Westminster Tutors

Data Protection Policy

2024-2025

Contents

1. Introduction & Process

1.1 Data and information that's collected, analysed, stored, communicated and reported upon may be subject to theft, misuse, loss and corruption. Data and information may be put at risk by poor education and training, and the breach of security controls.

1.2 Data breaches and information security incidents can give rise to embarrassment, financial loss, non-compliance with standards and legislation, as well as possible judgements being made against Westminster Tutors.

1.3 Our college aims to ensure that all personal data collected about staff, students, parents, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR), which came into effect on 1st January 2021, and the Data Protection Act 2018 (DPA 2018). This policy applies to all personal data, regardless of whether it is in paper or electronic format. An overview of the DPA 2018 has been published by the Information Commissioner's Office:

https://ico.org.uk/media/for-organisations/documents/2614158/ico-introduction-to-the-data-protection-bill.pdf

2. Legislation and guidance

2.1 This policy meets the requirements of the GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the Cabinet Office's code of practice for subject access requests. It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data. It also reflects the ICO's guidance for the use of surveillance cameras and personal information.

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 leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The Data Controller

4.1 Westminster Tutors processes personal data relating to parents, students, staff, visitors and others, therefore 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 and external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Proprietor, Principal and Senior Leadership Team (SLT)

5.2 The Proprietor, Principal, and Senior Leadership Team are overall responsible for ensuring that the college complies with all relevant data protection obligations.

The Proprietor is David Game.
The Principal is Sean Doherty.

5.3 The Senior Leadership Team comprises Sean Doherty, Principal; Virginia Maguire, Senior Consultant and Director of Studies; and Will Bynoe, Director of Studies (Academic).

Data Protection Officer

5.4 Westminster Tutors does not meet the requirements for appointing a Data Protection Officer (essentially larger organisations and/or those working with large amounts of data). Therefore, the SLT, particularly the Principal, will protect data. For any issues regarding data, the college can be contacted on info@westmintertutors.co.uk.

All staff

5.5 Staff are responsible for:

- Collecting, storing and processing any personal data following this policy.
- Informing the college of any changes to their personal data, such as a change of address
- Contacting the Principal or SLT in the following circumstances:
- If you have any questions about the operation of this policy, data protection law, retaining personal data, or keeping personal data secure.
- If they have any concerns that this policy is not being followed.
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way.
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK or European Economic Area.
- If there has been a data breach.
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
- If they need help with contracts or sharing personal data with third parties.

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.
- Processed in a way that ensures it is appropriately secure.

7. Collecting Personal Data

Lawfulness, Fairness and Transparency

7.1 We will only process personal data where we have one of six 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the college can fulfil a contract with the individual, or the individual has asked the college to take specific steps before entering into a contract.
- The data needs to be processed so that the college can comply with a legal obligation
- The data must be processed to ensure the individual's vital interests, e.g., to protect someone's life.

- The data needs to be processed so that the college, as a public authority, can perform a task in the public interest and perform its official functions.
- The data needs to be processed for the legitimate interests of the college or a third party (provided the individual's rights and freedoms are not overridden).
- The individual (or their parent/carer when appropriate in the case of a student) has freely given clear consent.

7.2 We will also meet one of the special category conditions for processing set out in the GDPR and Data Protection Act 2018 for special categories of personal data. Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

Limitation, Minimisation and Accuracy

7.3 We will only collect personal data for specified, explicit and legitimate reasons. When we first collect their data, we will explain these reasons to the individuals.

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 must only process personal data where necessary to do their jobs.

7.6 When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done following the college's record retention policy.

8. Sharing Personal Data

8.1 We will not usually share personal data with anyone else but may do so where:

- There is an issue with a student or parent/carer that puts the safety of our staff at risk.
- We need to liaise with other agencies – we will seek consent as necessary before doing this.
- Our suppliers or contractors may need data to enable us to provide services to our staff and students – for example, IT companies. If this situation arises, we will:
- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish a data-sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.
- Only share data that the supplier or contractor needs to carry out their service and information necessary to keep them safe while working with us.

8.2 We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud.
- The apprehension or prosecution of offenders.
- The assessment or collection of tax owed to HMRC.
- In connection with legal proceedings.

- Where the disclosure is required to satisfy our safeguarding obligations.
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

8.3 We may also share personal data with emergency services and local authorities to help them respond to an emergency affecting any of our students or staff.

8.4 We will follow data protection law when we transfer personal data to a country or territory outside the UK or European Economic Area.

