



ARTS EDUCATIONAL SCHOOLS
Privacy Notice & Retention of Records Policy

Document Title	Privacy Notice & Retention of Records Policy
Maintained by	Headteacher, SLT, Finance Director
Owned by	Deputy Headteacher
Institutional/Directorate Policy	Day School and Sixth Form
Approved by	DSSF Board
Last Reviewed	September 2026
Next Review	September 2027

ArtsEd - Day School and Sixth Form
Privacy Notice & Retention of Records Policy

1. SCOPE

This policy applies to the Day School and Sixth Form 'The School'. The School is part of The Arts Educational Schools, referred to as ArtsEd, a charity registered in England and Wales with Charity Registration number 311087; the company registration number is 00712444 and the registered address is at Cone Ripman House, 14 Bath Road, London, W4 1LY.

2. WHAT THIS PRIVACY NOTICE IS FOR

This policy is intended to provide information about how the School will collect, use and hold (or "process") personal data about individuals including: current, past and prospective pupils; and their parents, carers or guardians (referred to in this policy as "parents") and visitors to the School. Collectively, we refer to these individuals in the Privacy Notice as the School's community.

This makes the School a data controller of your personal information and this information is provided because data protection law gives individuals rights to understand how their data is processed and this Privacy Notice sets out how we will use that information and what your rights are in respect of the data we hold about you. Please note that the School has a separate Data Protection Policy applicable to its employees and other staff.

This Privacy Notice applies alongside any other information the School may provide about a particular use of personal data, for example when collecting data via an online or paper form.

This Privacy Notice also applies in addition to the School's other relevant terms and conditions and policies.

3. RESPONSIBILITY FOR DATA PROTECTION

Anyone who works for, or acts on behalf of, the School (including staff, volunteers, trustees and service providers) will be subject to suitable training and/or policies commensurate with their role.

The School has appointed a Data Protection Officer (DPO), the Finance Director, who will:

- Deal with all your requests and enquiries concerning the School's uses of your personal data (see section on Your Rights below); and
- Endeavour to ensure that all personal data is processed in compliance with this policy and Data Protection Law.

You can contact the DPO by email dataservices@judicium.com; or by post using the School's postal address above.

4. WHY THE SCHOOL NEEDS TO PROCESS PERSONAL DATA

In order to carry out its ordinary duties to staff, pupils and parents, the School needs to process a wide range of personal data about our community as part of its daily operation.

Some of this activity the School will need to carry out in order to fulfil its legal rights, duties or obligations – including those under a contract with its staff, or parents of its pupils.

Other uses of personal data will be made in accordance with the School's legitimate interests, or the legitimate interests of another, provided that these are not outweighed by the impact on individuals, and provided it does not involve special or sensitive types of data.

The School expects that the following uses will fall within that category of its (or its community's) "legitimate interests" (as recognised in law or determined by the school):

- For the purposes of pupil selection and to confirm the identity of prospective pupils and their parents, assess suitability for bursaries, and retain a record (if appropriate) for the purposes of future applications or openings;
- To carry out credit, identity and source of funds checks, whether with previous schools and/or other third party sources or service providers, including for the purposes of verifying that parents are not subject to (or within the purview of) sanctions;
- To provide education services, including musical education, physical training or spiritual development, career services, and extra-curricular activities to pupils, and monitoring pupils' progress and educational needs including where such services are provided remotely (either temporarily or permanently);
- To report to and liaise with parents about their child's progress, welfare and development, including by way of regular reports and parents' evenings;
- To organise and manage meetings, events and social engagements for pupils and parents;
- To maintain relationships with alumni and the School community, including direct marketing or fundraising activity;
- For the purposes of donor due diligence, and to confirm the identity of prospective donors and their background and relevant interests;
- For the purposes of management planning and forecasting, research and statistical analysis, including that imposed or provided for by law (such as tax, diversity or gender pay gap analysis);
- To enable relevant authorities to monitor the School's performance and to intervene or assist with incidents as appropriate;
- To give and receive information and references about past, current and prospective pupils, including relating to outstanding fees or payment history, to/from any educational institution that the pupil attended or where it is proposed they attend; and to provide references to potential employers of past pupils;
- To enable pupils to take part in national or other assessments, and to publish the results of public examinations or other achievements of pupils of the School;
- To safeguard pupils' health and welfare and provide appropriate pastoral care (including following the requirements and recommendations of the government's guidance on Keeping Children Safe in Education (or "KCSIE"));
- To monitor (as appropriate) use of the School's IT and communications systems in accordance with the School's IT Acceptable Use policy;
- To make use of photographic images and video content of pupils in School publications, on the School website and on the School's social media channels in accordance with the School's policy on taking, storing and using images of children;
- For security purposes, including CCTV in accordance with the School's CCTV Policy;
- For the prevention and detection of crime, and in order to assist with investigations (including criminal investigations) carried out by the police and other competent authorities;
- For regulatory record keeping/compliance purposes in respect of immigration requirements, as an employer and/or visa sponsor;
- To carry out or cooperate with any School or external complaints, disciplinary or investigation process;
- To promote the School to prospective parents and pupils; and
- Where otherwise reasonably necessary for the School's purposes, including to obtain appropriate professional advice and insurance for the School.

