# LONDON ENTERPRISE ACADEMY (LEA)

# PRIVACY POLICY AND PRIVACY NOTICES

*Data Protection, Privacy and Information Rights*

| | |
|---|---|
| **Document Reference** | LEA-DP-PRIV-001 |
| **Version** | 1.0 |
| **Effective Date** | 17 September 2026 |
| **Review Date** | 17 September 2027, or earlier if legislation/guidance changes |
| **Document Owner** | London Enterprise Academy |
| **Data Protection Officer** | Judicium Consulting Limited – dataservices@judicium.com |

## 1. Purpose

This Privacy Policy explains how London Enterprise Academy (LEA) collects, uses, stores, protects and shares personal data and how individuals can exercise their data protection rights. It provides the overarching framework for the privacy notices used by LEA and should be read alongside the applicable privacy notice in the appendices.

The policy has been developed from the privacy notice documents supplied for pupils and parents, staff, visitors and contractors, job applicants and application forms. Those notices are retained as appendices so that the audience-specific information remains accessible and operational.

## 2. Scope

This policy applies to personal data processed by or on behalf of LEA and covers pupils, parents/carers, staff, workers, contractors, visitors, job applicants and other individuals whose personal data LEA processes.

## 3. Data Protection Framework

LEA will process personal data in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other applicable data protection, education, safeguarding and information governance requirements. The supplied privacy notices also refer to the Data (Use and Access) Act 2025 and explain that it amended the UK GDPR and Data Protection Act 2018.

LEA will keep this policy and its notices under review and will update them where there are material changes to legislation, regulatory requirements, LEA processing activities or relevant guidance.

## 4. Key Data Protection Principles

- Lawfulness, fairness and transparency – personal data will be processed lawfully, fairly and transparently.
- Purpose limitation – data will be collected for specified, explicit and legitimate purposes and not used incompatibly with those purposes.
- Data minimisation – LEA will collect and use only information that is adequate, relevant and necessary.
- Accuracy – reasonable steps will be taken to keep personal data accurate and up to date.
- Storage limitation – information will not be retained for longer than necessary, subject to legal, safeguarding, accounting and other requirements.
- Security and confidentiality – appropriate technical and organisational measures will protect information against loss, unauthorised access, alteration, disclosure or destruction.
- Accountability – LEA will be able to demonstrate compliance through policies, procedures, records, training, contracts, risk assessments and appropriate documentation.

## 5. Data Controller and Governance

London Enterprise Academy is the data controller for the personal data it determines the purposes and means of processing. LEA will maintain appropriate governance arrangements and will ensure that responsibilities for data protection are understood by staff and relevant third parties.

The Data Protection Officer identified in the supplied notices is Judicium Consulting Limited, 5th Floor, 98 Theobalds Road, London, WC1X 8WB, dataservices@judicium.com. The supplied notices also identify the DPO as the escalation point for unresolved data protection queries.

## 6. Categories of Personal Data

Depending on the individual and purpose, LEA may process identification and contact information, emergency contact and family information, educational and assessment information, attendance and behaviour information, employment and payroll information, recruitment information, safeguarding and welfare information, CCTV and photographic information, IT and communications information, and information required for legal, regulatory and operational purposes.

The supplied notices identify special category data that may be processed where legally permitted and appropriately justified, including health information, racial or ethnic origin, religious or philosophical beliefs, sexual orientation, trade union membership, special educational needs information and, where applicable, biometric data. Criminal conviction and offence information is subject to additional legal restrictions.

## 7. Sources of Personal Data

LEA may obtain personal data directly from the individual and, where appropriate, from parents/carers, referees, previous employers or education providers, professional bodies, the Home Office, DBS, the Local Authority, health or occupational health professionals, service providers, LEA systems, CCTV, access control and IT/communications systems, and other lawful sources identified in the relevant privacy notice.

## 8. Lawful Bases for Processing

LEA will identify an appropriate lawful basis for each processing activity. Depending on the circumstances, this may include consent, performance of a contract or steps before entering a contract, compliance with a legal obligation, protection of vital interests, performance of a task in the public interest or in the exercise of official authority, and legitimate interests where applicable.

Consent will not be treated as the default lawful basis where another lawful basis is more appropriate. Where processing relies on consent, LEA will provide an appropriate mechanism for withdrawal, while recognising that withdrawal does not retrospectively make lawful processing unlawful and does not prevent processing where another lawful basis applies.

## 9. Special Category and Criminal Offence Data

Special category data will receive enhanced protection and will only be processed where an applicable Article 9 condition and, where required, a corresponding condition under the Data Protection Act 2018 are satisfied. LEA will maintain appropriate safeguards and policies where required.

Criminal conviction and offence data will only be processed where legally permitted and where the processing is appropriate for the relevant purpose. The supplied recruitment and visitor notices specifically identify DBS and safer recruitment-related processing.

## 10. Purposes of Processing

- Providing education, teaching, assessment, pastoral and support services.
- Safeguarding pupils and staff and supporting health, welfare and safety.
- Managing attendance, behaviour, educational progress and post-16 provision.
- Meeting statutory education, regulatory, funding, examination and reporting requirements.
- Recruitment, vetting, employment administration, payroll, pensions, training, performance and workforce management.
- Managing visitors, contractors, access arrangements, site security and health and safety.

- Managing applications, shortlisting, interviews, references and pre-employment checks.
- Operating IT, communications, access control and CCTV systems securely.
- Preventing and detecting fraud and crime and defending or pursuing legal claims.
- Obtaining professional advice, insurance and other services required for LEA's lawful operation.

## 11. Data Sharing

LEA may share personal data where there is a lawful basis and where sharing is necessary and proportionate. The supplied notices identify recipients including the Department for Education, Ofsted, Local Authority, NHS, social care/welfare services, police and other law enforcement bodies, DBS, LADO, professional advisers, HR and IT providers, training providers, examination or regulatory bodies, other schools or education providers, recruitment agencies and relevant software/service providers.

Information will be shared securely and, where appropriate and practicable, anonymised or pseudonymised. Third parties processing data on LEA's behalf will be subject to appropriate contractual and confidentiality requirements.

Where an individual has objected to a particular disclosure, LEA will consider that objection in accordance with applicable law. The pupil/parent notice recognises that compelling reasons, safeguarding/health and safety considerations or legal requirements may mean that information must still be shared.

## 12. International Transfers

Where personal data is transferred outside the UK, LEA will ensure that the transfer is made in accordance with applicable UK data protection requirements and that an appropriate level of protection and lawful transfer mechanism is in place.

## 13. Security and Confidentiality

LEA will use appropriate technical and organisational measures to protect personal data. Access will be limited to people who have a legitimate business, educational, safeguarding or legal need to know. Security arrangements include appropriate access controls, secure systems, confidentiality requirements and procedures for responding to data breaches.

Staff and contractors must not disclose personal data except where authorised and must follow LEA's information security, acceptable use, data breach and confidentiality procedures.

