

Privacy Notice

Results Consortium Limited

Last Updated: May 2026 | **Next Review:** May 2027

Data Protection Officer: Dominic Hammond: dpo@resultsco.org.uk

1. About Us

Results Consortium Limited is committed to protecting your personal data and respecting your privacy. We respect and value the privacy of all our clients, students and staff, and will only collect and use personal data as described in this notice, consistently with our obligations and your rights under the law.

Detail	Information
Registered Name	Results Consortium Limited
Company Number	04372425 (England & Wales)
Registered Address	London East-UK Business Technology Park, Yewtree Avenue, Dagenham, England, RM10 7FN
VAT Number	937567184
Data Controller Email	datacontroller@resultsco.org.uk
Telephone	+44 20 3961 7036

2. What Does This Notice Cover?

This Privacy Notice explains how we use your personal data: how it is collected, how it is held and how it is processed. It also explains your rights under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

3. What Is Personal Data?

Personal data is any information relating to an identifiable living person. Under the UK GDPR, this covers obvious information such as your name and contact details, but also less obvious information such as identification numbers, electronic location data, and online identifiers.

Special category data is a subset of personal data that warrants a higher level of protection. This includes information about health, disability, ethnicity, religion and similar sensitive characteristics. Where we process special category data, we do so only where an additional lawful basis under Article 9 UK GDPR applies.

4. What Personal Data Do We Collect?

We may collect some or all of the following personal data, depending on your relationship with us:

- Name
- Date of birth
- Gender
- Address
- Email address
- Telephone number
- Business name, job title and profession
- Information about your preferences and interests
- Special / sensitive category data such as ethnicity, disability, or health information (where relevant to your course or support needs)

5. How Do We Use Your Personal Data?

Under the UK GDPR, we must always have a lawful basis for using personal data. The table below sets out each purpose and the specific lawful basis we rely on.

Purpose	Lawful Basis (UK GDPR)
Providing and managing your account and registration	Performance of a contract (Art. 6(1)(b))
Delivering course materials, documents and assignment content	Performance of a contract (Art. 6(1)(b))
Sending essential service emails (enrolment, results, timetables)	Performance of a contract (Art. 6(1)(b)) — cannot be opted out of
Communicating with you in response to enquiries	Legitimate interests (Art. 6(1)(f))
Statutory reporting to OfS and HESA	Legal obligation (Art. 6(1)(c))
Sharing data with awarding bodies and partner universities	Performance of a contract (Art. 6(1)(b))
Student finance administration (Student Loans Company)	Legal obligation (Art. 6(1)(c))
Sending newsletters, promotional updates and course news (optional)	Consent (Art. 6(1)(a)) — you may withdraw at any time
Building a profile of learning interests based on activity	Consent (Art. 6(1)(a))
CCTV monitoring for safety and security	Legitimate interests (Art. 6(1)(f))
Processing health, disability or ethnicity data for support or compliance	Substantial public interest / explicit consent (Art. 9(2)(g) and Art. 9(2)(a)).
Safeguarding and welfare	Vital interests / substantial public interest Art. 6(1)(c) and 9(2)(b)

Marketing and Communication Preferences

We will only send you newsletters, promotional updates, or non-essential communications where you have given your explicit consent. You may withdraw consent at any time by:

- Emailing: datacontroller@resultsco.org.uk
- Using the unsubscribe link in any marketing email

Withdrawing marketing consent does not affect essential service communications required to deliver your course.

Automated Decision-Making and Profiling

Results Consortium Limited does not normally make decisions based solely on automated processing that produce legal or similarly significant effects on individuals under Article 22 of the UK GDPR.

We may use limited learning analytics, reporting tools, or automated systems to support student engagement monitoring, regulatory compliance, safeguarding, attendance monitoring, and academic administration. Any significant decisions affecting individuals involve meaningful human oversight.

You have the right to request further information about any automated processing and to request human review where applicable.

6. Special Category Data

Some of our programmes, including those in Health and Social Care, may require us to process special category data as defined under Article 9 of the UK GDPR. This may include information relating to physical or mental health, disability, ethnicity, or safeguarding concerns.

Where we process special category data, we do so on one or more of the following additional lawful bases:

- Substantial public interest (Schedule 1, DPA 2018) for safeguarding and equality monitoring
- Explicit consent where you have provided your clear agreement
- Vital interests in emergency or safeguarding situations

Special category data is treated with the highest level of care, accessible only to authorised staff and never used for marketing purposes.

7. How Long Do We Keep Your Personal Data?

We retain your personal data only for as long as necessary to fulfil the purposes for which it was collected, including legal, regulatory and contractual obligations.

