Progress - where the investigation is ongoing, we keep the complainant informed of progress and of any anticipated delay.
Outcome - we inform the complainant of the outcome without undue delay. The outcome of a data protection complaint is not withheld pending the resolution of any wider complaint.

Escalating to the ICO
Making a complaint to the school does not remove your right to complain to the Information Commissioner's Office. If you remain dissatisfied after the school has responded, or if the school fails to respond without undue delay, you may escalate your complaint to the ICO at https://ico.org.uk/make-a-complaint/ or by calling the ICO helpline on 0303 123 1113. We ask that you raise your concern with the school first so that we have the opportunity to put things right.

Oversight and records

The Data Protection Officer operates and oversees the school's data protection complaints process and maintains a central data protection complaints log recording the date of receipt, the nature of each complaint, the steps taken, the outcome and the date of response. The DPO reports to the Head of School on complaint volumes and outcomes who then reports to the Board of Directors. The Director of Inclusion, Wellbeing and Compliance ensures the process is embedded in school operations and reviewed annually. This process is operated in accordance with the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025. It operates alongside, and without conflict with, the parental complaints procedure required by Part 7 of the Independent School Standards.

12. Security

The school has put in place organizational, physical and technological measures to ensure that Personal Data is not lost, damaged, or accessed or used without proper authority, and the school shall take appropriate steps to prevent these events happening:

a. Paper records, which includes personal data and/or confidential information, shall be kept in a cabinet and/or office, which is kept locked when unattended. All paper records must be kept in a secure location.
b. Paper records that include safeguarding, child protection and sensitive information relating to safeguarding must be kept in a locked cabinet in a locked office.
c. The school uses an array of measures to protect personal data stored on computers, and internal IT systems including file encryption, anti-virus and security software, user passwords, audit trails, backup systems and two-factor authentications where required. Further information can be seen in our Online Safety Policy.
d. Staff must keep any passwords secure and must not share them. Staff should be mindful that passwords are not always effective and are not a substitute for encryption.
e. Staff should not remove personal data from the school's premises unless it is stored on a password-protected device or an encrypted memory device, in accordance with the school's Online Safety Policy.
f. All laptops and PCs are secured with the requirement for login and passwords.
g. Sensitive information held electronically should be individually password protected as an additional layer of security.
h. Persons who process (store or use) personal data on behalf of the school have a responsibility to ensure that the Data Protection Principles are observed and must comply with this Data Protection Policy and any associated record keeping and confidentiality policies, including our Records Retention, Online Safety and Confidentiality and Information Sharing Policies.
i. Persons who work for and on behalf of the school ('third parties') who may be given access to or process personal data in connection with the school should operate in accordance with UK GDPR and this policy. Third parties include suppliers or service providers.
j. Data is kept and maintained in accordance with the school's record retention schedule (please see Appendix 1 – Records and Data Retention Schedule Within The TASIS England Records Retention Policy available on the school website policy page).
k. We only appoint processors that provide sufficient guarantees of technical and organisational measures. We put a written data processing agreement in place that meets UK GDPR Article 28 (documented instructions, confidentiality, security, sub-processor controls, assistance with rights/breaches, return/deletion at end of contract, and audit provisions). We complete proportionate due diligence before onboarding and maintain a register of processors.

13. Data Breaches

All members of school faculty, staff, Board of Directors, contractors, agents and representatives, volunteers and temporary staff working for or on behalf of the school immediately report a suspected security incident or data breach to their line management or Head of School in accordance with points 'a' and 'b' below:

a. All suspected data breaches shall be brought to the attention of the Data Protection Officer (David Harris - dharris@tasisengland.org) within 24 hours of the school becoming aware of it.
b. Unless the breach is unlikely to result in a risk to individuals' rights and freedoms, the school will notify the ICO within 72 hours of becoming aware of it. Where the risk to individuals is high, affected individuals will also be informed without undue delay.

Personal Data Breach Procedure (summary)

- Report immediately to the DPO (and line manager) - ideally within 24 hours of becoming aware.
- Contain & secure: isolate affected systems/devices, revoke access where needed, preserve evidence.
- Assess risk to individuals: likelihood and severity of harm (e.g., identity theft, distress).
- Decide on notifications: if risk is likely, notify the ICO within 72 hours and inform affected individuals without undue delay where risk is high.
- Record everything in the breach log (facts, effects, decisions, notifications, timelines).
- Remediate & learn: implement corrective actions and update training/procedures.

14. CCTV

CCTV at TASIS England is operated in accordance with UK GDPR. All TASIS England Security Guards are qualified to monitor and operate CCTV. Specific procedures are in place for the CCTV operator on duty to sign in, log in and report CCTV faults and report any requests of viewing CCTV footage to the Operations Manager.