## 14. Retention and Disposal

LEA will retain personal data only for as long as necessary for the purposes for which it is processed, subject to statutory, safeguarding, legal, accounting, regulatory and claims-related requirements. Detailed retention periods will be set out in LEA's Data Retention Policy and associated retention schedules.

When information is no longer required, it will be securely destroyed, deleted or otherwise disposed of in accordance with the applicable retention schedule and security requirements.

## 15. Data Subject Rights

Subject to legal exemptions and the circumstances of the processing, individuals may have rights including access to their personal data, rectification of inaccurate data, erasure, restriction of processing, objection and data portability. The right to withdraw consent applies where consent is the lawful basis.

Requests should be directed to LEA using the contact arrangements in the relevant privacy notice. LEA may need to verify identity before responding.

## 16. Automated Decision-Making and AI

The supplied notices state that individuals will not be subject to significant automated decision-making without an appropriate lawful basis, required condition and safeguards. Where significant automated decision-making is introduced, LEA will provide the information required by law and implement appropriate safeguards, including meaningful human review where applicable.

Any new AI or automated processing that uses personal data must be assessed before implementation, including consideration of lawful basis, transparency, security, data minimisation, accuracy, fairness, risks to individuals and whether a Data Protection Impact Assessment is required.

## 17. Children's Data

LEA recognises that pupils require particular care and transparency when their personal data is processed. Information will be communicated in a form that is understandable and age-appropriate where appropriate. The pupil and parent notices explain the types of information processed, why it is required, who it may be shared with and how individuals can raise concerns.

## 18. Recruitment and Online Searches

The job applicant notice identifies recruitment processing including references, qualifications, right-to-work information, DBS/criminal record information, health information and pre-employment checks. It also identifies online searches for data as part of pre-employment checks. Where LEA undertakes such searches, it will do so lawfully, proportionately and in accordance with its recruitment procedures and the information provided to applicants.

The short-form application notice is intended to accompany application forms and expressly states that it does not replace the full privacy notice.

## 19. Visitors and Contractors

LEA may process visitor and contractor information including identity and contact details, visit details, vehicle registration, access arrangements, photographs used for identification, CCTV and, where necessary and lawful, DBS or other criminal records information. The supplied visitor notice identifies site safety, safeguarding, security, administration and health and safety as purposes.

## 20. Personal Data Breaches

Any actual or suspected loss, unauthorised disclosure, unauthorised access, accidental destruction or other personal data breach must be reported immediately through LEA's data breach procedure. LEA will assess incidents promptly, contain and investigate them, document decisions and make any required notification to the Information Commissioner's Office or affected individuals within applicable timescales.

## 21. Training and Responsibilities

- The Principal and senior leadership team are responsible for ensuring that data protection is embedded in LEA's governance and operations.

- The Data Protection Officer provides specialist advice, oversight and escalation support.
- All staff must process personal data only for authorised purposes and follow LEA policies and procedures.
- Managers must ensure that staff understand the data they handle and that access is proportionate to their role.
- Contractors and third-party processors must comply with contractual data protection requirements.
- Individuals must report suspected breaches, inappropriate access or other data protection concerns promptly.

## 22. Complaints and Escalation

Individuals should first raise concerns with LEA using the contact details published in the relevant privacy notice. The supplied notices provide for acknowledgement and investigation without undue delay. If the concern remains unresolved, individuals may contact LEA's Data Protection Officer, Judicium Consulting Limited.

Individuals also have the right to complain to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection matters.

## 23. Related Policies and Documents (available on the website or staff shared drive – Policies)

- Data Protection Policy / this Privacy Policy
- Data Retention Policy
- Data Breach Policy
- Information Security Policy
- Acceptable Use / IT Security procedures
- Safeguarding and Child Protection Policy
- Biometrics Policy, where biometric processing is used
- Records Management and information governance procedures
- Relevant recruitment, CCTV and monitoring policies

## 24. Review and Approval

This policy will be reviewed at least annually and sooner where there are material changes to legislation, regulatory guidance, LEA processing activities, systems, contracts or risk. The audience-specific privacy notices in the appendices must also be reviewed when the underlying processing changes.

# Appendix 1 – Privacy Notice for Pupils and Parents

## Document Owner and Approval

[INSERT NAME] is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with School's policy review schedule.

A current version of this document is available to all members of staff [insert shared policy location].

Signature: Date:

## Change History Record

This privacy notice describes how we collect and use personal information about pupils, in accordance with the UK General Data Protection Regulation (UK GDPR), section 537A of the Education Act 1996 and section 83 of the Children Act 1989.

Following Brexit, Regulation (EU) 2016/679, General Data Protection Regulation (GDPR) was incorporated into UK law as retained EU law and is now known as the UK GDPR. The UK GDPR operates alongside the Data Protection Act 2018, which supplements it by setting out additional provisions on matters such as the processing of personal data is specific sectors, exemptions, the powers of the Information Commissioner, and enforcement. The Data (Use and Access) Act 2025 further amends both the UK GDPR and Data Protection Act 2018 to modernise UK data protection rules and clarify certain rights and obligations. The GDPR continues to apply within the EU and to organisations that process personal data of individuals located in the EU.

This notice applies to all pupils and parents.

### Who Collects This Information

[NAME OF SCHOOL] is a "data controller" of personal data and gathers and uses certain information about pupils and parents. This means that we are responsible for deciding how we hold and use personal information about pupils and parents. Under data protection legislation, we are required to notify you of the information contained in this privacy notice.

This notice does not form part of any contract to provide services and we may update this notice at any time.

It is important that you read this notice with any other policies mentioned within this privacy notice, so that you are aware of how and why we are processing your information, what your rights are under data protection legislation and the procedures we take to protect your personal data.

### Data Protection Principles

We will comply with the data protection principles when gathering and using personal information, as set out in our data protection policy.

### Categories of Pupil Information We Collect, Process, Hold and Share

We may collect, store and use the following categories of personal information about you:

Personal information such as name, pupil number, date of birth, gender and contact information;

Emergency contact and family lifestyle information such as names, relationship, phone numbers and email addresses;

Characteristics (such as language, and free school meal eligibility);

Attendance details (such as sessions attended, number of absences and reasons for absence);

Performance and assessment information;

Behavioural information (including exclusions);

Images of pupils engaging in school activities, and images captured by the School's CCTV system;

Information about the use of our IT, communications and other systems, and other monitoring information;

Financial details;

Post 16 learning information;

Recordings of pupils and/or parents from the school's video conferencing platform;

[DETAILS]

We may also collect, store and use the following more sensitive types of personal information:

Information about your race or ethnicity, religious or philosophical beliefs

Information about your health, including any medical conditions and sickness records.

Special educational needs information;

[Biometric data]

**How We Collect this Information**

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. To comply with the UK GDPR, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your relationship with us.

