DATA PROTECTION POLICY

KRISHNAMURTI FOUNDATION TRUST

Core Policy, together with Schedule A: Brockwood Park School. Schedules for the Krishnamurti Centre and the Krishnamurti Foundation are in preparation.

Last Review Date	August 2026
Policy endorsed by	The Trustees (Core Policy); School Management Committee (Schedule A)
Policy is maintained by	Data Protection Officer (Tom Power)
Next review date	August 2027
Review body	School Management Committee

Table of contents

1. Introduction and Status of This Document

Krishnamurti Foundation Trust Ltd is a single legal entity and the data controller for the personal data it processes across all parts of its work, including Brockwood Park School. This policy sets out the principles, rights and responsibilities that apply across the Trust as a whole, and it is read together with a schedule for each part of the Trust's work that adds the detail specific to that setting.

Schedule A, below, carries the details for Brockwood Park School. Schedules for the Krishnamurti Centre and the Krishnamurti Foundation are in preparation and will be added to this policy as they are completed.

Where this policy and a schedule appear to differ on a point of detail, the schedule governs for that part of the Trust's work, because it is written for the people and the processing actually involved there.

2. The Data Controller

Krishnamurti Foundation Trust Ltd, of Brockwood Park, Bramdean, Hampshire SO24 0LQ, is the data controller for the personal data described in this policy and its schedules.

3. Data Protection Principles

The Trust processes personal data in accordance with the data protection principles set out in the UK GDPR: personal data must be processed lawfully, fairly and transparently; collected for specified, explicit and legitimate purposes; adequate, relevant and limited to what is necessary; accurate and kept up to date; kept for no longer than is necessary; and processed securely. The Trust is accountable for being able to demonstrate this, and this policy, together with the records and procedures that sit behind it, is part of how that accountability is met.

These principles are set out in the UK GDPR and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025 (together, "data protection law").

4. Roles and Responsibilities

The Trustees are accountable for the Trust's compliance with data protection law.

The Data Protection Officer, Tom Power, advises the Trust on its data protection obligations, monitors compliance, and is the point of contact for staff, students, parents and the Information Commissioner's Office on data protection matters. The Data Protection Officer also decides whether a new use of personal data, including a new AI tool, requires a Data Protection Impact Assessment.

The Data Protection Officer also holds the role of IT Manager. Where a decision touches both data protection and IT security, this overlap is recorded rather than left to be inferred, and the decision, with its reasoning, is reported to the Management Committee rather than made informally.

Each part of the Trust's work is responsible for complying with this policy and its own schedule, working with the Data Protection Officer. For the School, this responsibility sits with the School Management Committee, as set out in Schedule A.

5. Data Subject Rights

Anyone whose personal data the Trust holds has the right to ask to see it, to have inaccurate data corrected, and, in some circumstances, to have it erased, to restrict or object to its processing, or to receive it in a portable format. A request to exercise any of these rights (a "subject access request") should be made in writing to the Data Protection Officer. The Trust will respond within one month, extendable by a further two months for complex or numerous requests, and will explain if an extension is needed.

Some data is exempt from disclosure, including information that would identify another individual, information subject to legal professional privilege, examination scripts, and certain references. Schedule A sets out how these rights work in practice for students, given their age.

6. International Transfers

Personal data is sometimes transferred outside the UK — for example, through cloud services, or through AI tools used by staff. Where this happens, the Trust ensures the data continues to receive a standard of protection that is not materially lower than it would receive under UK data protection law, using a recognised safeguard such as adequacy regulations or standard contractual clauses, in line with the Data (Use and Access) Act 2025.

7. Shared Systems Used Across the Trust

Some systems are used by more than one part of the Trust's work. A register of these systems, and of the safeguard or assessment that applies to each, is being developed alongside the Centre and Foundation schedules. In the meantime, the systems the School uses, including AI tools, are set out in Schedule A.

8. Breach Reporting

Any suspected loss, theft, or unauthorised disclosure of personal data must be reported immediately, regardless of which part of the Trust's work it occurred in, following the Data Security Breach Incident Management Policy.

9. Queries and Complaints

Any question about how personal data is used, or a request to exercise a right under data protection law, should be directed to the Data Protection Officer, Tom Power (tom@brockwood.org.uk).