Data Category	Retention Period	Basis
Student registration and enrolment records	6 years after course completion	Regulatory / legal obligation
Financial and funding records (incl. HMRC)	6 years	Legal obligation
Assessment and academic records	5 years after course completion	Regulatory requirement
CCTV footage	30 days (longer if investigation required)	Legitimate interests
Marketing consent records	Until withdrawn	Accountability (Art. 5(2) UK GDPR)
Website analytics (cookies)	Up to 2 years	Consent

8. How and Where Do We Store or Transfer Your Personal Data?

We store your personal data within the UK, where it is subject to the full protections of the UK GDPR and the Data Protection Act 2018.

Access to our systems is managed through administratively controlled SharePoint logins. Only authorised staff can access personal data.

In limited cases, personal data may be accessed by a third-party IT contractor located outside the UK. Where this occurs, appropriate safeguards are in place, including a Data Processing Agreement incorporating an International Data Transfer Agreement (IDTA), ensuring protection equivalent to UK GDPR standards.

9. Do We Share Your Personal Data?

We share your personal data only where necessary, lawful and with appropriate safeguards in place. We do not sell, rent, or commercially disclose your personal data to third parties for marketing or advertising purposes.

Recipient	Purpose	Lawful Basis
Office for Students (OfS)	Regulatory reporting	Legal obligation
HESA / JISC	Statutory data returns	Legal obligation
Student Loans Company (SLC)	Student finance administration	Legal obligation
Awarding bodies / partner universities	Assessment and certification	Performance of contract
Employer Data Record Service (EDRS)	Employer registration records	Legal obligation
Employers (where relevant)	Work placements / progression opportunities	Consent / legitimate interests
Third-party IT contractor	IT infrastructure support	Legitimate interests (IDTA safeguards)
Courts / government authorities	Legal proceedings or statutory obligation	Legal obligation

Where any personal data is shared with a third party, we take steps to ensure it is handled safely and securely, in accordance with your rights and our obligations under the UK GDPR.

10. CCTV Data

The College uses closed-circuit television (CCTV) at its premises to help keep staff, students, visitors and property safe, and to support the prevention and detection of crime.

Why We Use CCTV

CCTV cameras may record images of anyone present in monitored areas. We do this on the basis of our legitimate interests in maintaining a safe and secure environment, and where required, to meet our legal obligations.

Storage and Retention

All CCTV recordings are held securely and accessible only to authorised staff. Footage is retained for 30 days, then securely deleted, unless needed in connection with an ongoing investigation, a safeguarding concern, or legal proceedings.

Sharing Footage

We may share CCTV footage with the police or other lawfully authorised bodies where it is necessary, proportionate, and lawful to do so.

Signage

Clear notices are displayed in all areas covered by CCTV to inform individuals that recording is taking place.

11. Cookies

We use cookies and similar technologies on our website and learning platforms (Canvas and Moodle). Some cookies are essential for the platforms to function; others help us improve our services. Where required by law, we will request your consent before placing non-essential cookies on your device. See the Results Consortium Privacy Policy for more details.

12. Your Rights as a Data Subject

Under the UK GDPR, you have the following rights, which we will always work to uphold:

Right	What it Means
Right to be informed	To know how your data is collected and used, as described in this notice.
Right of access	To request a copy of the personal data we hold about you (Subject Access Request).
Right to rectification	To ask us to correct inaccurate or incomplete data.
Right to erasure	To ask us to delete your data, subject to legal or regulatory obligations.
Right to restrict processing	To ask us to limit how we use your data in certain circumstances.
Right to object	To object to processing based on legitimate interests, or to direct marketing.
Right to data portability	To receive your data in a structured, portable format where processing is consent- or contract-based and automated.
Rights related to automated decision-making and profiling	To request human review of any automated decision made about you.

For further information about your rights, visit the Information Commissioner's Office at www.ico.org.uk or contact your local Citizens Advice Bureau. You have the right to lodge a complaint with the ICO if you believe your rights have been breached.

13. How Can You Access Your Personal Data?

To request a copy of the personal data we hold about you, please submit a Subject Access Request (SAR) in writing to the email or postal address in Section 14, clearly marking it as a 'Subject Access Request'.

We do not normally charge a fee for a SAR. However, a reasonable fee may be charged where a request is manifestly unfounded or excessive. We will respond within one month of receiving your request. In complex cases, this may extend to three months. We will keep you informed throughout.

14. How to Contact Us

To contact us about your personal data, data protection matters, or to submit a Subject Access Request, please use the details below. We will respond as soon as possible.

Email: datacontroller@resultsco.org.uk

DPO Email: dpo@resultsco.org.uk

Telephone: +44 20 3961 7036

Postal Address: London East-UK Business Technology Park, Yewtree Avenue, Dagenham, England, RM10 7FN

15. Changes to This Privacy Notice

We may update this Privacy Notice from time to time, for example, if the law changes or if we change our business in a way that affects how we handle personal data.

Where we make significant changes, we will notify you by email (where you have not opted out of communications) and will update the 'Last Updated' date at the top of this document. We encourage you to review this notice periodically. Continued use of our services following notification of any changes will constitute acceptance of those changes.