

Westminster Tutors



Data Protection Policy

2026-2027

Contents

1. Introduction & Process	1
2. Legislation and guidance.....	1
3. Definitions	1
4. The Data Controller.....	2
5. Roles and responsibilities	2
6. Data Protection Principles	3
7. Collecting Personal Data	3
8. Sharing Personal Data	4
9. Subject Access Requests and Other Rights of Individuals	5
10. Parental Requests to see the Educational Record	6
11. Biometric Recognition Systems	6
12. CCTV	8
13. Photographs and Videos	8
14. Data Protection by Design and Default	9
15. Data Security and Storage of Records	9
16. Disposal of Records	10
17. Personal Data Breaches	10
18. Training	10
Appendix I: Personal Data Breach Procedure	11

1. Introduction & Process

- 1.1 Data and information collected, analysed, stored, communicated, and reported upon may be subject to theft, misuse, loss, and corruption. Poor education and training, as well as the breach of security controls, may also put data and information at risk.
- 1.2 Data breaches and information security incidents can give rise to embarrassment, financial loss, non-compliance with standards and legislation, and possible judgments being made against Westminster Tutors.
- 1.3 Westminster Tutors aims to ensure that all personal data collected about staff, teachers, students, parents, visitors and other individuals is collected, used, stored, shared and disposed of in accordance with the [UK General Data Protection Regulation](#), the [Data Protection Act 2018](#) and other applicable data protection legislation. This policy applies to personal data held in both electronic and paper form.

2. Legislation and guidance

- 2.1 This policy reflects the requirements of the [UK General Data Protection Regulation](#), the [Data Protection Act 2018](#) and the [Data \(Use and Access\) Act 2025](#), together with relevant guidance issued by the [Information Commissioner's Office](#).

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data, which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics • Health – physical or mental • Sex life or sexual orientation

Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing, or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing personal data.
Data processor	A person or body other than an employee of the data controller who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, personal data.

4. The Data Controller

- 4.1 Westminster Tutors processes personal data relating to parents, students, staff, teachers, visitors, and others, acting as a data controller.
- 4.2 The college is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

- 5.1 This policy applies to all our college staff, teachers, external organisations, and individuals working on our behalf. Staff and teachers who do not comply with this policy may face disciplinary action.

Proprietor, Principal and Senior Leadership Team (SLT)

- 5.2 The Proprietor has overall responsibility for ensuring that Westminster Tutors complies with its legal obligations under data protection legislation.
- 5.3 The Principal is responsible for the day-to-day oversight of data protection compliance, including responding to data protection requests, maintaining relevant records, managing personal data breaches, and ensuring that staff and teachers receive appropriate guidance and training.

Data Protection Officer

- 5.4 Westminster Tutors has assessed whether it is required to appoint a Data Protection Officer under Article 37 of the UK GDPR and has concluded that it does not currently meet the statutory criteria. The college will keep this assessment under review. Data protection enquiries should be directed to the Principal at info@westminstertutors.co.uk.

All staff and teachers

5.5 Staff and teachers are responsible for:

- Processing personal data only as authorised and in accordance with this policy.
- Informing Westminster Tutors promptly of relevant changes to their own personal data.
- Contacting the Principal or SLT promptly if:
 - They have questions about this policy, data protection law, retention, or security;
 - They are concerned that this policy is not being followed;
 - They are unsure whether personal data may lawfully be processed or shared;
 - They receive a request concerning an individual's data protection rights;
 - They become aware of an actual or suspected personal data breach;
 - They propose a new activity that may significantly affect individuals' privacy; or
 - They need to engage a processor, share personal data with a third party, or make a restricted transfer to an organisation outside the UK.

6. Data Protection Principles

6.1 The GDPR is based on data protection principles that our college must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes;
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed;
- Accurate and, where necessary, kept up to date;
- Kept for no longer than is necessary for the purposes for which it is processed; and
- Processed in a way that ensures it is appropriately secure.