CCTV at TASIS England is configured to provide surveillance of:

- Priority security doors and gates that provide access to critical areas in which school functions are carried out.
- Areas where business critical activity is carried out.

CCTV provides:

- Identification of all persons entering and leaving the main entrances.
- Identification of faculty and staff entering and leaving the main entrances.
- Identification of persons moving between the boundary of public and private space.
- Observation of courier entrances/drop off points.
- Monitoring of external and internal parking.

Areas where CCTV surveillance systems are installed are clearly marked by relevant signs advising that such systems are in place. CCTV signage and privacy notices state the **purpose**, **retention period**, and a **contact point for queries (the DPO)**.

CCTV footage is stored and destroyed in accordance with the school's Records Retention Policy.

Biometric data: TASIS England does not use biometric recognition systems. If this situation changes, we will update this policy and comply with the Protection of Freedoms Act 2012.

15. Artificial intelligence

Artificial intelligence (AI) tools are now widespread and easy to access. Faculty and staff, students and parents/carers may be familiar with generative AI tools and chatbots. TASIS England recognises that AI has many uses to help students learn but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, TASIS England will treat this as a data breach, and will follow the personal data breach procedure outlined in the Data Breaches section of this policy above.

16. References

References given by any member of school staff, whether for faculty, staff or students, may be given only with the consent of the Head of School, Section Head or the Director of Human Resources unless the reference is written directly by the Head of School, Section Head or the Director of Human Resources, in consultation with other staff where appropriate. Any reference will be fair, balanced and reasonable and will be provided in good faith.

a. Where a reference involves the transfer of personal data outside the UK, the school will ensure that the transfer is permitted under UK data protection law, including through applicable UK adequacy regulations, appropriate safeguards or another lawful transfer mechanism or exception.
b. The school will not disclose special category data in a reference unless lawfully justified and necessary.

   In exceptional circumstances the Head of School or the Director of Human Resources may agree to provide a written testimonial. It should be noted that this does not constitute a reference or an open reference**.** The school will not disclose special category data in a reference unless lawfully justified and necessary.

Appendix 1 – Privacy Notice for Parents and Students

Introduction

This notice is to help you understand **how** and **why** we collect personal information about you and **what** we do with that information. It also explains the decisions that you can make about your own information.

We collect and hold personal data and information relating to our students directly from their parents/guardian and students, where applicable, at the time of application to register and join the school. We may also receive information about students from their previous school, local authority and/or the Department for Education (DfE). We also create personal information about the student during their time in the school in the form of assessments, marking of work and reports.

The categories of student information that we collect, hold and share include:

- Personal information (such as name, unique student number, contact details and address);
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility).
- Attendance information (such as sessions attended, number of absences and absence reasons).
- Relevant medical, special education needs (SEN) and mental health information.
- Exclusions/behavioural information.
- Financial information such as bank account details.
- Special category data such as racial or ethnic origin / philosophical beliefs / health information / sex life / sexual orientation information / biometric data which may uniquely identify an individual.
- Photographs: We collect photographic images of our students, which we use for purposes of identification and also for marketing purposes.
- We document consent choices, make it easy to withdraw consent at any time, and act promptly on withdrawals.
- CCTV: images of staff, faculty members, parents, students and other visitors to the school will be captured by our CCTV system which monitors public areas including the main entrance used by visitors, the pedestrian and vehicle gates, and the entrances to all other school buildings.

Why we collect and use this information

We process personal information to enable us to provide education and training conducted outside the state education system, welfare and educational support services, to administer school property and library services, to maintain our own accounts and records, for administration in connection with boarding and the organisation of alumni associations and events, for fundraising purposes, to ensure physical security of the school and its assets and to support and manage our staff.

The information we process that is relevant to the above reasons/purposes include:

- personal details
- family details
- lifestyle and social circumstances
- financial details
- education and employment details
- disciplinary and attendance records
- visa-related checks and references from previous schools
- visual images, personal appearance and behaviour
- details of goods and services provided

For 'special category' data, we only collect and use it where we have a lawful basis under Article 6 *and* a separate condition under Article 9 UK GDPR (e.g., vital interests, healthcare, substantial public interest for safeguarding). We process sensitive classes of information that may include:

- physical or mental health details
- sexual life

- racial or ethnic origin
- religious or other beliefs
- information relating to offences or alleged offences

Collecting information

Whilst the majority of student information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the UK General Data Protection Regulation (UK GDPR), we will inform you whether you are required to provide certain student information to us or if you have a choice in this and, where necessary, seek your consent for us to use that data and information in the way we intend.