In addition, the School will on occasion need to process special category personal data (concerning health, ethnicity, religion, biometrics or sexual life) or criminal records information (such as when carrying out DBS checks) in accordance with rights or duties imposed on us by law, including as regards safeguarding, or from time to time by explicit consent where required. These reasons will include:

- To safeguard pupils' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency, incident or accident, including by disclosing details of an individual's health / medical condition or other

relevant information where it is in the individual's interests to do so: for example for emergency medical care, to arrange the assessment and diagnosis of a pupil's special educational needs, for social protection, safeguarding, and cooperation with police or social services, for insurance purposes or to caterers or organisers of School trips who need to be made aware of dietary or medical needs;

- To comply with public health requirements;
- To provide educational services in the context of making reasonable adjustments for a pupil's disability and/or any special educational needs of a pupil;
- To provide spiritual education in the context of any religious beliefs;
- As part of any School or external complaints, disciplinary or investigation process that involves such data, for example if there are SEND, health or safeguarding elements; or
- For legal and regulatory purposes (for example child protection, diversity monitoring and health and safety and immigration/visa sponsorship compliance) and to comply with its legal obligations and duties of care.

5. TYPES OF PERSONAL DATA PROCESSED BY THE SCHOOL

This will include by way of example:

- Names, addresses, telephone numbers, e-mail addresses and other contact details;
- Car details (about those who may park from time to time at ArtsEd);
- Bank details and other financial information, e.g. about parents (or others) who pay fees to the School, and any source of funds and/or anti-money laundering information we are required to collect by law;
- Past, present and prospective pupils' academic, disciplinary, admissions, safeguarding and attendance records, and examination scripts and marks;
- Nationality and other immigration status information (e.g. right to enter, live and work or study in the United Kingdom), including copies of passport information;
- Contact details for next of kin;
- References given or received by the School about pupils, and relevant information provided by previous educational establishments and/or other professionals or organisations working with pupils;
- Correspondence with and concerning pupils and parents (past and present); and
- Images and video content of pupils (and occasionally other individuals) engaging in School activities, including content captured by the School's CCTV system and as part of filming, recording or streaming of School events, (in accordance with the School's policy on taking, storing and using images of children).

6. HOW THE SCHOOL COLLECTS DATA

Generally, the School receives personal data from the individual directly (including, in the case of pupils, from their parents). This may be via a form, or simply in the ordinary course of interaction or communication (such as email or written assessments).

However, in some cases, personal data will be supplied by third parties (for example, another school, or other professionals or authorities, or third party service providers who credit and identity check parents and their source of funds); or collected from publicly available resources

7. WHO HAS ACCESS TO PERSONAL DATA AND WHO THE SCHOOL SHARES IT WITH

Processing by third parties. For the most part, personal data collected by the School will remain within the School, and will be processed by appropriate individuals only in accordance with access protocols (i.e. on a 'need to know' basis). However, some functions are outsourced including, eg IT, cloud storage/ records management, monitoring, and mailing. In accordance with Data Protection Law, this type of external data processing is always subject to contractual assurances that personal data will be kept securely and used only in accordance with the School's specific directions.