7. Collecting Personal Data

Lawfulness, Fairness and Transparency

7.1 Westminster Tutors will process personal data only where it has identified and documented an appropriate lawful basis. Depending on the circumstances, this may be:

- Processing necessary to enter into or perform a contract with the individual;
- Processing necessary to comply with a legal obligation;
- Processing necessary to protect someone's vital interests;
- Processing necessary for the legitimate interests of Westminster Tutors or a third party, except where those interests are overridden by the individual's interests, rights or freedoms;
- Processing necessary for a task carried out in the public interest or in the exercise of an official function, where that task or function has a clear basis in law; or
- The individual having given valid consent for a specified purpose.

7.2 Where Westminster Tutors processes special-category personal data, it will identify both an appropriate lawful basis under Article 6 of the UK GDPR and an additional condition under Article 9 and, where applicable, Schedule 1 of the Data Protection Act 2018. Where consent is relied upon for special-category data, it must be explicit.

Limitation, Minimisation and Accuracy

- 7.3 We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.
- 7.4 If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.
- 7.5 Staff and teachers must only process personal data where necessary to do their jobs.
- 7.6 When staff and teachers no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the college's record retention policy.

8. Sharing Personal Data

- 8.1 Westminster Tutors will share personal data only where there is a lawful basis for doing so, and the disclosure is necessary, proportionate and limited to relevant information. Depending on the circumstances, personal data may be shared:
- With safeguarding, health, emergency, law-enforcement or local-authority services where necessary to protect an individual or meet a legal or safeguarding obligation;
 - With parents, carers or other authorised representatives where appropriate and lawful;
 - with awarding bodies, examination organisations, universities, local authorities or other education providers where necessary for educational administration or progression;
 - With suppliers, professional advisers or contractors who require the information to provide services to Westminster Tutors; or
 - Where the individual has given valid consent.
- 8.2 Consent will be relied upon only where it is the appropriate lawful basis. Westminster Tutors will not seek consent where another lawful basis applies and seeking consent would be inappropriate, impracticable, or inconsistent with its legal or safeguarding responsibilities.
- 8.3 Westminster Tutors may share personal data with law-enforcement, government, regulatory or judicial bodies where disclosure is required by law or where another appropriate lawful basis applies. Any disclosure will be necessary, proportionate and limited to relevant information. This may include disclosures concerning:
- The prevention, investigation or detection of crime or fraud;
 - The apprehension or prosecution of offenders;
 - The assessment or collection of tax by HMRC;
 - Legal proceedings, court orders or the exercise or defence of legal rights; or
 - Safeguarding or the protection of an individual.
- 8.4 We may also share personal data with emergency services and local authorities to help them respond to an emergency affecting any of our students, staff, or teachers.
- 8.5 Where Westminster Tutors makes a restricted transfer of personal data outside the UK, it will ensure that the transfer is permitted under applicable data protection law, including through UK adequacy regulations, appropriate safeguards or a relevant statutory exception.

9. Subject Access Requests and Other Rights of Individuals

Subject Access Requests

- 9.1 Subject to any applicable exemption, an individual making a subject access request is entitled to:
- Confirmation of whether their personal data is being processed;
 - A copy of their personal data;
 - The purposes of the processing and categories of personal data concerned;
 - The recipients or categories of recipients to whom the data has been or will be disclosed;
 - The applicable retention period or, where this is not possible, the criteria used to determine it;
 - Information about the source of the data where it was not obtained from the individual;
 - Information about applicable rights, including the right to request rectification, erasure or restriction, to object to processing, and to complain to the ICO;
 - Information about relevant safeguards where personal data is transferred outside the UK; and
 - Where applicable, meaningful information about solely automated decision-making, including the logic involved and its significance and envisaged consequences for the individual.
- 9.2 A subject access request may be made verbally or in writing and does not need to use the words “subject access request”. Requests should preferably be directed to the Principal at info@westminstertutors.co.uk. Any staff member or teacher who receives a request for access to personal data must forward it to the Principal without delay. Westminster Tutors may ask for information reasonably required to verify the requester’s identity, confirm their authority to act for another person, or clarify the information requested.

