



DATA PROTECTION & GDPR POLICY

Data Protection & GDPR

London, United Kingdom

ravenscroftcollege.co.uk

Version 1.0 | 2026

DATA PROTECTION & GDPR POLICY

PURPOSE

This Data Protection and GDPR Policy sets out how Ravenscroft College collects, processes, stores, and protects personal data in compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and all relevant UK data protection legislation. The College is committed to upholding the rights of all data subjects and to maintaining the highest standards of data protection practice.

SCOPE

This policy applies to all personal data processed by Ravenscroft College, whether in digital or physical form. It covers data relating to learners, applicants, staff, contractors, visitors, and any other individuals whose personal data the College holds. It applies to all departments, staff, and third-party processors acting on the College's behalf.

This policy covers personal data processed in support of online delivery, including virtual learning environment activity, submitted assessment evidence, similarity and AI-detection reports where applicable, and records of correspondence with learners.

DATA CONTROLLER

Ravenscroft College is the data controller for all personal data collected and processed in the course of its operations. The Director is ultimately responsible for data protection compliance. Day-to-day data protection matters are managed by the designated data protection lead.

DATA PROTECTION PRINCIPLES

In accordance with UK GDPR, the College will ensure that personal data is:

- Processed lawfully, fairly, and in a transparent manner
- Collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes



RAVENS CROFT COLLEGE

- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept in a form which permits identification of data subjects for no longer than is necessary
- Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage

LAWFUL BASIS FOR PROCESSING

The College will identify and document a lawful basis for each processing activity before any personal data is processed. The lawful bases relied upon include:

- Consent of the data subject
- Performance of a contract with the data subject
- Compliance with a legal obligation
- Vital interests of the data subject or another person
- Public interest or official authority
- Legitimate interests of the College, where these do not override the data subject's rights

Where special category data is processed (e.g., health, ethnicity, religious beliefs), an additional condition under Article 9 UK GDPR will be identified and documented.

DATA SUBJECT RIGHTS

The College recognises and upholds the following rights of data subjects under UK GDPR:

- Right to be informed about how personal data is collected and used
- Right of access to personal data held by the College (Subject Access Request)
- Right to rectification of inaccurate or incomplete data
- Right to erasure ('right to be forgotten') where there is no compelling reason to retain the data



RAVENSCROFT COLLEGE

- Right to restrict processing
- Right to data portability
- Right to object to processing, including processing for direct marketing
- Rights in relation to automated decision-making and profiling

Requests to exercise any of these rights should be submitted in writing to dataprotection@ravenscroftcollege.co.uk. The College will respond within one calendar month, or within an extended timeframe of up to three months where the request is complex, with notification to the data subject.

Subject Access Requests

A learner or member of staff may request a copy of the personal data the College holds about them, including their submitted work, assessor feedback and virtual learning environment activity records. The request is a Subject Access Request and, with the words Subject Access Request in the subject line, stating what is being asked for and enough information to identify the requester. No fee is charged. The College responds within one calendar month of receiving the request, and may extend that by up to two further months where the request is complex, in which case it will say so within the first month and explain why. Where records contain personal data about another person, the College will assess whether that material can be redacted and will explain any redaction. All Subject Access Requests are logged.

Data Security

The College implements appropriate technical and organisational measures to protect personal data, including:

- Encryption of personal data in transit and at rest where appropriate
- Access controls restricting personal data to authorised personnel only
- Regular security assessments and vulnerability testing
- Secure disposal of personal data at the end of the retention period
- Staff training on data protection responsibilities and best practice
- Documented procedures for responding to data breaches



Access to assessment evidence and exported evidence packages is restricted to authorised staff and is recorded in an access log capturing user identity, date and time, reason for access and action taken. The College maintains an Evidence Register for assessment-related exports to preserve the chain of custody for appeals, malpractice investigations and external quality assurance requests.

DATA PROTECTION IMPACT ASSESSMENTS AND THIRD-PARTY PROCESSORS

The College will complete a Data Protection Impact Assessment for any processing likely to result in a high risk to the rights and freedoms of individuals. All third-party processors, including the virtual learning environment and the similarity and AI-detection service, must have a signed Data Processing Agreement specifying data types, retention, security measures, access controls, sub-processor lists and cross-border transfer safeguards.

DATA BREACHES

In the event of a personal data breach, the College will follow its Data Breach Procedure. Unless a breach is unlikely to result in a risk to the rights and freedoms of individuals, the College will notify the Information Commission without undue delay and, where feasible, not later than 72 hours after becoming aware of it. Where the breach is likely to result in a high risk to affected individuals, those individuals will be notified directly without undue delay.

DATA SHARING AND THIRD-PARTY PROCESSORS

The College may share personal data with third parties where necessary and lawful, including the awarding body, OTHM Qualifications, regulatory bodies, IT service providers and professional advisors. All third-party processors are required to enter into a Data Processing Agreement with the College that meets the requirements of UK GDPR.

INTERNATIONAL TRANSFERS

Where personal data is transferred outside the United Kingdom, the College will ensure that appropriate safeguards are in place, including Standard Contractual Clauses, adequacy decisions, or other mechanisms approved under UK GDPR.

DATA RETENTION

Assessment evidence, virtual learning environment export packages and similarity reports where applicable, used to support assessment decisions, appeals, complaints or malpractice investigations are retained for a minimum of three years from the date of the final decision, or longer where the awarding body requires it, in accordance with the Evidence Retention and Records Management Policy. All deletion actions are logged.

TRAINING AND AWARENESS

All staff will receive data protection training at induction and refresher training at least annually. Staff with specific data protection responsibilities will receive enhanced training appropriate to their role.

COMPLAINTS

Any individual who believes that their personal data has been mishandled or that the College has breached its data protection obligations may raise a complaint through the College's Complaints Policy. They also have the right to lodge a complaint with the Information Commission at ico.org.uk.

OPERATIONAL LINKAGES

Operational procedures for evidence handling, retention and disclosure are set out in the Assessment and Internal Verification Policy, the Academic Integrity, Malpractice and Maladministration Policy, the Academic Appeals Policy and the Complaints Policy. Those documents must be read together with this one, and any processing of personal data arising from them is governed by this policy.



RAVENSCROFT COLLEGE

REVIEW

This policy will be reviewed annually or following any data breach, significant change in legislation, or update to regulatory or awarding body expectations.

Last reviewed: October 2026