Data sharing: Occasionally, the School – including its governing board – will need to share personal information relating to its community of pupils and parents with third parties, such as

- The Arts Parents (parent and friends association)
- Appropriate contractors, such as visiting music teachers or external investigators or consultants;
- Professional advisers (e.g. lawyers, insurers, PR advisers and accountants)
- Organisations that provide a service to the School.
- Testing services and examination boards;
- Stage 3 complaints panels, which may include independent panel members such as when a complaint is raised (and in accordance with the School Complaints Procedure, this requires the involvement of independent panel members);
- Third parties and their advisors in the event of a possible or actual sale, merger or other restructuring of the School;
- Government authorities (e.g. HMRC, DfE, CAFCASS, police, Home Office, a relevant public health/NHS body and/or local authority) and/or appropriate regulatory bodies e.g. The Teaching Regulation Agency, the Independent Schools Inspectorate, the Charity Commission;

8. ACCESS TO, AND SHARING OF, SENSITIVE DATA

Particularly strict rules of access apply in the context of ‘special category’ data, most notably:

- health and medical / special needs records; and
- pastoral or safeguarding files.

Medical Data: The School needs to process such information to comply with statutory duties and to keep pupils and others safe, but the School will ensure only authorised staff can access information on a need-to-know basis. This may include wider dissemination if needed for School trips or for catering purposes. Express consent will be sought where appropriate. However, a certain amount of relevant information will need to be provided to staff more widely in the context of providing the necessary care and education that the pupil requires.

Safeguarding data: The School is under duties imposed by law and statutory guidance (including Keeping Children Safe in Education or ‘KCSIE’) to record or report incidents and concerns that arise or are reported to it, in some cases regardless of whether they are proven, if they meet a certain threshold of seriousness in their nature or regularity. This is likely to include notes on personnel or safeguarding files, low-level concerns records kept about adults (which may include references to pupils or family members), and in some cases referrals to relevant authorities such as the LADO, Children’s Services, CAMHS or the police.

KCSIE also requires that, whenever a child leaves the School to join another school or School, his or her child protection file is promptly provided to the new organisation, along with any other information which the School’s Designated Safeguarding Lead considers material to the ongoing care needs of any pupil. Where appropriate, the School will consult with parents as to how these needs are best served, but ultimately the decision as to what information is necessary to share with the new school or School is a safeguarding question that must be reserved to the School. The School will retain a copy of the child protection file in accordance with its retention policy for material related to safeguarding matters.

For further information about this, please view the School’s policy on Child Protection & Safeguarding.

9. HOW LONG WE KEEP PERSONAL DATA

The School will retain personal data securely and only in line with how long it is necessary to keep for a legitimate and lawful reason. Typically, the legal recommendation for how long to keep ordinary parent and pupil personnel files is up to 7 years following departure from the School. However, incident reports and safeguarding files will need to be kept much longer, in accordance with specific legal requirements.

If you have any specific queries about how our retention policy is applied, or wish to request that personal data that you no longer believe to be relevant is considered for erasure, please contact the Data Protection Officer. However, please bear in mind that the School will often have lawful and necessary reasons to hold on to some personal data even following such a request.

A limited and reasonable amount of information will be kept for archiving purposes, for example; and even where you have requested we no longer keep in touch with you, we will need to keep a record of the fact in order to fulfil your wishes (called a "suppression record").

Please refer to the [Appendix 1 for retention of records](#).

10. KEEPING IN TOUCH AND SUPPORTING THE SCHOOL

The School and/or any relevant other organisation will use the contact details of parents, alumni and other members of the School community to keep them updated about the activities of the School, or alumni and parent events of interest, including by sending updates and newsletters, by email and by post. Unless the relevant individual objects, the School will also:

- Share personal data about parents and/or alumni, as appropriate, with organisations set up to help establish and maintain relationships with the School community
- Contact parents and/or alumni by post and email in order to promote and raise funds for the School and, where appropriate, other worthy causes;
- Collect information from publicly available sources about parents' and former pupils' occupation and activities, in order to maximise the School's fundraising potential.

Should you wish to limit or object to any such use, or would like further information about them, please contact the Data Protection Lead in writing. You always have the right to withdraw consent, where given, or otherwise object to direct marketing or fundraising. However, the School is nonetheless likely to retain some of your details (not least to ensure that no more communications are sent to that particular address, email or telephone number).