How we use student information

We use this personal data:

- for the purposes of student assessment and to confirm the identity of prospective students and their parents;
- to provide education services (including Special Educational Needs (SEN)), career services, and extra-curricular activities to students; monitoring students' progress and educational needs; and maintaining relationships with alumni and the school community;
- for the purposes of management planning and forecasting, research and statistical analysis, and to enable the relevant authorities to monitor the school's performance;
- to give and receive information and references about past, current and prospective students, including relating to outstanding fees or payment history, to/from any educational institution that the student attended or where it is proposed they attend;
- to enable students to take part in national or other assessments, and to publish the results of public examinations or other achievements of students at the school;
- to safeguard students' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency or accident, including by disclosing details of an individual's medical condition where it is in the individual's interests to do so, for example for medical advice, insurance purposes or to organizers of school trips;
- to monitor (as appropriate) use of the school's IT and communications systems in accordance with the school's Online Safety Policy; to make use of photographic images of students for identification purposes and in school publications, on the school website and (where appropriate) on the school's social media channels, where parental permission has been given, and in accordance with the school's Online Safety Policy. We avoid naming students alongside externally published images unless clearly justified and permitted.
- for security purposes, and for regulatory and legal purposes (for example child protection and health and safety) and to comply with its legal obligations; and
- where otherwise reasonably necessary for the school's purposes, including to obtain appropriate professional advice and insurance for the school.

We may keep details of your address when you leave the school so we can send you news about the school and find out how your child is progressing. For graduates we may also pass your details onto our alumni section.

We may use information about you if we need this for historical research purposes or for statistical purposes, with such information being anonymized/pseudonymized.

We do not use personal data for automated decision making or for personal profiling.

Who we share student information with.

In accordance with our legal obligations, we may share information with local authorities, the Independent Schools Inspectorate and the Department for Education, for example, where we have any safeguarding concerns. Other instances where we may share information include:

- On occasion, we may need to share information with the police and other authorities, such as social services
- We may also need to share information with our legal advisers for the purpose of obtaining legal advice.
- Occasionally we may use consultants, experts and other advisors to assist the school in fulfilling its obligations and to help run the school properly. We might need to share your information with them if this is relevant to their work.
- If your child is not of British nationality we are required to ensure that your child has the right to study in the UK. We might have to provide information about you to UK Visas and Immigration to comply with our duties as a Student sponsor, including in relation to students sponsored under the Child Student route where applicable.
- We may share some information with our insurance company, for example, where there is a serious incident at the school.
- If you have unpaid fees while your child is at the school we may share information about this with other schools or educational establishments to which you intend to send your child.
- If your child leaves us to attend another school we may need to provide that school with information about you. For example, details of family circumstances for safeguarding reasons and the safeguarding file of the student.
- We may share information about you with others in your family, such as another parent or step-parent. For example, where this is part of our obligation to take care of your child, as part of our wider legal and regulatory obligations, or in connection with school fees.
- We may need to share information if there is an emergency, for example, if you are hurt whilst on school premises.
- For any international transfers of personal data, TASIS England will ensure that appropriate safeguards are in place. Where personal data is transferred internationally, we will do so in accordance with UK GDPR and ICO guidance.
- We rely on UK adequacy regulations where available or appropriate safeguards (e.g., the ICO's International Data Transfer Agreement (IDTA) or the UK Addendum to the EU SCCs), supported by transfer risk assessments and any supplementary measures required.

We do not share information about our students with anyone without consent unless the law and our policies require or allow us to do so. Where we use third-party processors, they act on our written instructions under **Article 28** contracts and are subject to appropriate confidentiality, security and audit provisions.

How we use parent information

We collect and process personal data relating to the parents/guardians of students at the school. This is for contractual purposes and/or to enable the payment of fees.

This personal data includes identifiers such as names, addresses, email addresses and telephone numbers, characteristics such as ethnic group and financial information such as credit card/banking details.

Upon accepting an offer of a place at the school for your child, you will have been offered an opportunity to consent or otherwise to our sharing your contact information with other parents in your child's cohort/class/grade. The purpose of this sharing of information is to facilitate the wider school community including the promotion of fundraising efforts. We will not share your contact information unless explicit consent has been given.

Consent for the sharing of your data in this way may be given or withdrawn by you at any time during your child's attendance at the school. If you wish to change your consent please contact Joshua Clark, Director of Student Recruitment and Admissions at jclark@tasisengland.org

We will not share information about you with third parties without your consent unless the law or our policies require or allow us to do so.