Children and Subject Access Requests

- 9.3 A child is the data subject in relation to personal data held about them and may exercise their own data protection rights where they are competent to do so. Whether a parent or carer may exercise the child’s right of access on their behalf depends on the child’s competence, any authority given by the child, and the particular circumstances. Further information is available in the ICO’s guidance on children and subject access requests: [A guide to subject access | ICO: Children](#)
- 9.4 A student’s competence to exercise their data protection rights will be assessed on a case-by-case basis, taking account of their maturity, understanding, the nature and sensitivity of the information, and the consequences of exercising the right. Where a student is competent, Westminster Tutors will normally respond directly to them unless they have authorised another person to act on their behalf. Where a student is not competent, a person with parental responsibility may ordinarily exercise the student’s rights on their behalf where this is consistent with the student’s best interests.
- 9.5 Data requests for adults (individuals over 18) must be made by the individual, not by their parents, carers or any other third party, unless that third party is entitled to do so. It is the responsibility of the third party to provide proof of this entitlement, for instance, a written authority signed by the individual. Further information can be found at: [A guide to subject access | ICO](#)

Responding to Subject Access Requests

- 9.6 Westminster Tutors will respond to a subject access request without undue delay and normally within one month. Where necessary because the request is complex or the individual has made several requests, the response period may be extended by up to two further months. The individual will be informed of any extension and the reasons for it within the initial one-month period.
- 9.7 Westminster Tutors will not normally charge a fee. A reasonable fee may be charged, or the request may be refused in whole or in part, where it is manifestly unfounded or excessive. A reasonable fee may also be charged for additional copies of information already provided. Any refusal or fee will be considered individually and explained to the requester.
- 9.8 Each repetitive request will be assessed individually to determine whether it is manifestly unfounded or excessive. Westminster Tutors may charge a reasonable fee based on its administrative costs for further copies of the same personal data. Any fee will be explained before the request is processed.
- 9.9 When we refuse a request, we will tell the individual why, and they have the right to complain to the ICO.

Other Data Protection Rights of the Individual

- 9.10 In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:
- Withdraw their consent to processing at any time;
 - Ask us to rectify, erase or restrict the processing of their personal data or object to its processing (in certain circumstances);
 - Prevent the use of their personal data for direct marketing;
 - Challenge processing, which has been justified based on public interest;
 - Request a copy of agreements under which their personal data is transferred outside of the UK or the European Economic Area;
 - Object to decisions based solely on automated decision-making or profiling (decisions taken with no human involvement that might negatively affect them);
 - Prevent processing that is likely to cause damage or distress;
 - Be notified of a data breach in certain circumstances;
 - Make a complaint to the ICO; and
 - Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)
- 9.11 Individuals should submit any request to exercise these rights to the Principal. If staff and teachers receive such a request, they must immediately forward it to the Principal.

10. Parental Requests to see the Educational Record

- 10.1 Westminster Tutors is not a maintained school. Parents and carers do not therefore have a separate statutory right under the Education (Pupil Information) (England) Regulations 2005 to inspect a student's educational record.