11. YOUR RIGHTS

You have the following rights:

- to obtain access to, and copies of, the personal data that we hold about you;
- to require us to correct the personal data we hold about you if it is incorrect;
- to require us (in certain circumstances) to erase your personal data;
- to request that we restrict our data processing activities (and, where our processing is based on your consent, you may withdraw that consent, without affecting the lawfulness of our processing based on consent before its withdrawal);
- to receive from us the personal data we hold about you which you have provided to us, in a reasonable format specified by you, including for the purpose of you transmitting that personal data to another data controller;
- to object, on grounds relating to your particular situation, to any of our particular processing activities where you feel this has a disproportionate impact on your rights.

Please note that the above rights are not absolute, and we may be entitled to refuse requests where exceptions apply. The School will endeavour to respond to any such requests as soon as is reasonably practicable and in any event within statutory time-limits (which is generally one month, but actually

fulfilling more complex or multiple requests, e.g. those involving third party information, may take 1-2 months longer).

12. DATA ACCURACY AND SECURITY

The School will endeavour to ensure that all personal data held in relation to an individual is as up to date and accurate as possible. Individuals must please notify the relevant School office of any significant changes to important information, such as contact details, held about them.

An individual has the right to request that any out-of-date, irrelevant or inaccurate or information about them is erased or corrected (subject to certain exemptions and limitations under Data Protection Law): please see above for details of why the School may need to process your data, of how you may contact if you disagree.

The School will take appropriate technical and organisational steps to ensure the security of personal data about individuals, including policies around use of technology and devices, and access to School systems.

13. THIS POLICY

The School will update this Privacy Notice from time to time. Any substantial changes that affect your rights will be provided to you directly as far as is reasonably practicable.

14. QUERIES AND COMPLAINTS

If you believe that the School has not complied with this Privacy Notice or acted otherwise than in accordance with data protection law, you should email dataservices@judicium.com with details of your complaint. The School will acknowledge your complaint within 30 days of receipt and will investigate and inform you of the outcome of your complaint without undue delay (keeping you informed of progress as necessary).

If you are not satisfied with the outcome of your complaint, or if you feel the School has not handled it appropriately, you have the right to complain to the [Information Commissioner's Office \(ICO\)](#).

Appendix 1 Data Retention Periods

	Type of Record/Document	Retention Period
SCHOOL-SPECIFIC RECORDS	Registration documents of School	Permanent (or until closure of the School)
	Admission Register ('the school roll')	At least 6 years from date of entry (monthly backup required).
	Attendance Register	6 years from the date of entry, (monthly backup required).
	Minutes of Trustees' meetings	6 years from date of meeting
	Annual curriculum	From end of year: 3 years (or 1 year for other class records: eg marks/timetables/assignments)
	Complaints Register / Log	7 years from pupil leaving school
INDIVIDUAL PUPIL RECORDS	Admissions: application forms, assessments, records of decisions	25 years from date of birth (or up to 7 years from the pupil leaving) If pupil not admitted, up to 1 year from that decision
	Student immigration records	Duration of student sponsorship plus min 1 year
	Examination results (external or internal)	7 years from pupil leaving School
	Pupil file including: • Pupil reports • Pupil performance records • Pupil medical records (not accidents) • Pupil disciplinary records (not issues of safeguarding) • Attendance data	ALL: 25 years from date of birth (subject where any material may be relevant to potential claims: see below)
	Special educational needs records	Date of birth plus up to 35 years (risk assessed)
EMAILS ON SERVER	Pupil emails account	Delete upon leaving school, or within 1 year
	Staff emails	Delete account within 1 year of leaving school.
SAFEGUARDING	Policies, procedures and insurance	Keep a permanent record of historic policies
	DBS disclosure certificates (if held)	<u>No longer than 6 months</u> from decision on recruitment, unless police specifically consulted. A record of the checks being made must be kept on the SCR/personnel file, but not the certificate itself
	Accident / Incident reporting	Keep on record for as long as any living victim may bring a claim (NB civil claim limitation periods can be set aside in cases of abuse). Ideally, files to be reviewed from time to time if resources allow and a suitably qualified person is available.
	Child Protection files	If a referral has been made or social care has been involved or child has been subject of a multi-agency plan; or if any risk of future claim(s): 75 years.
	Video recordings of meetings	Where any one-on-one meetings of classes, counselling, or application interviews are recorded (e.g. for safeguarding purposes), a shorter-term retention policy is acceptable based on the DSL's view of how quickly a concern will likely be raised: e.g. 3-6 months or immediately upon DSL review.
	CCTV Footage	Routinely, CCTV footage is stored for 30 days before being automatically overwritten.
CORPORATE RECORDS (where applicable)	Certificates of Incorporation	Permanent (or until dissolution of the company)
	Minutes, Notes and Resolutions of Boards or Management Meetings	Minimum – 10 years
	Register of Members	Permanent (minimum 10 years for ex-members)
	Annual reports	Minimum – 6 years
ACCOUNTING RECORDS	Accounting records	7 years from the end of the financial year in which the transaction took place
	Tax returns	7 years
	VAT returns	7 years
	Budget and internal financial reports	3 years