We are required, by law to pass on some of this personal data to:

- the local authority (Surrey)

- the Department for Education (DfE)

The lawful basis on which we use this information
We process this information under a number of Articles of the UK GDPR, including but not limited to**:**

Article 6 processing is carried out for at least one of the following bases:

- You have provided consent for us to process your personal data for one or more specific purposes;
- Processing is necessary for the performance of a contract to which you are a party or in order to take steps at your request to enter into a contract;
- Processing is necessary for compliance with a legal obligation to which the school is subject;
- Processing is necessary to protect the vital interests of you or another natural person;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the school;
- Processing is necessary for the pursuit of legitimate interests pursued by the school or by a third party, except where these interests are overridden by your interests or fundamental rights and freedoms, in particular where you, as the data subject, are a child.

Consent: Where the school processes data with consent (for example, to publish photographs of children or to send direct marketing emails) it will ensure that the consent is freely given, specific, informed and unambiguous**,** and the consent is recorded. Where consent is the lawful basis for processing your data, you can withdraw that consent at any time by contacting the school

Article 9 the processing of special categories of personal data for the purposes such as identifying a natural person, data concerning health or revealing racial or ethnic origin.

Storing student and parent information
We hold student data in accordance with our Data Protection and Records Retention Policies, which can be accessed on our website.

We keep your information for as long as we need to in order to educate and look after your child. We will keep some information after your child has left the school.

In exceptional circumstances we may keep your information for a longer time than usual, but we would only do so if we had a good reason and only if we are allowed to do so under data protection law and regulations.

We may keep information about you indefinitely for historical, research or statistical purposes. For example, if we consider the information might be useful if someone wanted to write a book about the school.

Sending information to other countries
We may send your information to other countries outside the UK, where:

- we store information on computer servers based overseas; or
- we communicate with you or your child when you are overseas (for example, during the summer holidays if you live in a different country).
- we share your personal data with third party service providers in order to achieve the processing purpose. In these cases, we will ensure that adequate data sharing agreements are in place with those third parties as described in our Data Protection Policy.
- We only transfer personal data internationally where permitted by UK law, using adequacy or appropriate safeguards (IDTA/UK Addendum). We keep records of transfer assessments and contracts.

Rights of parents and students

UK GDPR gives you a number of rights regarding your personal data and information. Some of these are new rights under UK GDPR whilst others build on your existing rights. Your rights are as follows:

- if information is incorrect, you can ask us to correct it;
- you can also ask what information we hold about you and be provided with a copy;
- you can ask us to delete the information that we hold about you in certain circumstances, although the consequences of such a request could include us not being able to execute the purpose for which we collected and are processing the data.
- you can ask us to send you, or another organisation, certain types of information about you in a format that can be read by computer;
- you can restrict our use of information about you in some cases. For example, if you tell us that the information is inaccurate, we can only use it for limited purposes while we check its accuracy;
- you can prevent us using personal data and information for the purposes of marketing.

If you have provided consent for the processing of your data you have the right (in certain circumstances) to withdraw that consent at any time, which will not affect the lawfulness of the processing before your consent was withdrawn. The giving and withdrawing of consent are subject to the person's age and capacity.

To make a request for personal data (a Data Subject Access Request, SAR), please refer to Appendix 4 of this policy.

Further information

Like other organisations we need to keep your information safe, up to date, only use it for what we said we would, destroy it when we no longer need it and most importantly - treat the information we get fairly. This notice is to explain how we use your personal information.

Please contact us if:

- you object to us using your information for marketing purposes e.g., to send you information about school events. We will stop using your information for marketing purposes if you tell us not to;
- you would like us to update the information we hold about you; or
- you would prefer that certain information is kept confidential.

If you have a concern about the way we are collecting or using your personal data, you have the right to make a data protection complaint to the school under section 164A of the Data Protection Act 2018 (see the 'Data Protection Complaints' section of this policy); we will acknowledge it within 30 days and tell you the outcome without undue delay. We ask that you raise your concern with us in the first instance: please contact our Data Protection Officer, David Harris at dharris@tasisengland.org

Alternatively, please visit the Information Commissioner's Office: https://ico.org.uk/concerns/ if you believe that we have not complied with the requirements of the UK GDPR with regard to your personal data.

If you require more information about how the DfE store and use your personal data, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data.

Appendix 2 – Privacy Notice for Staff and Faculty

Introduction

As your employer, the school needs to keep and process information about you for normal employment purposes. The information we hold, and process will be used for our management and administrative use only. We will keep and use it to enable us to run the school and manage our relationship with you effectively, lawfully and appropriately, during the recruitment process, whilst you are working for us, at the time when your employment ends and after you have left. This includes using information to enable us to comply with the employment contract, to comply with any legal requirements including the safeguarding of our students, pursue the legitimate interests of the school, and protect our legal position in the event of legal proceedings. If you do not provide this information, we may be unable, in some circumstances, to comply with our obligations and we will tell you about the implications of that decision.