- 10.2 Personal data held about a student relates to the student as the data subject. A request for access to a student's personal data or educational information will be considered under the UK GDPR, the Data Protection Act 2018 and any other applicable legislation.
- 10.3 Westminster Tutors routinely shares specified information about a student's attendance, academic progress, assessment outcomes and engagement with identified parents, carers or fee-payers as part of its educational and contractual arrangements. The categories of information shared, the recipients, the purposes of sharing and the applicable lawful basis are explained in the Student Privacy Notice. Pastoral, health, safeguarding or other sensitive information will be shared only where there is an appropriate lawful basis and, where required, an additional condition for processing special-category data.
- 10.4 Where a student under 18 is competent to exercise their own data protection rights, a parent or carer may make a subject access request on the student's behalf only where the student has authorised them to do so. Where the student is not competent to exercise those rights, a person with parental responsibility may ordinarily exercise them on the student's behalf, provided that this is consistent with the student's best interests. The right of access belongs to the student.
- 10.5 Where a student is aged 18 or over, a parent, carer or fee-payer has no automatic right under UK data protection law to access the student's personal data or educational information solely because of their parental involvement or payment of the student's fees. However, Westminster Tutors normally shares specified routine information about the student's attendance, academic progress, assessment outcomes and engagement with identified parents, carers or fee-payers where this is necessary for its legitimate interests or those of the recipient and those interests are not overridden by the student's rights and interests.
- 10.6 The nature, purpose and extent of this routine sharing will be explained to the student through the Student Privacy Notice and, where appropriate, the enrolment arrangements. Sharing will be limited to information that is relevant and proportionate to the educational services being provided.
- 10.7 A student aged 18 or over may object to this routine sharing. Westminster Tutors will consider the objection in accordance with applicable data protection law, taking account of the student's circumstances, the reasons for the objection and the legitimate interests supporting continued sharing. Information may also be disclosed where another lawful basis applies, including where disclosure is required by law or is necessary and proportionate for safeguarding purposes.
- 10.8 Routine reporting to a parent, carer or fee-payer does not give that person an unrestricted right to the student's full educational record, correspondence, safeguarding information or other personal data. Any separate request for access will be considered under the subject access provisions in section 9.
- 10.9 Westminster Tutors may withhold or limit information where disclosure would be unlawful, would disclose another person's personal data or confidential information, would conflict with safeguarding responsibilities, or would otherwise be inappropriate under applicable data protection law.

11. Biometric Recognition Systems

- 11.1 Westminster Tutors uses an automated biometric recognition system to identify authorised users and control access to the college premises. Biometric data used to identify an individual uniquely is special-category personal data.
- 11.2 Westminster Tutors processes this data on the basis of consent under Article 6(1)(a) of the UK GDPR and explicit consent under Article 9(2)(a). Participation is optional. Consent must be specific, informed, freely given, and capable of being withdrawn at any time without disadvantage. An equivalent non-biometric method of entry will always be available.
- 11.3 For a student under 18, Westminster Tutors will obtain the student's explicit consent where they are competent to provide it. The College will also follow the safeguards contained in the Protection of Freedoms Act 2012 and relevant Department for Education guidance as a matter of policy. Parents or carers will be notified, written consent will be obtained from at least one parent or carer, and the student's biometric data will not be processed if the student or a parent or carer objects.
- 11.4 For students aged 18 or over, staff, independent teachers, and other authorised adults, Westminster Tutors will obtain the individual's explicit consent. Refusing or withdrawing consent will not affect the individual's access to the premises or otherwise place them at a disadvantage.
- 11.5 Westminster Tutors has completed a Data Protection Impact Assessment and risk assessment for the biometric system, which can be found in Appendix II. The assessment addresses the necessity and proportionality of the system, alternative access methods, risks to individuals, accuracy, security, retention, and the responsibilities of Westminster Tutors and its system provider. It will be reviewed periodically and before any material change to the system or its use.
- 11.6 Westminster Tutors will apply appropriate technical and organisational measures to protect biometric templates and related records. Biometric data will be used only for authorised access, maintaining occupancy records and supporting emergency evacuation procedures. Biometric templates will be retained only while the individual requires access and continues to consent. They will be securely deleted promptly when the individual leaves Westminster Tutors, no longer requires access, or withdraws consent.

12. CCTV

- 12.1 We use CCTV in designated entrance, circulation and examination-security areas for safeguarding, access control, crime prevention, protection of property and examination materials, and investigation of specific incidents. We will adhere to the ICO's guidance for the use of CCTV.
- 12.2 We do not need to ask individuals' permission to use CCTV, but we clarify where individuals are being recorded. Security cameras are visible and accompanied by prominent signs explaining that CCTV is in use.
- 12.3 Any enquiries about the CCTV system should be directed to the Principal.