**How and Why We Use Your Personal Information**

We will only use your personal information when the law allows us to do so. Most commonly, we will hold pupil data and use it for:

Pupil selection (and to confirm the identity of prospective pupils and their parents);

Providing education services and extra-curricular activities to pupils, and monitoring pupils' progress and educational needs;

Informing decisions such as the funding of schools;

Assessing performance and to set targets for schools;

Safeguarding pupils' welfare and providing appropriate pastoral (and where necessary medical) care;

Support teaching and learning;

Giving and receive information and references about past, current and prospective pupils, and to provide references to potential employers of past pupils;

Managing internal policy and procedure;

Enabling pupils to take part in assessments, to publish the results of examinations and to record pupil achievements;

To carry out statistical analysis for diversity purposes;

Legal and regulatory purposes (for example child protection, diversity monitoring and health and safety) and to comply with legal obligations and duties of care;

Enabling relevant authorities to monitor the school's performance and to intervene or assist with incidents as appropriate;

Monitoring use of the school's IT and communications systems in accordance with the school's IT security policy;

Making use of photographic images of pupils in school publications, on the school website and on social media channels;

Security purposes, including CCTV; and

Where otherwise reasonably necessary for the school's purposes, including to obtain appropriate professional advice and insurance for the school.

To provide support to pupils after they leave the school

[DETAILS]

**The Lawful Bases on which we use this Information**

We will only use your information when the law allows us to. Most commonly, we will use your information in the following circumstances:

Consent: the individual has given clear consent to process their personal data for a specific purpose;

Contract: the processing is necessary for a contract with the individual;

Legal obligation: the processing is necessary to comply with the law (not including contractual obligations);

Vital interests: the processing is necessary to protect someone's life.

Public task: the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law; and

The Education Act 1996: for Departmental Censuses 3 times a year. More information can be found at: .

We mainly use pupils' personal data to comply with legal obligations and to perform tasks carried out in the public interest Please note that we may process information without knowledge or consent, where this is required or permitted by law.

**How we use particularly sensitive personal information**

Special categories of particularly sensitive personal information, such as information about your health, racial or ethnic origin, sexual orientation, or biometrics (as defined under UK GDPR as "special category data") require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

In limited circumstances, with your explicit written consent.

Where we need to carry out our legal obligations in line with our data protection policy.

For reasons of substantial public interest, such as for equal opportunities monitoring.

Where necessary to establish, exercise or defend legal claims;

Where necessary to protect your vital interests (or those of another person) and you are unable to consent.

**Sharing Data**

We may need to share your data with third parties where it is necessary. There are strict controls on who can see your information. We will not share your data if you have advised us that you do not want it shared unless we have compelling reasons to continue sharing it which override your rights and interests, it's the only way we can make sure you stay safe and healthy, or we are legally required to do so.

We share pupil information with:

the Department for Education (DfE) - on a statutory basis under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013;

Ofsted;

Other Schools that pupils have attended/will attend;

NHS;

Welfare services (such as social services);

Law enforcement officials such as police, HMRC;

Local Authority Designated Officer;

Professional advisors such as lawyers and consultants;

Support services (including insurance, IT support, information security);

Providers of learning software such as [e.g., Timetables Rockstar, Edukey] and

The Local Authority.

Youth support services – under section 507B of the Education Act 1996, to enable them to provide information regarding training and careers as part of the education or training of 13–19-year-olds;

other schools within the Federation/Trust;

The Department for Education request regular data sharing on pupil attendance to help support those vulnerable students and to assist with intervention strategies. Further information on how the Department for Education collects this data will be made available on the school website.

Information will be provided to those agencies securely and/or anonymised where possible.

The recipient of the information will be bound by confidentiality obligations, we require them to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the UK and the EU. If we do, you can expect a similar degree of protection in respect of your personal information.

**Youth Support Services**

*Pupils aged 13+*

Once our pupils reach the age of 13, we also pass pupil information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13–19-year-olds under section 507B of the Education Act 1996.

We must provide the pupils name, the parents name(s) and any further information relevant to the support services role.

This enables them to provide services as follows:

youth support services

careers advisers

A parent or guardian can request that only their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / pupil once he/she reaches the age 16.

*Pupils aged 16+*

We will also share certain information about pupils aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13–19-year-olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

post-16 education and training providers

youth support services

careers advisers

For more information about services for young people, please visit our local authority website.]

**Biometric Data**

At [name of school] we would like to use your information as part of an automated (i.e. electronically operated) recognition system. This is for the purposes of [specify what purpose is – e.g., catering, library access]. The information that we wish to use is referred to as 'biometric information'. This data will only be processed once we have obtained appropriate consent. For further information in relation to this, please see our Biometrics Policy.

**Automated Decision Making**

Automated decision making takes place when an electronic system uses personal information to make a decision without human intervention. We are required to ensure that appropriate safeguards are in place when using automated decision making for significant decisions and the circumstances in which we are permitted to use special category data (sensitive information) in automated decision making are limited.

You will not be subject to automated decision making for significant decisions unless we have a lawful basis, and a valid condition where required, for doing so and appropriate safeguards are in place. Appropriate safeguards include informing the relevant individuals about the automated decision making and their rights to request a human review, express their views, and contest the decision.

**Retention Periods**

Except as otherwise permitted or required by applicable law or regulation, the school only retains personal data for as long as necessary to fulfil the purposes they collected it for, as required to satisfy any legal, accounting or reporting obligations, or as necessary to resolve disputes.

Information about how we retain information can be found in our Data Retention Policy. This document can be found [LOCATION].

**Security**

We have put in place measures to protect the security of your information (i.e., against it being accidentally lost, used or accessed in an unauthorised way). In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know.

You can find further details of our security procedures within our Data Breach Policy and our Information Security Policy, which can be found [LOCATION].

It is important that the personal information we hold about you is accurate and current. Please keep us information if yours or your child's personal information changes while your child attends our school.

**The National Pupil Database**

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to .

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

conducting research or analysis

producing statistics

providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

who is requesting the data?

the purpose for which it is required

the level and sensitivity of data requested: and

the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit:

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:

To contact DfE:

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, [or be given access to your child's education record], contact [NAME].

**Your Rights of Access, Correction, Erasure and Restriction**

Under certain circumstances, by law you have the right to:

Access your personal information (commonly known as a "subject access request"). This allows you to receive a copy of the personal information we hold about you and to check we are lawfully processing it. You will not have to pay a fee to access your personal information. However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

Correction of the personal information we hold about you. This enables you to have any inaccurate information we hold about you corrected.

Erasure of your personal information. You can ask us to delete or remove personal data if there is no good reason for us continuing to process it.

Restriction of processing your personal information. You can ask us to suspend processing personal information about you in certain circumstances, for example, if you want us to establish its accuracy before processing it.

To object to processing in certain circumstances (for example for direct marketing purposes).

To transfer your personal information to another party.

If you want to exercise any of the above rights, please contact [NAME/EMAIL] in writing.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights).

**Right to Withdraw Consent**

In circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact [NAME/EMAIL]. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

**Contact**

If you would like to discuss anything within this privacy notice or have a concern about the way we are collecting or using your personal data, we request that you raise your concern with [NAME] in the first instance. We will acknowledge receipt of your complaint within 30 calendar days, and we will investigate and respond without undue delay. Further information about the way we handle data protection complaints can be found in our Data Protection Policy, available [HERE].