Much of the information we hold will have been provided by you, but some may come from other internal sources, such as your manager, or in some cases, external sources, such as referees during your recruitment.

The following are examples of information and data that is personal to you, that we typically require and hold:

- Application form submitted at initiation of recruitment process.
- Proof of identification (such as copy of passport photo page).
- DBS checks.
- References as provided as part of the recruitment process.
- Personal information (such as name, employee or teacher number, national insurance number);
- Qualifications and experience (and, where relevant, subjects taught).
- Contract information (such as start dates, hours worked, post, roles and salary information as well as any amendments).
- Special categories of data including characteristics information such as gender, age, ethnic group and health.
- Attendance and absence information (such as number of absences and reasons).
- Medical information and, where necessary, information relating to your health, which could include reasons for absence and GP reports and notes. This information will be used in order to comply with our health and safety and occupational health obligations as well as, where appropriate, the provision of employment-related benefits (such as pensions and life assurance).
- Records relating to your career history, such as training records, appraisals, other performance measures and, where appropriate, disciplinary and grievance records.
- Payroll-related information (such as personal bank details for salary and expenses payments).
- Photographs: We collect photographic images of staff and faculty members, which we use for purposes of identification.
- CCTV: images of staff, faculty members, parents, students and other visitors to the school will be captured by our CCTV system which monitors public areas including the main entrance used by visitors, the pedestrian and vehicle gates, and the entrances to all other school buildings.
- In addition, we monitor computer [and telephone/mobile telephone] use, as detailed in our Online Safety Policy and Faculty and Staff Code of Conduct and Handbook.

You will inevitably be referred to in many school documents and records, which are produced by you and/or your colleagues in the course of carrying out your duties (such as telephone lists and staff profiles).

Why we collect and use this information

We control and process personal information to enable us to provide education and training conducted outside the state education system, welfare and educational support services, to administer school property and library services, to maintain our own accounts and records, for administration in connection with boarding and the organisation of alumni associations and events, for fundraising purposes and to support and manage our staff and faculty. Our

processing also includes the use of CCTV to maintain the security of the premises and for preventing and investigating crime.

We use school workforce data to:

- enable the development of a comprehensive picture of staff and faculty and how they are deployed;
- inform the development of recruitment and retention policies;
- enable individuals to be paid and receive relevant benefits;
- ensure the school's compliance with relevant statutory requirements

The lawful basis on which we process this information

We process this information under a number of Articles of the UK GDPR, including but not limited to**:**

Article 6 processing is carried out for at least one of the following bases:

- You have provided consent for us to process your personal data for one or more specific purposes. Where consent is the lawful basis for processing your data, you can withdraw that consent at any time by contacting the school;
- Processing is necessary for the performance of a contract to which you are a party or in order to take steps at your request to enter into a contract;
- Processing is necessary for compliance with a legal obligation to which the school is subject;
- Processing is necessary to protect the vital interests of you or another natural person;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the school;
- Processing is necessary for the pursuit of legitimate interests pursued by the school or by a third party, except where these interests are overridden by your interests or fundamental rights and freedoms, in particular where you, as the data subject, are a child.

Consent: Where the school processes data with consent (for example, to publish photographs of you on the school website) it will ensure that the consent is freely given, specific, informed and unambiguous**,** and the consent is recorded. Where consent is the lawful basis for processing your data, you can withdraw that consent at any time by contacting the school

Article 9: we rely on appropriate conditions for processing special category data (e.g., employment, social security and social protection law; vital interests; substantial public interest including safeguarding; legal claims; occupational health).

Collecting this information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are **required** to provide certain school workforce information to us, or if you have a choice in this, and we will do so before you submit it.

Storing this information

We hold your personal data in accordance with our Data Protection and Records Retention Policies, and we keep your information for as long as we need to in order to fulfill legal and contractual obligations. Some of these obligations may mean that we keep this information after your employment with the school has ended.

Who we share this information with

We routinely share this information with:

- Our **local authority (Surrey)** - We may be required to share information about our workforce members with our local authority (LA) or the DfE where a specific legal obligation or lawful request applies. The School Workforce Census duty under the Education (Supply of Information about the School Workforce) (England) Regulations 2007

applies to maintained schools and does not generally extend to privately funded independent schools.