Anyone who believes the Trust has not complied with data protection law can complain to the Data Protection Officer directly, by any reasonable means. The complaint will be acknowledged within 30 days of receipt, and looked into in a way that is proportionate to what has been raised, with an update given if it will take longer than expected to resolve. A complainant can also complain to the Information Commissioner's Office at any time, whether or not they have complained to the Trust first, at ico.org.uk. A record is kept of when each complaint is received and acknowledged, the steps taken to look into it, and its outcome, so that this can be produced to the Information Commissioner's Office if requested.

10. Review

This policy is reviewed annually by the Data Protection Officer and approved by the Trustees, or sooner if the law or the Trust's practice changes materially.

SCHEDULE A – BROCKWOOD PARK SCHOOL

A1 Scope and Relationship to This Policy

This schedule applies to Brockwood Park School, and it sits alongside the policy above, adding the detail of how the School processes personal data about its students, their parents, and its staff. Where the two documents differ on a point that concerns the School, this schedule governs.

A2 Categories of Data Processed

The School processes personal data including, by way of example:

- names, addresses, telephone numbers, email addresses and other contact details;
- car details, for those who use the School's car parking;
- bank details and other financial information, for example about parents who pay fees;
- students' academic, disciplinary, admissions and attendance records, including information about any special educational needs, and examination scripts and marks;
- personnel files, including academic, employment and safeguarding records;
- information about health and welfare, and next of kin contact details, where relevant;
- references given or received about students, and information from previous schools or other professionals working with a student;
- correspondence with and about staff, students and parents, past and present; and
- images of students engaging in school activities, in accordance with the School's policy on taking, storing and using images of students.

A3 Rationale for Processing

Some of this processing is necessary to meet the School's legal duties, including its safeguarding duties, its duties under Keeping Children Safe in Education, and its statutory returns to the Department for Education. Some are necessary to perform the School Agreement with parents and students. Some is carried out in the School's legitimate interests, or those of another, where this is not outweighed by the impact on the individual concerned.

The School expects the following uses, among others, to fall within one of these lawful bases: admissions and confirming the identity of prospective students and their parents; providing education, pastoral care and extra-curricular activities, and monitoring students' progress and welfare; maintaining relationships with alumni and the wider school community, including fundraising; management planning, research and statistical returns required by law; giving and receiving references; enabling students to sit public examinations and publishing their results; monitoring use of the School's IT systems in accordance with its Technology, Internet

and Devices Policy; using images of students in accordance with the School's policy on taking, storing and using images of students; and cooperating with any complaints, disciplinary or investigation process.

Some of this processing involves special category data — health, ethnicity, religious belief, disability, or, exceptionally, criminal records information such as the results of a DBS check. This is processed only where the law allows it, most often for safeguarding, medical care, and employment purposes, or with explicit consent where this is required.

A4 Rights of Access – Students

A student can make a subject access request for their own personal data, provided they have sufficient maturity to understand the request they are making. Students aged 12 or over are generally assumed to have this maturity, although this depends on the individual student and what is being requested, and each request is considered on its own facts.

A parent will generally make a subject access request on behalf of a younger student, and a student of any age may ask a parent or another representative to make a request on their behalf.

The School will generally assume that a student consents to their personal data being shared with their parents, for example to keep parents informed of the student's progress, behaviour and welfare, unless there is good reason to do otherwise. Where a student raises a concern in confidence and does not want it shared with their parents, the School will maintain that confidence unless it judges, in the student's interests or those of other students, that it should not.

A5 Staff Use of AI Tools

Staff at Brockwood Park School use a range of artificial intelligence tools in their work, including generative AI chatbots and AI features built into everyday software. This section sets out what is expected when personal data is involved, so that staff use of AI develops within the same principles that govern every other use of personal data at the School, rather than as an exception to them.

This section does not cover students' own use of AI, which sits within the School's e-safety and safeguarding framework, addressed in the Online Safety Policy and the Online Safety Risk Assessment; nor does it cover purely personal use of a personal AI account, on a personal device, for non-work purposes.