We have appointed a data protection officer (DPO) to oversee compliance with data protection and this privacy notice. If you have any questions about how we handle your personal information which cannot be resolved by [NAME], then you can contact the DPO on the details below:

Data Protection Officer: Judicium Consulting Limited

Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB

Email:

Web:

Should you remain dissatisfied with our response, you also have the right to make a complaint to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

**Changes to this Privacy Notice**

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

| Version | Description of Change | Date of Policy Release by Judicium |
|---|---|---|
| 1 | Initial Issue | 06.05.18 |
| 2 | Updated for UK GDPR and international transfers outside of the UK | 06.05.21 |
| 3 | Added reference to sharing data section about Department for Education request for regular attendance data collection | 18.02.22 |
| 4 | Added reference to Biometric Data. | 19.08.22 |
| 5 | Created a separate paragraph for collecting special category data. | 22.08.23 |
| 6 | Removed Craig Stilwell's name, included additional security information and Rights of Access, Correction, Erasure and Restriction | 29.08.24 |
| 7 | Changed Judicium's Address | 22.04.25 |
| 8 | Amendments to introduction, 'Automated Decision Making', and 'How to Raise a Concern' in line with amendments to UK GDPR by Data (Use and Access) Act 2025.<br><br>Removal of duplicated wording from 'How we use your Information'<br><br>Clarification of conditions for processing special category data.<br><br>Clarification re data sharing when there are compelling reasons to continue despite data subject 'opt out' added to 'Sharing Data'.<br><br>Removal of duplicate wording from 'Security' | 06.03.2026 |

# Appendix 2 – Privacy Notice for Pupils (Short Form)

## Document Owner and Approval

[INSERT NAME] is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with School's policy review schedule.

A current version of this document is available to all members of staff [insert shared policy location].

Signature: Date:

## Change History Record

This privacy notice is a short form and easily accessible privacy notice for pupils. It is generally aimed at pupils of primary school age but can also be adapted and used for secondary school pupils.

## What is Personal Data?

Personal data is information about you. This is information that could potentially identify you. This includes your name, your date of birth, your address and phone number.

## What Personal Data does School Collect?

Your information, including your name, address and date of birth;

Your school grades and records;

Safeguarding information;

Medical information;

Attendance records;

Photographs and CCTV;

Information about your homelife.

## Why does School need this Information?

We have a duty of care under the law to you. The law states that we need this information to know who is attending the school and to provide you with an education.

It is important for the school to keep you safe and hold this information to enable us to do this.

## Who does School Share Your Data With?

It is important for us to share some of this information with the police, the NHS and exam boards.

We must also share this information with the local authority.

We share information with other schools and colleges you may wish to attend.

## Where does School Keep this Data?

We keep this data within the school, in a large manner of ways. This could be in files under lock and key or on a computer with strong security.

## How long does the school keep this data for?

We often review our files to ensure we are only holding the documents we need. Once you leave the school, we may be required to keep some information about you.

**Any questions, please contact [NAME OF CONTACT WITHIN SCHOOL] or the school's data protection officer, Judicium Education at dataservices@judicium.com.**

| Version | Description of Change | Date of Policy Release by Judicium |
|---|---|---|
| 1 | Initial Issue | 29.09.20 |
| | | |
| | | |

# Appendix 3 – Privacy Notice for Staff

## Document Owner and Approval

[INSERT NAME] is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with School's policy review schedule.

A current version of this document is available to all members of staff [insert shared policy location].

Signature: Date:

## Change History Record

This privacy notice describes how we collect and use personal information about you during and after your work relationship with us, in accordance with the UK General Data Protection Regulation (UK GDPR).

Following Brexit, Regulation (EU) 2016/679, General Data Protection Regulation (GDPR) was incorporated into UK law as retained EU law and is now known as the UK GDPR. The UK GDPR operates alongside the Data Protection Act 2018, which supplements it by setting out additional provisions on matters such as the processing of personal data is specific sectors, exemptions, the powers of the Information Commissioner, and enforcement. The Data (Use and Access) Act 2025 further amends both the UK GDPR and Data Protection Act 2018 to modernise UK data protection rules and clarify certain rights and obligations. The GDPR continues to apply within the EU and to organisations that process personal data of individuals located in the EU.

This notice applies to all current and former employees, workers and contractors.

### Who Collects this Information

[NAME OF SCHOOL] is a "data controller" of personal data and gathers and uses certain information about you. This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice does not form part of any contract of employment or other contract to provide services and we may update this notice at any time.

It is important that you read this notice with any other policies mentioned within this privacy notice, so that you are aware of how and why we are processing your information, what your rights are under data protection legislation and the procedures we take to protect your personal data.

### Data Protection Principles

We will comply with the data protection principles when gathering and using personal information, as set out in our data protection policy.

### Categories of Information We Collect, Process, Hold and Share

Depending on your employment status, we may collect, store and use the following categories of personal information about you:

Personal information and contact details such as name, title, addresses, date of birth, marital status, phone numbers and personal email addresses;

Emergency contact information such as names, relationship, phone numbers and email addresses;

Information collected during the recruitment process that we retain during your employment including references, proof of right to work in the UK, application form, CV, qualifications;

Employment contract information such as start dates, hours worked, post, roles;

Education and training details;

Details of salary and benefits including payment details, bank details, payroll records, tax status information, national insurance number, pension and benefits information;

Details of any dependants;

Your nationality and immigration status and information from related documents, such as your passport or other identification and immigration information;

Information in your sickness and absence records such as number of absences and reasons(including sensitive personal information regarding your physical and/or mental health);

Criminal records information as required by law to enable you to work with children;

Information on grievances raised by or involving you;

Information on conduct and/or other disciplinary issues involving you;

Details of your appraisals, performance reviews and capability issues;

Details of your time and attendance records;

Information about the use of our IT, communications and other systems, and other monitoring information;

Details of your use of business-related social media, such as LinkedIn;

Images of staff captured by the School's CCTV system;

Your use of public social media (only in very limited circumstances, to check specific risks for specific functions within the School, you will be notified separately if this is to occur); and

Details in references about you that we give to other;

Recordings of staff from the School's video conferencing platform

We may also collect, store and use the following more sensitive types of personal information:

Information about your race or ethnicity, religious beliefs, sexual orientation, and political opinions.

Trade union membership.

Information about your health, including any medical condition and sickness records, including:

where you leave employment and under any share plan operated by a group company the reason for leaving is determined to be ill health, injury or disability, the records relating to that decision;

details of any absences (other than holidays) from work including time on statutory parental leave and sick leave; [and]

any health information in relation to a claim made under the permanent health insurance scheme; and

where you leave employment and the reason for leaving is related to your health, information about that condition needed for pensions and permanent health insurance purposes.

[Biometric data].

Information about criminal convictions and offences.