- The **Department for Education** (DfE) - We share personal data with the DfE on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment of educational attainment. To find out more about the data collection requirements placed on us by the DfE including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

We will only disclose information about you to third parties if we are legally obliged to do so or where we need to comply with our contractual duties to you, for instance we may need to pass on certain information to pension or health insurance schemes.

We may transfer information about you to other group companies for purposes connected with your employment or the management of the school's business.

Where we use third-party processors, they act on our written instructions under Article 28 contracts and are subject to appropriate confidentiality, security and audit provisions.

In limited and necessary circumstances, your information may be transferred outside of the UK or to an international organisation to hold and process the personal data of you and your colleagues (such as our use of on-line databases to manage records). We have in place safeguards to ensure the security of your data, as described in our Data Protection Policy. Where we transfer personal data internationally, we rely on UK adequacy or appropriate safeguards (IDTA/UK Addendum), and we retain transfer risk assessments and contractual safeguards.

We do not share information about workforce members with anyone without your consent unless the law and our policies require or allow us to do so.

We do not use personal data for automated decision-making (including profiling).

Your rights

UK GDPR gives you a number of rights regarding your personal data and information. Some of these are new rights under UK GDPR whilst others build on your existing rights. Your rights are as follows:

- if information is incorrect, you can ask us to correct it;
- you can also ask what information we hold about you and be provided with a copy;
- you can ask us to delete the information that we hold about you in certain circumstances, although the consequences of such a request could include us not being able to execute the purpose for which we collected and are processing the data and our lawful basis for processing may override such a requests, such as a contractual or legal obligation.
- you can ask us to send you, or another organisation, certain types of information about you in a format that can be read by computer;
- our use of information about you may be restricted in some cases. For example, if you tell us that the information is inaccurate, we can only use it for limited purposes while we check its accuracy;
- prevent us using personal data and information for the purposes of marketing.

If you have provided consent for the processing of your data you have the right (in certain circumstances) to withdraw that consent at any time, which will not affect the lawfulness of the processing before your consent was withdrawn. To make a request for your personal data and information, contact Bryan Nixon, Head of School at bnixon@tasisengland.org.

Further information

Like other organisations we need to keep your information safe, up to date, only use it for what we said we would, destroy it when we no longer need it and most importantly - treat the information we get fairly.

This notice is to explain how we use your personal information. Please contact us if:

- you would like us to update the information we hold about you; or
- you would prefer that certain information is kept confidential.

If you have a concern about the way we are collecting or using your personal data, you have the right to make a data protection complaint to the school under section 164A of the Data Protection Act 2018 (see the 'Data Protection Complaints' section of this policy); we will acknowledge it within 30 days and tell you the outcome without undue delay. We ask that you raise your concern with us in the first instance: please contact our Data Protection Officer, David Harris at dharris@tasisengland.org

Alternatively, please visit the Information Commissioner's Office: https://ico.org.uk/concerns/ if you believe that we have not complied with the requirements of the UK GDPR with regard to your personal data.

If you require more information about how the DfE store and use your personal data, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data.

Appendix 3 – Privacy Notice for Visitors

Privacy Notice for Visitors

As a visitor to the school, we need to hold certain information about you (your 'Personal Data'). This notice will inform you about the data we hold about you and how we use it.

You have certain rights, including how to get a copy of your data, how to get it corrected or deleted, and how to complain. These rights are set out in more detail below.

Please note that on occasions we may process 'special categories' of information about you. Examples of this information include the revealing of racial or ethnic origin; the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person or data concerning health.

Your rights in relation to your personal data

You have a number of rights over your personal information, which are:

- if information is incorrect, you can ask us to correct it;
- you can also ask what information we hold about you and be provided with a copy;
- you can ask us to delete the information that we hold about you in certain circumstances, although the consequences of such a request could include us not being able to execute the purpose for which we collected and are processing the data and our lawful basis for processing may override such a requests, such as a contractual or legal obligation;
- you can ask us to send you, or another organisation, certain types of information about you in a format that can be read by computer;
- our use of information about you may be restricted in some cases. For example, if you tell us that the information is inaccurate, we can only use it for limited purposes while we check its accuracy; and
- prevent us using personal data and information for the purposes of marketing.

If you have provided consent for the processing of your data you have the right (in certain circumstances) to withdraw that consent at any time, which will not affect the lawfulness of the processing before your consent was withdrawn.

What personal data do we hold?

As part of your visit to the school we store and use your personal details and information about your visit for the purposes of managing and operating the school. We use CCTV throughout the school for the purposes of crime prevention, security and health and safety and, accordingly, will capture imagery of visitors to the school.