13. Photographs and Videos

- 13.1 We obtain written consent from parents/carers, or students aged 18 and over, for the use of students' photographs and videos for communication, marketing and promotional materials to be taken in our Client Terms and Conditions and through our Over-18 Annex Form. Uses may include:
- Internal displays and college publications;
 - Printed marketing and promotional materials;
 - The Westminster Tutors website;
 - Westminster Tutors' social media accounts; and
 - Publication or use by a specifically identified external organisation.
- 13.2 Consent is optional and may be withdrawn at any time by contacting Westminster Tutors. Withdrawal will not affect the lawfulness of any use made before consent was withdrawn. Westminster Tutors will cease future use and, where reasonably practicable, remove the image from materials and channels within its control. It may not be possible to recall printed materials already distributed or copies already published or retained by others.
- 13.3 When publishing photographs or videos, Westminster Tutors may identify a student by their forename or initials. It will not normally publish the student's full name or other identifying personal information alongside the image. A full name or additional personal information will be used only where appropriate consent has been obtained in advance and where publication does not present a safeguarding risk.

14. Data Protection by Design and Default

- 14.1 We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in the relevant data protection law;
 - Completing privacy impact assessments where the college's processing of personal data presents a high risk to individuals' rights and freedoms, and when introducing new technologies;
 - Integrating data protection into internal documents, including this policy, any related policies and privacy notices;
 - Regularly training members of staff and teachers on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance;
 - Regularly conducting reviews and audits to test our privacy measures and ensure compliance;
 - Maintaining accurate privacy notices that explain how Westminster Tutors processes personal data;
 - Maintaining a written record of relevant processing activities, including the purposes of processing, categories of individuals and personal data, recipients, international transfers and safeguards, retention periods, and a general description of security measures; and
 - Reviewing and updating these records whenever processing activities materially change.

15. Data Security and Storage of Records

- 15.1 We will protect personal data and keep it safe from unauthorised access, alteration, processing or disclosure and against accidental or unlawful loss, destruction or damage. In particular:
- Paper records must be secured when not in use. Laptops, tablets, smartphones, portable devices, and removable storage media containing personal data must use appropriate encryption and access controls. Personal data must not be stored on unencrypted removable media;

- Papers containing confidential personal data must not be left on office and classroom desks, staff and teachers' room tables, pinned to notice/display boards, or anywhere else with general access;
- Where personal information must be taken off-site, staff and teachers must sign in and out of the college office;
- College computers, laptops, and other electronic devices require passwords that are at least eight characters long and contain letters and numbers. Staff, teachers, and students are reminded to change their passwords regularly;
- Staff and teachers or students who store personal information on their devices must follow the same security procedures as for college-owned equipment; and
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

16. Disposal of Records

- 16.1 Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or outdated will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred or incinerate paper-based records, overwrite or delete electronic files and ensure any backup files are also deleted.

17. Personal Data Breaches

- 17.1 The college will make all reasonable endeavours to ensure no personal data breaches.
- 17.2 In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix I.
- 17.3 Where a personal data breach is likely to result in a risk to individuals' rights and freedoms, Westminster Tutors will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of it. Where the breach is likely to result in a high risk, affected individuals will also be informed without undue delay. Breaches requiring careful risk assessment may include:
- Publication of a non-anonymised dataset on the college website;
 - Safeguarding information being made available to an unauthorised person; or
 - Loss or theft of an unencrypted college device containing students' personal data.

18. Training

- 18.1 All staff and teachers receive data protection training during their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the college's processes are necessary.

19. Complaints

- 19.1 An individual who wishes to make a complaint about Westminster Tutors' handling of personal data or compliance with data protection law should use the College's Complaints Procedure, which is set out in the Complaints Policy available on the Westminster Tutors website. Westminster Tutors will acknowledge the complaint within 30 days, investigate it without undue delay, keep the complainant

appropriately informed of its progress, and communicate the outcome. The complainant may also raise the matter with the Information Commissioner's Office.