**How We Collect this Information**

We may collect this information from you in your application form, but we will also collect information in a number of different ways. This could be through the Home Office, our pension providers, medical and occupational health professionals we engage with, your trade union, the Disclosure and Barring Service (DBS), consultants and other professionals we may engage, e.g. to advise us generally and/or in relation to any grievance, conduct appraisal or performance review procedure, and even other employees. Information is also collected through CCTV, access control systems and any IT system the school has in place, such as email, communication systems, remote access systems, instant messaging and voicemail.

**How and Why we use your Information**

We will only use your personal information when the law allows us to. Most commonly, we will use your information in the following circumstances:

Where we need to perform the contract we have entered into with you;

Where we need to comply with a legal obligation (such as health and safety legislation, under statutory codes of practice and employment protection legislation);

Where it is needed in the public interest or for official purposes;

Where it is necessary for our legitimate interests (or those of a third party) and your interests, rights and freedoms do not override those interests.

When you have provided us with consent to process your personal data.

The situations in which we will process your personal information are listed below:

To determine recruitment and selection decisions on prospective employees;

In order to carry out effective performance of the employees contract of employment and to maintain employment records;

To comply with regulatory requirements and good employment practice;

To carry out vetting and screening of applicants and current staff in accordance with regulatory and legislative requirements;

Enable the development of a comprehensive picture of the workforce and how it is deployed and managed;

To enable management and planning of the workforce, including accounting and auditing;

Personnel management including retention, sickness and attendance;

Performance reviews, managing performance and determining performance requirements;

In order to manage internal policy and procedure;

Human resources administration including pensions, payroll and benefits;

To determine qualifications for a particular job or task, including decisions about promotions;

Evidence for possible disciplinary or grievance processes;

Complying with legal obligations;

To monitor and manage staff access to our systems and facilities in order to protect our networks, the personal data of our employees and for the purposes of safeguarding;

To monitor and protect the security of our network and information, including preventing unauthorised access to our computer network and communications systems and preventing malicious software distribution;

Education, training and development activities;

To monitor compliance with equal opportunities legislation;

To answer questions from insurers in respect of any insurance policies which relate to you;

Determinations about continued employment or engagement;

Arrangements for the termination of the working relationship;

Dealing with post-termination arrangements;

Health and safety obligations;

Prevention and detection of fraud or other criminal offences; and

To defend the School in respect of any investigation or court proceedings and to comply with any court or tribunal order for disclosure.

[DETAILS]

[Further information on the monitoring we undertake in the workplace and how we do this is available in [DETAILS OF POLICY].]

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you, or we may be prevented from complying with our legal obligations.

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose.

**How We Use Particularly Sensitive Information**

Sensitive personal information (as defined under the UK GDPR as “special category data”) requires higher levels of protection and further justification for collecting, storing and using it. We may process this data in the following circumstances:

In limited circumstances, with your explicit written consent;

Where we need to carry out our legal obligations in line with our Data Protection Policy (for example, employment, social-security or social-protection obligations);

For reasons of substantial public interest, such as for equal opportunities monitoring;

To establish, exercise or defend legal claims;

Where it is necessary to protect your vital interests (or those of another person) and you are unable to give consent.

We will use this information in the following ways:

Collecting information relating to leave of absence, which may include sickness absence or family related leave;

To comply with employment and other laws;

Collecting information about your physical or mental health, or disability status, to ensure your health and welfare in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to manage sickness absence and to administer benefits;

Collecting information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

To record trade union membership information to pay trade union premiums and to comply with employment law obligations.

**Criminal Convictions**

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where it is necessary to carry out our legal obligations. We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.

Where appropriate we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of working for us.

**Sharing Data**

We may need to share your data with third parties, including third party service providers where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so. These include the following:

the Department for Education (DfE);

Ofsted;

Prospective Employers;

Welfare services (such as social services);

Law enforcement officials such as police, HMRC;

LADO;

Training providers;

Professional advisors such as lawyers and consultants;

Support services (including HR support, insurance, IT support, information security, pensions and payroll);

The Local Authority;

Occupational Health;

DBS;

Recruitment and supply agencies; and

[other schools within the Federation/Trust].

Information will be provided to those agencies securely and/or anonymised where possible.

The recipient of the information will be bound by confidentiality obligations; we require them to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the UK and the EU. If we do, you can expect a similar degree of protection in respect of your personal information.

**Retention Periods**

Except as otherwise permitted or required by applicable law or regulation, the School only retains personal data for as long as necessary to fulfil the purposes they collected it for, as required to satisfy any legal, accounting or reporting obligations, or as necessary to resolve disputes.

Once you are no longer a staff member at the School, we will retain and securely destroy your personal information in accordance with our Data Retention Policy. This can be found [LOCATION].

**Security**

We have put in place measures to protect the security of your information (i.e. against it being accidentally lost, used or accessed in an unauthorised way). In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know.

You can find further details of our security procedures within our Data Breach Policy and our Information Security Policy, which can be found [LOCATION].

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

**Automated Decision Making**

Automated decision making takes place when an electronic system uses personal information to make a decision without human intervention. We are required to ensure that appropriate safeguards are in place when using automated decision making for significant decisions and the circumstances in which we are permitted to use special category data (sensitive information) in automated decision making are limited.

You will not be subject to automated decision making for significant decisions unless we have a lawful basis, and a valid condition where required, for doing so and appropriate safeguards are in place. Appropriate safeguards include informing the relevant individuals about the automated decision making and their rights to request a human review, express their views, and contest the decision.

**Biometric Data**

At [name of school] we would like to use your information as part of an automated (i.e. electronically operated) recognition system. This is for the purposes of [specify what purpose is – e.g., catering, library access]. The information that we wish to use is referred to as ‘biometric information’. This data will only be processed once we have obtained appropriate consent. For further information in relation to this, please see our Biometrics Policy.

**Your Rights of Access, Correction, Erasure and Restriction**

Under certain circumstances, by law you have the right to:

Access your personal information (commonly known as a “subject access request”). This allows you to receive a copy of the personal information we hold about you and to check we are lawfully processing it. You will not have to pay a fee to access your personal information. However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

Correction of the personal information we hold about you. This enables you to have any inaccurate information we hold about you corrected.

Erasure of your personal information. You can ask us to delete or remove personal data if there is no good reason for us continuing to process it.

Restriction of processing your personal information. You can ask us to suspend processing personal information about you in certain circumstances, for example, if you want us to establish its accuracy before processing it.

To object to processing in certain circumstances (for example for direct marketing purposes).

To transfer your personal information to another party.

If you want to exercise any of the above rights, please contact [NAME/EMAIL] in writing.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights).

**Right to Withdraw Consent**

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact [NAME/EMAIL]. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

**Contact**

If you would like to discuss anything within this privacy notice or have a concern about the way we are collecting or using your personal data, we request that you raise your concern with [NAME] in the first instance. We will acknowledge receipt of your complaint within 30 calendar days, and we will investigate and respond without undue delay. Further information about the way we handle data protection complaints can be found in our Data Protection Policy, available [HERE].