The following points give you an indication of the personally identifiable data we could ask for and hold about you, depending on your reason for visiting the school and how long/how often you may be visiting us:

- Contact details, contact preferences, date of birth, identification documents, car registrations
- Safeguarding information
- Photographs
- CCTV images captured in school

Why we use this data

We use this data to:

- Protect student welfare
- Protect the school buildings and site
- Protect the safety of visitors to our school
- Assess the quality of our services
- Comply with the law regarding data sharing

What is the legal basis on which we collect and use your personal data?
Except in the circumstances highlighted in the bullet points below, we process this information on the basis of our legitimate interests:

- We have a legitimate interest in wishing to interact with you to manage and operate our school effectively and to ensure that the school is safe and secure for all persons visiting; and
- to be able to do so, we need to understand details of who is on site and to be able to communicate with them.

Where we are required by law to hold certain records, then we collect and hold those records to comply with that legal obligation. Less commonly, we may also process visitors' personal data in situations where:

- we have obtained consent to use it in a certain way; or
- we need to protect the individual's vital interests (or someone else's interests).

Where we have obtained consent to use visitors' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent and explain how consent can be withdrawn. Some of the reasons listed above for collecting and using visitors' personal data overlap, and there may be several grounds that justify our use of this data.

How do we share your personal data?
Where we transfer personal data to a country or territory outside the UK, we will do so in accordance with data protection law. We do not share information about visitors with any third party without consent unless the law and our policies allow us to do so. Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about visitors with:

- The Department for Education – to meet our legal obligations;
- School Inspectors – to demonstrate our effective management of the school;
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as our visitor management system;
- Central and local government – to meet our legal obligations;
- Professional advisers and consultants – to ensure the smooth running of the school; and
- Police forces, courts, tribunals – as and when needed, to meet any legal obligations and to ensure the safety of the whole school community.

How long do we keep your personal data?
We maintain personal data in accordance with our Data Protection and Records Retention policies, which is available on our website.

Who can you contact?
Like other organisations we need to keep your information safe, up to date, only use it for what we said we would, destroy it when we no longer need it and, most importantly, treat the information we get fairly and lawfully.
This notice is to explain how we use your personal information. Please contact us if:

- you would like us to update the information we hold about you; or
- you would prefer that certain information is kept confidential.

If you have a concern about the way we are collecting or using your personal data, you have the right to make a data protection complaint to the school under section 164A of the Data Protection Act 2018 (see the 'Data Protection Complaints' section of this policy); we will acknowledge it within 30 days and tell you the outcome without undue delay. We ask that you raise your concern with us in the first instance: please contact our Data Protection Officer, David Harris at dharris@tasisengland.org

Alternatively, please visit the Information Commissioner's Office: https://ico.org.uk/concerns/ if you believe that we have not complied with the requirements of the UK GDPR with regard to your personal data.

If you require more information about how the DfE store and use your personal data, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data.

Appendix 4 –Data Subject Access Request (SAR)

Rights of access to information
There are two distinct rights of access to information held by schools about students.

1. Under the UK General Data Protection Regulation (UK GDPR) any individual has the right to make a request to access the personal information held about them.

2. The right of those entitled to have access to curricular and educational records as defined within the Education (Pupil Information) (England) Regulations 2005 (which apply to maintained schools; at TASIS England such records are provided under the UK GDPR subject access regime)

These procedures relate to subject access requests made under the UK GDPR.

Requests for information can be made verbally or in writing, which includes email, using the form below.

Responding to a SAR
If the initial request does not clearly identify the information required, then further enquiries will be made.
Before we process a SAR or release information to you, we need to be confident of your identity so we may ask you for additional information in order to verify it, for example:

- Passport
- Driving license
- Utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

This list is not exhaustive.

Any individual has the right of access to information held about them. However, with children this is dependent upon their age (and level of understanding) and the nature of the request. The Head of School should discuss the request with the child and take their views into account when making a decision. Whether a child can exercise their own access rights depends on their age and level of understanding. As a guide, children of around 12 and over are often considered capable, but this will be assessed case by case. Where a child is not deemed capable, an individual with parental responsibility may act on their behalf.

The response time for SARs, once officially received, is one month from the day of receipt (calendar days, not working or school days, irrespective of school holiday periods). UK GDPR allows exemptions as to the provision of some information; therefore, all information will be reviewed prior to disclosure. As stated in section 9 above, complex or numerous requests may take longer to process. If this is the case the school will inform the individual of this within 1 month and explain the reasons why an extension is necessary

Third party information is that which has been provided by another, such as the police, local authority, a health care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need for us to adhere to the one-month statutory timescale.

Any information which may cause serious harm to the physical or mental health or emotional condition of the student, or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

If there are concerns over the disclosure of information, then additional advice should be sought.