Krishnamurti Foundation Trust Ltd remains the data controller for all personal data about students, staff and parents, whichever tool is used to process it. Where an AI provider receives personal data through a staff member's use of its tool, that provider becomes a data processor, and UK GDPR Article 28 requires a written contract covering matters including confidentiality, security, and any transfer of data outside the UK. A member of staff does not have individual authority to appoint a new processor by choosing, on their own initiative, to

put personal data into an AI tool: that decision, including whether a Data Protection Impact Assessment is needed, sits with the Data Protection Officer (see Section 4, above, on the Data Protection Officer's overlap with the IT Manager role).

Whichever tool is used, including one approved for work use, staff must not enter safeguarding or pastoral case detail; special category data; a name combined with identifying context, such as a behaviour incident, a medical need or a family circumstance; financial or banking detail; or anything that would let a reader work out who a specific student, parent or member of staff is, even without naming them — unless the particular use has been agreed with the Data Protection Officer in advance. Where AI assistance would genuinely help with this kind of material, the safer course is to anonymise or generalise first, for example describing "a Year 12 student with an EHCP" rather than using a name.

AI-generated content must be checked by the staff member before it is used or sent, and treated as a first draft rather than a finished answer. An AI tool must not be allowed to make, or effectively make, a decision affecting a specific student, parent or member of staff without a person reviewing it and taking responsibility for the outcome — reflecting both the accuracy principle in data protection law and the safeguards required where the Data (Use and Access) Act 2025 permits automated decision-making.

The tools currently approved for staff use with personal data, and the conditions attached to each, are set out at Appendix A5.1 to this schedule, kept up to date by the Data Protection Officer between full reviews of this policy so that an approval or a withdrawal doesn't wait on a full policy cycle. A tool not on that list should not be used with personal data without checking with the Data Protection Officer first, setting out which tool, what data would be involved, and what it would be used for.

If personal data is accidentally entered into a tool not approved for it, or an AI tool discloses something it should not, this is reported immediately as a data security breach under Section 8, above — deleting the chat afterwards is not a substitute for reporting, since a provider may retain the data regardless of what is deleted from the visible history.

Appendix A5.1

AI tools approved for staff use with personal data, current as at the date this schedule is approved. Maintained by the Data Protection Officer; the position for each tool may change between full reviews of this policy.

Tool	Who uses it	Status	Notes
Claude (Team account)	Staff (school-provided account)	Approved for work use	Covered by Anthropic's commercial terms, including the UK International Data Transfer Addendum; no training on Brockwood's chat or connector data by default. Filing the signed Data Processing Agreement and confirming connector retention terms are tracked separately. Follow the data minimisation rules above.
Google Gemini (Google Workspace for Education)	Students	Approved for student use	Covered by the Google Workspace for Education agreement; addressed further in the Online Safety Risk Assessment.
Google Gemini (Google Workspace)	Staff	Approved for work use, subject to the rules above	Covered by the same Google Workspace for Education agreement as other Workspace tools.
ChatGPT (individual accounts)	Some staff	Not yet assessed — do not use with personal data	No Article 28 contract or transfer safeguard has been confirmed for staff use of individual accounts.
Microsoft Copilot	Some staff	Not yet assessed — do not use with personal data	Status depends on account type (consumer or organisational licence); needs confirming before approval.
Leo (Brave browser AI assistant)	Some staff	Not yet assessed — do not use with personal data	No contract or terms review has been carried out.

Any other AI tool	—	Not approved by default	Contact the Data Protection Officer before use with personal data.

A6 Related School Documents

This schedule is read alongside: the Online Safety Policy and Online Safety Risk Assessment; the Technology, Internet and Devices Policy for Students; the Records Retention and Disposal Policy; the Data Security Breach Incident Management Policy; the IT Incident Response Plan and Back-Up Policy; and the School's Privacy Notices for staff, current and prospective parents, students aged 12 and above, and alumni and other supporters — all available on the School's website or on request from the Data Protection Officer.

A7 Governance and Review

This schedule is owned by the School Management Committee, which is responsible for its day-to-day application, working with the Data Protection Officer. It is reviewed annually alongside the policy above, or sooner if practice changes materially — for example, when a new AI tool is approved.