CONTRACTS AND AGREEMENTS	Signed or final/concluded agreements (<i>plus any signed or final/concluded variations or amendments</i>)	7 years from completion of contractual obligations or term of agreement, whichever is the later
	Deeds (or contracts under seal)	13 years from completion of contractual obligation or term of agreement
INTELLECTUAL PROPERTY RECORDS	Formal documents of title (trade mark or registered design certificates; patent or utility model certificates)	Permanent (in the case of any right which can be permanently extended, eg trade marks); otherwise expiry of right plus minimum of 7 years.
	Assignments of intellectual property to or from the School	As above in relation to contracts (7 years) or, where applicable, deeds (13 years).
	IP / IT agreements (including software licences and ancillary agreements eg maintenance; storage; development; coexistence agreements; consents)	Minimum – 7 years from completion of contractual obligation concerned or term of agreement
EMPLOYEE / PERSONNEL RECORDS NB these records will contain personal data.	Single Central Record of employees	Keep a permanent record of all mandatory checks that have been undertaken (but do <u>not</u> keep DBS certificate information itself: 6 months as above)
	Contracts of employment	7 years from effective date of end of contract
	Employee appraisals or reviews	Duration of employment plus minimum of 7 years
	Staff personnel file	As above, but do <u>not delete any information which may be relevant to historic safeguarding claims.</u>
	Payroll, salary, maternity pay records	Minimum – 6 years
	Pension or other benefit schedule record	Possibly permanent, depending on nature of scheme
	Job application and interview/rejection records (unsuccessful applicants)	12 months
	Staff immigration records (Right to work etc)	Minimum – 2 years from end of employment
	Tier 2 migrant worker sponsor records	Minimum – 1 year from end of employment (none used at Queen's)
	Health records relating to employees	7 years from end of employment
INSURANCE RECORDS	Insurance policies (will vary – private, public, professional indemnity)	Duration of policy (or as required by policy) plus a period for any run-off arrangement and coverage of insured risks: ideally, until it is possible to calculate that no living person could make a claim.
	Correspondence related to claims/renewals/notification re: insurance	Minimum – 7 years (<i>but this will depend on what the policy covers and whether e.g. historic claims may still be made</i>)
ENVIRONMENTAL HEALTH & DATA GENERAL	Maintenance logs	10 years from date of last entry
	Accidents to children	25 years from birth (longer for safeguarding)
	Accident at work records (staff)	Minimum – 4 years from date of accident, but review on a case-by-case where possible
	Staff use of hazardous substances	Minimum – 7 years from end of date of use
	Covid-19 risk assessments, policies and other key documents	7 years from date of creation
	Risk assessments (carried out in respect of above)	7 years from completion of relevant project, incident, event or activity.
	Art.30 UK GDPR records of processing activity (ROPAs) and “Appropriate Policy Document” (if different) where relying on certain special category data processing grounds	No limit (as long as no personal data held), but must be kept up-to-date, accurate and relevant.
	Data protection impact assessments (DPIAs)	As Above
	Data Breach log / register.	Keep up to date and retain details of breaches for the last 6 years (where risk of claims) and at least 3 years in the ordinary course.