Where redaction (information which has been blanked out or removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what information was redacted and the reasons why.

Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

Information can be handed over to the data subject at the school, with a member of staff on hand to help and explain matters if requested or provided at face-to-face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used, then registered/recorded mail must be used.

Data Subjects may ask us to rectify, erase or restrict processing of their personal data. There may be circumstances, such as a legal or regulatory need to retain data, where erasure may not be possible.

Complaints

A data protection complaint — including any complaint about the handling of a subject access request — may be made to the school as data controller under section 164A of the Data Protection Act 2018 by contacting the Data Protection Officer, David Harris (dharris@tasisengland.org); the school will acknowledge it within 30 days and inform the complainant of the outcome without undue delay (see the 'Data Protection Complaints' section of this policy). Complaints about this procedure should be made to the Head of School who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's Complaint's Policy.

Complaints which are not appropriate to be dealt with through the school's complaint procedure or cannot be resolved by the school can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Contacts

If you have any queries or concerns regarding this procedure then please contact either Bryan Nixon, Head of School at bnixon@tasisengland.org or Darren Singh-MacPherson, Director of Inclusion, Wellbeing and Compliance at dsinghmacpherson@tasisengland.org.

You may also contact the school's Data Protection Officer, David Harris at dharris@tasisengland.org.

Further advice and information can be obtained from the Information Commissioner's Office, http://www.ico.gov.uk.

SUBJECT ACCESS REQUEST FORM

If you want a copy of any personal data TASIS England holds about you, please complete this form and either email or post it the addresses below.

The information you supply in this form will only be used for the purposes of identifying the personal data you are requesting and enabling us to respond to your request.

Please send your completed form and proof of identity to: Bryan Nixon, Head of School, Coldharbour Ln, Thorpe TW20 8TE - bnixon@tasisengland.org.

Section 1: Details of the person requesting information

Your full name:	
Your address:	
Your telephone number:	
Your email address:	

Section 2: Are you the data subject?

Please tick the appropriate box.

☐ **YES**: I am the data subject. I enclose proof of my identity (see below).

Please proceed to Section 4, or

☐ **NO**: I am acting on behalf of the data subject. I have enclosed the data subject's written authority and proof of the data subject's identity and my own identity (see below).

Please proceed to **Section 3.**
To ensure that we are releasing data to the right person we require you to provide us with proof of your identity and of your address. Please supply us with a photocopy or scanned image (do not send the originals) of one of both of the following two categories:

1) **Proof of Identity.** We need one of the following: passport, photo driving license, national identity card or birth certificate.
2) **Proof of Address.** We need one of the following: utility bill, bank statement, credit card statement (no more than 3 months old), current driving license or local authority council tax bill.

If we are not satisfied you are who you claim to be, we reserve the right to request further proof or refuse to grant your request.

Section 3: Details of the data subject

Full name:	
Address:	
Telephone number:	
Email address:	

Section 4: What information are you seeking?

Please describe the information you are seeking. Please provide any relevant details you think will help us to identify the information you require.

……
……
……
……
……
……
……

Please note that if the information you request reveals details directly or indirectly about another person, we will have to seek the consent of that person before we can let you see that information. In certain circumstances, where disclosure would adversely affect the rights and freedoms of others, we may not be able to disclose the information to you, in which case you will be informed promptly and given full reasons for that decision.

While in most cases we will be happy to provide you with copies of the information you request, we nevertheless reserve the right, in accordance with Article 12 of the UK GDPR to charge a fee or refuse the request if it is considered to be 'manifestly unfounded or excessive'. However, we will make every effort to provide you with a satisfactory form of access or summary of information if suitable.

Section 5: Information about the data collection and processing

If you want information about any of the following, please tick the boxes:

☐ Why we are processing your personal data
☐ To whom your personal data are disclosed
☐ The source of your personal data

Section 6: Disclosure of CCTV images

If the information you seek is in the form of video images captured by our CCTV security cameras, would you be satisfied with viewing these images?

☐ **YES**
☐ **NO**

Section 7: Declaration

Please note that any attempt to mislead may result in legal action.

I confirm that I have read and understood the terms of this Data Subject Access Request Form and certify that the information given in this application to TASIS England is true. I understand that it is necessary for TASIS England to confirm my / the data subject's identity and it may be necessary to obtain more detailed information in order to locate the correct personal data.

…….. ……

Signature Date

Attachments:

I am enclosing the following copies as proof of identity:

……
……
……
……

Note: Information about personal data we collect, how we use it and with whom we share it can be found in our Data Protection Policy, available on our website.