Appendix I: Personal Data Breach Procedure

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

- When finding or causing a breach or potential breach, the staff member, teacher, or data processor must immediately notify the principal or SLT.
- The Principal or member of the SLT will investigate the report and determine whether a breach has occurred. To decide, the Principal/SLT will consider whether personal data has been accidentally or unlawfully:
 - lost
 - stolen
 - destroyed
 - altered
- disclosed or made available where it should not have been
- made available to unauthorised people
- The Principal will alert the proprietor.
- The Principal/SLT will make all reasonable efforts to contain and minimise the breach's impact, assisted by relevant staff and teachers, members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure.)
- The Principal/SLT will assess the potential consequences based on their severity and likelihood.
- The Principal will determine whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the Principal will consider whether the breach is likely to affect people's rights and freedoms negatively and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
 - Loss of control over their data.
 - Discrimination.
 - Identity theft or fraud.
 - Financial loss.
 - Unauthorised reversal of pseudonymisation (for example, key-coding).
 - Damage to reputation.
 - Loss of confidentiality.
 - Any other significant economic or social disadvantage to the individual(s) concerned.
- If the Principal reasonably believes there will be a risk to people's rights and freedoms, the Principal must notify the ICO.
- The Principal will document the decision (either way) if it is challenged later by the ICO or an individual affected by the breach. Documented decisions are stored on the Google Drive Cloud.
- Where the ICO must be notified, the Principal will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the Principal will set out:
 - A description of the nature of the personal data breach, including, where possible:
 - The categories and approximate number of individuals concerned.
 - The categories and approximate number of personal data records concerned.
 - The name and contact details of the Principal.
 - A description of the likely consequences of the personal data breach.
 - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

If all the above details are not yet known, the Principal will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the Principal expects to have further information. The Principal will submit the remaining information as soon as possible.

The Principal will also assess the severity and likelihood of potential harm to individuals. Where the breach is likely to result in a high risk to individuals' rights and freedoms, affected individuals will be informed without undue delay in clear and plain language. The notification will include:

- A description of the nature of the personal data breach;
- The name and contact details of the Principal or another appropriate contact;
- A description of the likely consequences of the breach; and
- A description of the measures taken or proposed to address the breach and mitigate its possible adverse effects.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breaches, focusing primarily on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information is being disclosed via email (including safeguarding records).

If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.

Members of staff and teachers who receive personal data sent in error must alert the sender and the Principal as soon as they become aware of the error and confirm its deletion.

In any case where the recall is unsuccessful, the Principal will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and not share, publish, save or replicate it in any way.

The Principal will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.

The Principal will conduct an internet search to ensure that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that it be removed from their website and deleted.

A college laptop containing non-encrypted sensitive personal data is being stolen or hacked.

- Where a laptop is lost or stolen, the incident must be reported to the Principal immediately. Westminster Tutors will take prompt steps to secure the device and associated accounts, including remote locking or deletion where available, and will assess the nature and sensitivity of the personal data involved, the effectiveness of encryption and access controls, and the likelihood and severity of harm. The incident and the assessment will be recorded. The ICO will be notified without undue delay and, where feasible, within 72 hours where the breach is likely to result in a risk to individuals' rights and freedoms. Affected individuals will be informed without undue delay where the risk is likely to be high. The police will be notified where the device is believed to have been stolen or where reporting may assist recovery, investigation, insurance requirements, or the prevention of further harm.

Appendix II: Data Protection Impact Assessments (Biometric Door Entry and CCTV)

1. Assessment details

Date completed: August 2026

Completed and approved by: Principal

Next scheduled review: August 2028

This assessment will be reviewed sooner if either system, its purposes, equipment, software, suppliers, storage arrangements, security measures, retention periods, or use changes materially; following a significant malfunction or personal-data breach; or if relevant law or regulatory guidance changes.

This Data Protection Impact Assessment considers Westminster Tutors' biometric access-control and CCTV systems.

2. Individuals affected

The systems may process information relating to:

- Students;
- Staff;
- Independent teachers;
- Visitors and contractors;
- Other individuals entering or approaching the premises.

Part A: Biometric access-control system

3. System and purposes

Westminster Tutors uses a Suprema biometric access-control system and BioStar 2 software. The current system was installed in June 2026, replacing an older system that had begun to fail.

The system is used to:

- Restrict access to authorised individuals;
- Maintain a record of who is recorded as being in the building;
- Support evacuation procedures by providing an occupancy list for use during a roll call.