We have appointed a data protection officer (DPO) to oversee compliance with data protection and this privacy notice. If you have any questions about how we handle your personal information which cannot be resolved by [NAME], then you can contact the DPO on the details below:

Data Protection Officer: Judicium Consulting Limited

Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB

Email: dataservices@judicium.com

Web: www.judicium.com

Should you remain dissatisfied with our response, you also have the right to make a complaint to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

**Changes to this Privacy Notice**

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

| Version | Description of Change | Date of Policy Release by Judicium |
|---|---|---|
| 1 | Initial Issue | 06.05.18 |

| | | |
|---|---|---|
| 2 | Updated for UK GDPR and international transfers outside of the UK | 06.05.21 |
| 3 | Added reference to Biometric Data | 19.08.22 |
| 4 | Created a separate paragraph for collecting special category data. | 22.08.23 |
| 5 | Removed Craig Stilwell's name and added reference to Automated Decision Making | 29.08.24 |
| 6 | Changed Judicium's Address | 22.04.25 |
| 7 | Amendments to introduction, 'Automated Decision Making', and 'How to Raise a Concern' in line with amendments to UK GDPR by Data (Use and Access) Act 2025.<br><br>Removal of duplicated wording from 'How we use your Information'<br><br>Clarification of conditions for processing special category data.<br><br>Removal of duplicate wording from 'Security' | 06.03.2026 |

# Appendix 4 – Privacy Notice for Visitors and Contractors

## Document Owner and Approval

[INSERT NAME] is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with School's policy review schedule.

A current version of this document is available to all members of staff [insert shared policy location].

Signature: Date:

## Change History Record

This privacy notice describes how we collect and use personal information about you during and after your visit with us, in accordance with the UK General Data Protection Regulation (UK GDPR).

Following Brexit, Regulation (EU) 2016/679, General Data Protection Regulation (GDPR) was incorporated into UK law as retained EU law and is now known as the UK GDPR. The UK GDPR operates alongside the Data Protection Act 2018, which supplements it by setting out additional provisions on matters such as the processing of personal data is specific sectors, exemptions, the powers of the Information Commissioner, and enforcement. The Data (Use and Access) Act 2025 further amends both the UK GDPR and Data Protection Act 2018 to modernise UK data protection rules and clarify certain rights and obligations. The GDPR continues to apply within the EU and to organisations that process personal data of individuals located in the EU.

This notice applies to all current and former visitors and contractors.

### Who Collects this Information

[NAME OF SCHOOL] is a "data controller" of personal data and gathers and uses certain information about you. This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice does not form part of a contract to provide services and we may update this notice at any time.

It is important that you read this notice, with any other policies mentioned within this privacy notice, so you understand how we are processing your information and the procedures we take to protect your personal data.

### Data Protection Principles

We will comply with the data protection principles when gathering and using personal information, as set out in our data protection policy.

### Categories of Visitor Information we Collect, Process, Hold and Share

We process data relating to those visiting our school (including contractors). Personal data that we may collect, process, hold and share (where appropriate) about you includes, but is not restricted to:

Personal information and contact details such as name, title, addresses, date of birth, marital status, phone numbers and personal email addresses;

Criminal records information as required by law to enable you to work with children e.g. the Disclosure and Baring Service checks;

Information relating to your visit, e.g. your company or organisations name, arrival and departure time, car number plate;

Information about any access arrangements you may need;

Photographs for identification purposes for the duration of your visit;

CCTV footage captured by the school.

We may also collect, store and use the following more sensitive types of personal information:

Information about your race or ethnicity, religious or philosophical beliefs

Information about your health, including any medical conditions.

[Biometric data]

**How we Collect this Information**

We may collect this information from you, the Home Office, the DBS, other professionals we may engage (e.g. to advise us generally), our signing in system, automated monitoring of our websites and other technical systems such as our computer networks and connections, CCTV and access control systems, remote access systems, email and instant messaging systems, intranet and internet facilities.

**How we use your Information**

We will only use your personal information when the law allows us to. Most commonly, we will use your information in the following circumstances:

Where we need to perform the contract we have entered into with you;

Where we need to comply with a legal obligation (such as health and safety legislation, under statutory codes of practice and employment protection legislation);

Where it is needed in the public interest or for official purposes;

Where it is necessary for our legitimate interests (or those of a third party) and your interests, rights and freedoms do not override those interests.

When you have provided us with consent to process your personal data.

We need all the categories of information in the list above primarily to allow us to perform our contract with you, with your consent and to enable us to comply with legal obligations.

The situations in which we will process your personal information are listed below:

Ensure the safe and orderly running of the school;

To manage our workforce and those deployed on site;

Personnel management including retention

In order to manage internal policy and procedure;

Complying with legal obligations;

Carry out necessary administration functions to allow visitors and contractors on site;

To monitor and manage access to our systems and facilities in order to protect our networks and for the purposes of safeguarding;

To monitor and protect the security of our network and information, including preventing unauthorised access to our computer network and communications systems and preventing malicious software distribution;

To answer questions from insurers in respect of any insurance policies which relate to you;

Health and safety obligations;

Prevention and detection of fraud or other criminal offences; and

To defend the School in respect of any investigation or court proceedings and to comply with any court or tribunal order for disclosure.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and will explain the legal basis which allows us to do so.

**How we use Particularly Sensitive Information**

Sensitive personal information (as defined under the UK GDPR as "special category data") require higher levels of protection and further justification for collecting, storing and using this type of personal information. We may process this data in the following circumstances:

In limited circumstances, with your explicit written consent;

Where we need to carry out our legal obligations in line with our Data Protection Policy (for example, to comply with health and safety duties for contractors or visitors on site);

For reasons of substantial public interest, such as safeguarding pupils and staff, preventing unlawful acts, or ensuring site security;

To establish, exercise or defend legal claims;

Where it is necessary to protect your vital interests (or those of another person) and you are unable to give consent.

**Criminal Convictions**

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where it is necessary to carry out our legal obligations. We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.

**Sharing Data**

We may need to share your data with third parties, including third party service providers where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so. These include the following:

the Department for Education (DfE);

Ofsted;

[other schools within the Federation/Trust];

Law enforcement officials such as police, HMRC;

LADO;

Professional advisors such as lawyers and consultants;

Support services (including HR support, insurance, IT support, information security, pensions and payroll);

The Local Authority; and

DBS.

Information will be provided to those agencies securely and/or anonymised where possible.

The recipient of the information will be bound by confidentiality obligations, we require them to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the UK and the EU. If we do, you can expect a similar degree of protection in respect of your personal information.

**Retention Periods**

Except as otherwise permitted or required by applicable law or regulation, the School only retains personal data for as long as necessary to fulfil the purposes they collected it for, as required to satisfy any legal, accounting or reporting obligations, or as necessary to resolve disputes.

We will retain and securely destroy your personal information in accordance with our Data Retention Policy, whichcan be found [LOCATION].

**Security**

We have put in place measures to protect the security of your information (i.e. against it being accidentally lost, used or accessed in an unauthorised way). In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know.

You can find further details of our security procedures within our Data Breach Policy and our Information Security Policy, which can be found [LOCATION].

**Automated Decision Making**

Automated decision making takes place when an electronic system uses personal information to make a decision without human intervention. We are required to ensure that appropriate safeguards are in place when using automated decision making for significant decisions and the circumstances in which we are permitted to use special category data (sensitive information) in automated decision making are limited.

You will not be subject to automated decision making for significant decisions unless we have a lawful basis, and a valid condition where required, for doing so and appropriate safeguards are in place. Appropriate safeguards include informing the relevant individuals about the automated decision making and their rights to request a human review, express their views, and contest the decision.

**Biometric Data**

At [name of school] we would like to use your information as part of an automated (i.e., electronically operated) recognition system. This is for the purposes of [specify what purpose is – e.g., catering, library access]. The information that we wish to use is referred to as ‘biometric information’. This data will only be processed once we have obtained appropriate consent. For further information in relation to this, please see our Biometrics policy.

**Your Rights of Access, Correction, Erasure and Restriction**

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your relationship with us.

Under certain circumstances by law you have the right to:

Access your personal information (commonly known as a “subject access request”). This allows you to receive a copy of the personal information we hold about you and to check we are lawfully processing it. You will not have to pay a fee to access your personal information. However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

Correction of the personal information we hold about you. This enables you to have any inaccurate information we hold about you corrected.

Erasure of your personal information. You can ask us to delete or remove personal data if there is no good reason for us continuing to process it.

Restriction of processing your personal information. You can ask us to suspend processing personal information about you in certain circumstances, for example, if you want us to establish its accuracy before processing it.

To object to processing in certain circumstances (for example for direct marketing purposes).

To transfer your personal information to another party.

If you want to exercise any of the above rights, please contact [NAME/EMAIL] in writing.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights).

**Right to Withdraw Consent**

In the limited circumstances where you may have provided your consent to the collection, processing, and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact [NAME/EMAIL]. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

**Contact**

If you would like to discuss anything within this privacy notice or have a concern about the way we are collecting or using your personal data, we request that you raise your concern with [NAME] in the first instance. We will acknowledge receipt of your complaint within 30 calendar days, and we will investigate and respond without undue delay. Further information about the way we handle data protection complaints can be found in our Data Protection Policy, available [HERE].

We have appointed a data protection officer (DPO) to oversee compliance with data protection and this privacy notice. If you have any questions about how we handle your personal information which cannot be resolved by [NAME], then you can contact the DPO on the details below:

Data Protection Officer: Judicium Consulting Limited

Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB

Email:

Web:

Should you remain dissatisfied with our response, you also have the right to make a complaint to the Information Commissioner’s Office (ICO), the UK supervisory authority for data protection issues.

**Changes to this Privacy Notice**

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

| Version | Description of Change | Date of Policy Release by Judicium |
|---|---|---|
| 1 | Initial Issue | 06.05.18 |
| 2 | Updated for UK GDPR and international transfers outside of the UK | 06.05.21 |
| 3 | Created a separate paragraph for collecting special category data. | 22.08.23 |
| 4 | Removed Craig Stilwell's name and have included information on biometric data and automatic decision making. | 29.08.24 |
| 5 | Changed Judicium's Address | 22.04.25 |
| 6 | Amendments to introduction, 'Automated Decision Making', and 'How to Raise a Concern' in line with amendments to UK GDPR by Data (Use and Access) Act 2025.<br><br>Clarification of conditions for processing special category data.<br><br>Removal of duplicate wording from 'Security' | 06.03.2026 |

# Appendix 5 – Privacy Notice for Job Applicants

## Document Owner and Approval

[INSERT NAME] is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with School's policy review schedule.

A current version of this document is available to all members of staff [insert shared policy location].

Signature: Date:

## Change History Record

This privacy notice describes how we collect and use personal information about you during and after your work relationship with us, in accordance with the UK General Data Protection Regulation (UK GDPR).

Following Brexit, Regulation (EU) 2016/679, General Data Protection Regulation (GDPR) was incorporated into UK law as retained EU law and is now known as the UK GDPR. The UK GDPR operates alongside the Data Protection Act 2018, which supplements it by setting out additional provisions on matters such as the processing of personal data is specific sectors, exemptions, the powers of the Information Commissioner, and enforcement. The Data (Use and Access) Act 2025 further amends both the UK GDPR and Data Protection Act 2018 to modernise UK data protection rules and clarify certain rights and obligations. The GDPR continues to apply within the EU and to organisations that process personal data of individuals located in the EU.

This privacy notice applies to all job applicants. Successful candidates should refer to our privacy notice for staff for information about how their personal data is stored and collected.

### Who Collects this Information

[NAME OF SCHOOL] is a "data controller" of personal data and gathers and uses certain data about you. This means that we are responsible for deciding how we hold and use personal information about you.

We are required under data protection legislation to notify you of the information contained in this privacy notice. This notice does not form part of any contract of employment or other contract to provide services and we may update this notice at any time.

It is important that you read this notice, together with any other policies mentioned within this privacy notice. This will assist you with understanding how we process your information and the procedures we take to protect your personal data.

### Data Protection Principles

We will comply with the data protection principles when gathering and using personal information, as set out in our data protection policy.

### Categories of Information We Collect, Process, Hold and Share

We may collect, store and use the following categories of personal information about you up to the shortlisting stage of the recruitment process: -

Personal information and contact details such as name, title, addresses, date of birth, marital status, phone numbers and personal email addresses;

Emergency contact information such as names, relationship, phone numbers and email addresses;

Information collected during the recruitment process that we retain during your employment including proof of right to work in the UK, information entered on the application form, CV, qualifications;

Details of your employment history including job titles, salary and working hours;

Information regarding your criminal record as required by law to enable you to work with children;

Details of your referees and references;

Details collected through any pre-employment checks including online searches for data;

Your racial or ethnic origin, sex and sexual orientation, religious or similar beliefs.

We may also collect information after the shortlisting and interview stage in order to make a final decision on where to recruit:

Data about your previous academic and/or employment history, including details of any conduct, grievance or performance issues, appraisals, time and attendance, from references obtained about you from previous employers and/or education providers;

Data regarding your academic and professional qualifications;

Data regarding your criminal record**,** in a criminal records certificate (CRC) or enhanced criminal records certificate (ECRC) as appropriate**;**

Your nationality and immigration status and data from related documents, such as your passport or other identification and immigration information;

A copy of your driving licence; and

Data relating to your health.

**How We Collect this Information**

We may collect this information from you, your referees, your education provider, by searching online resources, from relevant professional bodies the Home Office and from the Disclosure and Barring Service (DBS).

**How and Why We Use Your Information**

We will only use your personal information when the law allows us to. Most commonly, we will use your information in the following circumstances:

Where we need to take steps to enter into a contract with you;

Where we need to comply with a legal obligation (such as health and safety legislation, under statutory codes of practice and employment protection legislation);

Where it is needed in the public interest or for official purposes;

Where it is necessary for our legitimate interests (or those of a third party) and your interests, rights and freedoms do not override those interests.

Where you have provided your consent for us to process your personal data.