The system is not used to record lesson attendance, monitor punctuality, or assess the conduct or performance of students, staff, or teachers.

4. Personal data processed

The system processes:

- The individual's full name;
- Measurements taken from selected characteristics of the individual's fingertip;
- A biometric template generated from those measurements;
- Entry and exit records;
- The individual's current recorded occupancy status.

A conventional fingerprint image is not intentionally retained.

5. Collection, storage, and access

Biometric templates are enrolled by authorised administrative staff. Access to the system and its records is restricted to staff with an operational need.

Appropriate physical and technical measures are used to protect the system against unauthorised access, alteration, disclosure, loss, or destruction.

The College's maintenance provider may access the equipment on site where necessary for authorised servicing or maintenance. The provider does not routinely retrieve or access the College's personal data remotely.

6. Lawful basis and special-category condition

Westminster Tutors relies on:

- Consent under Article 6(1)(a) of the UK GDPR;
- Explicit consent under Article 9(2)(a) of the UK GDPR for biometric data used to identify an individual uniquely.

Written authorisation is obtained before enrolment. For students under 18, written authorisation is obtained from both the student and their parent or carer. Students aged 18 or over, staff, and independent teachers provide their own written authorisation.

Participation is voluntary. Consent may be refused or withdrawn without disadvantage. Consent may be withdrawn by emailing info@westminstertutors.co.uk. Biometric use will be disabled on withdrawal, and the biometric template will normally be deleted within one working day after the request is received. Working days are Monday to Friday, excluding bank holidays in England, and include working days during College holidays.

7. Alternative access arrangements

Students who do not use the biometric system may use the reception buzzer when entering or leaving. Staff and independent teachers who do not use the biometric system will be issued with an access card.

If the system does not recognise an authorised user, reception staff can verify the person's identity, grant access manually, and update the occupancy record.

Emergency exit from the premises does not depend on the use of a biometric template, access card, or buzzer.

8. Necessity and proportionality

Biometric access provides reliable controlled entry and supports the maintenance of an occupancy record. It was selected because access cards may be lost, forgotten, transferred, or shared.

The processing is considered proportionate because:

- Participation is optional;
- Non-biometric alternatives are available;
- Only limited identifying information is held;
- The system is not used to monitor lesson attendance, behaviour, or performance;
- Access is restricted to authorised staff;
- Consent may be withdrawn;
- Defined retention and deletion arrangements apply;
- Emergency exit does not depend on biometric recognition.

Keys, cards, and reception-controlled entry were considered as alternatives. These remain available to individuals who do not consent to biometric processing.

9. Transparency and individual rights

Information about the system and the use of personal data is provided through:

- The Data Protection Policy;
- Relevant student, parent, staff, and teacher handbooks;
- Written consent materials;
- The College's privacy notices.

Individuals may exercise their data protection rights or withdraw consent by contacting Westminster Tutors.

10. Retention and deletion

Biometric templates and active user profiles are deleted within five working days of confirming that access is no longer required. The annual September review checks that departures have been dealt with.

Where consent is withdrawn, biometric use is disabled and the template is normally deleted within one working day after the request is received, including working days during College holidays.

Entry and exit records are retained until the end of the relevant academic year plus three years and are then deleted in accordance with the College's Data Retention Policy.

11. Risks and safeguards

The principal risks include unauthorised access, loss or misuse of biometric information, individuals feeling compelled to consent, inaccurate entry or exit records, incorrect rejection by the reader, and retention beyond the period required.

These risks are reduced through:

- Restricted access to the system;
- Appropriate physical and technical security;
- The use of biometric templates rather than intentionally retained fingerprint images;
- Written consent and clear withdrawal arrangements;
- Non-biometric alternatives;
- Manual access arrangements where recognition fails;
- Separate systems for lesson attendance;
- Physical roll calls during evacuations;
- Defined retention and deletion procedures.

There have been no known security breaches, unauthorised access incidents, false matches, or other significant problems involving the system.

The remaining risk is considered low to medium and proportionate to the purposes of the processing.