Generally, the purpose of us collecting your data is to enable us to facilitate safe recruitment and determine suitability for the role. We also collect data in order to carry out equal opportunities monitoring and to ensure appropriate access arrangements are put in place if required.

If you fail to provide certain information when requested, we may not be able to take the steps to enter into a contract with you, or we may be prevented from complying with our legal obligations.

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose.

**How We Use Particularly Sensitive Information**

Sensitive personal information (as defined under the UK GDPR as "special category data") require higher levels of protection and further justification for collecting, storing, and using this type of personal information. We may process this data in the following circumstances:

In limited circumstances, with your explicit written consent;

Where we need to carry out our legal obligations in line with our data protection policy;

For reasons of substantial public interest, such as for equal opportunities monitoring;

To establish, exercise or defend legal claims;

Where it is necessary to protect your vital interests (or those of another person) and you are unable to give consent.

**Criminal Convictions**

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where it is necessary to carry out our legal obligations. We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.

Where appropriate we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of working for us.

**Sharing Data**

We may need to share your data with third parties, including third party service providers where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

These include the following: -

Academic or regulatory bodies to validate qualifications/experience (for example the teaching agency);

Referees;

Other schools;

HR advisors and professional advisers;

The DBS to carry out background checks where legally required;

Recruitment and supply agencies;

[our Local Authority/Academy/Trust] in order to meet our legal obligations for sharing data with it;

[other schools within the Federation/Trust].

We may also need to share some of the above categories of personal information with other parties, such as our legal or professional advisers. Where possible, information will be anonymised, but this may not always be feasible.

All recipients are required to handle personal data securely and only for the purposes for which it was shared. We may also be required to share some personal information with our regulators or as required to comply with the law.

**Retention Periods**

We keep the personal data that we obtain about you during the recruitment process for no longer than is necessary for the purposes for which it is processed. How long we keep your data will depend on whether your application is successful and you become employed by us, the nature of the data concerned and the purposes for which it is processed.

We will keep recruitment data (including interview notes) for no longer than is reasonable, taking into account the limitation periods for potential claims such as race or sex discrimination (as extended to take account of early conciliation), after which they will be destroyed. If there is a clear business reason for keeping recruitment records for longer than the recruitment period, we may do so but will first consider whether the records can be pseudonymised or anonymised, and the longer period for which they will be kept.

If your application is successful, we will keep only the recruitment data that is necessary in relation to your employment.

Once we have finished recruitment for the role you applied for, we will then store your information in accordance with our Retention Policy. This can be found [LOCATION].

**Security**

We have put in place measures to protect the security of your information (i.e. against it being accidentally lost, used or accessed in an unauthorised way). In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know.

You can find further details of our security procedures within our Data Breach policy and our Information Security policy, which can be found [LOCATION].

**Automated Decision Making**

[SCHOOL] does not make decisions about job applicants based soled on automated processing. All recruitment and selection decisions involve meaningful human review.

If this position changes in the future (for example, if we introduce automated screening or scoring tools) we will update this notice and provide you with information about the logic involved and your rights in relation to such processing.

**Your Rights of Access, Correction, Erasure and Restriction**

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Under certain circumstances by law you have the right to:

Access your personal information (commonly known as a “subject access request”). This allows you to receive a copy of the personal information we hold about you and to check we are lawfully processing it. You will not have to pay a fee to access your personal information. However, we may charge a reasonable fee if your request for

access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

Correction of the personal information we hold about you. This enables you to have any inaccurate information we hold about you corrected.

Erasure of your personal information. You can ask us to delete or remove personal data if there is no good reason for us continuing to process it.

Restriction of processing your personal information. You can ask us to suspend processing personal information about you in certain circumstances, for example, if you want us to establish its accuracy before processing it.

To object to processing in certain circumstances (for example for direct marketing purposes).

To transfer your personal information to another party.

If you want to exercise any of the above rights, please contact [NAME/EMAIL] in writing.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights).

**Right to Withdraw Consent**

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact [NAME/EMAIL]. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

**Contact**

If you would like to discuss anything within this privacy notice or have a concern about the way we are collecting or using your personal data, we request that you raise your concern with [NAME] in the first instance. We will acknowledge receipt of your complaint within 30 calendar days, and we will investigate and respond without undue delay. Further information about the way we handle data protection complaints can be found in our Data Protection Policy, available [HERE].

We have appointed a data protection officer (DPO) to oversee compliance with data protection and this privacy notice. If you have any questions about how we handle your personal information which cannot be resolved by [NAME], then you can contact the DPO on the details below:

Data Protection Officer: Judicium Consulting Limited

Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB

Email:

Web:

Should you remain dissatisfied with our response, you also have the right to make a complaint to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

**Changes to this Privacy Notice**

We reserve the right to update this Privacy Notice at any time, and we will provide you with a new privacy notice when we make any substantial changes. We may also notify you in other ways from time to time about the processing of your personal information.

| Version | Description of Change | Date of Policy Release by Judicium |
|---|---|---|
| 1 | Initial Issue | 06.05.18 |
| 2 | Updated for UK GDPR and international transfers outside of the UK | 06.05.21 |
| 3 | Updated to include reference to online searches | 20.07.22 |
| 4 | Removed Craig Stilwell's name. Included additional information on retention periods and online searches. | 29.08.24 |
| 5 | Changed Judicium's Address | 22.04.25 |
| 6 | Amendments to introduction, 'Automated Decision Making', and 'How to Raise a Concern' in line with amendments to UK GDPR by Data (Use and Access) Act 2025.<br><br>Clarification of conditions for processing special category data.<br><br>Removal of duplicate wording from 'Security' | 06.03.2026 |

# Appendix 6 – Short Form Privacy Notice for Application Forms

Short Form Privacy Notice For Application Forms

This wording is intended to be used within or to accompany your application forms, giving information on how you use the application information. This is not intended to be used instead of a privacy notice and is used solely to explain how the information contained within the application form is used.

This notice explains what personal data we will hold about you, how we collect it, and how we will use and may share information about you during the application process. We are required to notify you of this information, under data protection legislation.

Please ensure that you read this notice as well as our privacy notice which can be found at [DETAILS] which detail how we use your information.

Why Do We Collect This Information?

Once you have submitted an application form, the School use this information in order to assess your suitability for employment, to comply with our legal obligations relating to safer recruitment, and to take steps at your request before entering into an employment contract.

What Information Do We Collect?

We collect the following information from the application form in order to take a decision as to recruitment: [DETAILS]

How we may share the information

We may also need to share some of the above categories of personal information with other parties, such as HR consultants and professional advisers. Usually, information will be anonymised but this may not always be possible. The recipient of the information will be bound by confidentiality obligations. We may also be required to share some personal information as required to comply with the law.

How long we keep your information

We keep the personal information that we obtain about you during the recruitment process for no longer than is necessary for the purposes for which it is processed. How long we keep your information will depend on whether your application is successful and you become employed by us, the nature of the information concerned and the purposes for which it is processed. Full details on how long we keep personal data for is set out in our data retention policy.