Part B: CCTV system

12. System and purposes

Westminster Tutors operates CCTV covering designated entrance, circulation, and examination-security areas.

The system is used for:

- Controlling and securing access to the premises;
- Safeguarding students, staff, teachers, and visitors;
- Preventing and detecting crime;
- Protecting College property;
- Identifying people requesting entry;
- Protecting examination materials and supporting examination security;
- Investigating specific incidents, concerns, or complaints.

The system records when movement is detected. It does not record audio or use facial recognition, biometric analysis, or other automated analytics.

Cameras do not cover classrooms, offices, toilets, changing areas, or other areas where individuals would reasonably expect greater privacy.

13. Personal data and storage

The system records video images of individuals passing through monitored areas, together with the associated date and time.

Footage is stored securely on College-controlled equipment. Appropriate physical and technical measures are used to protect it against unauthorised access, alteration, disclosure, loss, or destruction.

14. Lawful basis

Westminster Tutors relies on legitimate interests under Article 6(1)(f) of the UK GDPR.

The College's legitimate interests are:

- Protecting students, staff, teachers, visitors, premises, and property;
- Controlling access to the building;
- Preventing and investigating security and safeguarding incidents;
- Protecting the integrity and security of examination materials.

These interests are not considered to be overridden by individuals' rights because coverage is limited to areas where surveillance is reasonably necessary; audio and automated analytics are not used; signs and privacy information are provided; and access to footage is restricted.

15. Access, monitoring, and disclosure

Only authorised administrative staff may operate the CCTV system or export footage.

Other authorised senior staff may view relevant footage where necessary for a legitimate safeguarding, security, disciplinary, complaints, or incident-investigation purpose.

The entrance camera may be viewed routinely by reception staff to identify people requesting access. Other footage is not used for general monitoring of students, staff, or teachers and will ordinarily be viewed only in response to a specific incident, concern, or legitimate request.

Relevant footage may be provided to the police or another authorised body where the request is lawful, necessary, and proportionate. The reason for, and extent of, any disclosure will be recorded.

16. Transparency and individual rights

CCTV warning signs are displayed. The use and purposes of CCTV are explained in the College's privacy information.

Requests for access to footage will be handled in accordance with the Data Protection Policy. The rights and privacy of other identifiable individuals will be considered before footage is disclosed.

17. Retention

Routine CCTV footage must be automatically deleted or overwritten no later than 30 calendar days after recording.

Relevant footage may be preserved for an identified safeguarding concern, incident, investigation, complaint, information-rights request or legal obligation. Preserved footage is kept securely for only as long as necessary for that purpose, with the reason and review date recorded.

18. Risks and safeguards

The remaining risk is considered low, except for retention, which will remain under review until the 30-calendar-day maximum has been implemented and verified.

These risks are reduced through:

- Limited camera coverage;
- No surveillance of areas with heightened expectations of privacy;
- No audio recording, facial recognition, or automated analysis;
- Restricted access to footage;
- Defined purposes for viewing and disclosure;
- CCTV warning signs and privacy information;
- Automatic overwriting of footage;
- Periodic review of camera coverage, retention, and system use.

The remaining risk is considered low, except for retention, which will remain under review until the automatic overwrite period has been confirmed.

Part C: Conclusion and review

19. Overall conclusion

The biometric access-control and CCTV systems serve legitimate security, safeguarding, occupancy, and examination-integrity purposes.

Taking account of the purposes, the amount of information collected, the individuals affected, the available alternatives, and the safeguards in place, the processing is considered necessary and proportionate.

No high residual risk has been identified that would require prior consultation with the Information Commissioner's Office.

20. Actions

Westminster Tutors will:

- Configure, verify and document the CCTV system's 30-calendar-day maximum retention period for each camera;
- Keep the necessity of the retention period and any preserved footage under review;

Ownership and consultation	
Document author (name)	Sean Doherty, Principal

Audience	
Audience	Staff, teachers, parents, and students

Version control	
Implementation date	September 2024
Reviewed dates:	September 2025 August 2026
Next Review date	September 2027