9. Subject Access Requests and Other Rights of Individuals

Subject Access Requests

9.1 Individuals have a right to make a 'subject access request' to gain access to personal information that the college holds about them. This may include:

- Confirmation that their data is being processed.
- Access to a copy of the data.
- The purposes of the data processing.
- The categories of personal data concerned.
- Who the data has been, or will be, shared with.
- How long will the data be stored for, or if this is not possible, the criteria used to determine this period?
- The source of the data, if not the individual.
- Whether any automated decision-making is being applied to their data and the significance and consequences of this might be for the individual.

9.2 Subject access requests may take various forms, but ideally should be submitted in writing by letter or email to the Principal via info@westminstertutors.co.uk. They should include:

- Name of individual.
- Correspondence address.
- Contact number and email address.
- Details of the information requested.

Children and Subject Access Requests

9.3 Personal data about a child (an individual under the age of 18) belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request concerning their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent. Further information can be found at:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/how-do-we-recognise-a-subject-access-request-sar/#children

9.4 Students at our college are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students at our college may not be granted without the student's express permission. This is not a rule, and a student's ability to understand their rights will always be judged on a case-by-case basis.

9.5 Data requests for adults (individuals over 18) must be made by the individual themselves, not by their parents or 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:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/how-do-we-recognise-a-subject-access-request-sar/#behalf

Responding to Subject Access Requests

9.6 When responding to requests, we:

- May ask the individual to provide two forms of identification.
- May contact the individual via phone to confirm the request was made.
- Will respond without delay and within one month of receipt of the request.
- Will provide the information free of charge.
- We may tell the individual we will comply within three months of receipt of the request, where the request is complex or numerous. We will inform the individual of this within one month and explain why the extension is necessary.
- We will not disclose information if it:
- Might cause serious harm to the student's or another individual's physical or mental health.
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Is contained in adoption or parental order records.
- is given to a court in proceedings concerning the child.

9.6 If the request is unfounded or excessive, we may refuse to act on it or charge a reasonable fee considering administrative costs.

9.7 A request will be deemed unfounded or excessive if it is repetitive or asks for further copies of the same information.

9.8 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

9.9 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 the processing of it (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 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.
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

9.10 Individuals should submit any request to exercise these rights to the Principal. If staff receive such a request, they must immediately forward it to the Principal.

10. Parental Requests to see the Educational Record

10.1 Parental requests to see a child's education record are not covered by Data Protection legislation and, therefore, are outside the ambit of this policy. However, independent colleges in England do not legally have to provide an education record to parents. The principal will treat requests on a case-by-case basis.

11. Biometric Recognition Systems

11.1 Where we use students' biometric data as part of an automated biometric recognition system, such as for registering students using a fingerprint recognition system, we will comply with the Protection of Freedoms Act 2012 requirements.

11.2 Parents/carers will be notified before any biometric recognition system is implemented or before their child takes part in it. The college will get written consent from students aged 18 and over or from at least one parent or carer of students under 18 before we take any biometric data and first process it.

11.3 Parents/carers and students can choose not to use the college's biometric system(s). We will provide alternative means of accessing the relevant services for those students. For example, students can use the buzzer, and whoever is in reception will manually record their attendance at the college.

11.4 Parents/carers and students can object to participation in the college's biometric recognition system(s) or withdraw consent at any time, and we will make sure that any relevant data already captured is deleted.

11.5 As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the student's parent(s)/carer(s).

11.6 Where staff members or other adults (18 or over) use the college's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the college will delete any relevant data already captured.

11.7 See our Door Entry System Policy for more information.

12. CCTV

12.1 We use CCTV at the entrance to the college site to ensure it remains safe. 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 make it clear where individuals are being recorded. Security cameras are clearly 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 will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.
Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used. Uses may include:

- Within college, on notice boards and in college magazines, brochures, newsletters, etc.
- Outside college by external agencies such as the college photographer, newspapers, and campaigns.
- Online on our college website or social media pages.

13.2 Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

13.3 When using photographs and videos in this way, we will not accompany them with any other personal information about the child to ensure they cannot be identified unless explicit consent is given. See our Child Protection and Safeguarding Policy for more information.

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 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 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 records of our processing activities, including:
- For the benefit of data subjects, making available the name and contact details of our college and all information we are required to share about how we use and process their personal data (via our privacy notices)
- For all personal data that we hold, maintaining an internal record of the type of data, the data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

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-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or anywhere else with general access.
- Where personal information needs to be taken off-site, staff must sign it in and out from the college office.
- College computers, laptops, and other electronic devices require passwords that are at least 8 characters long and contain letters and numbers. Staff and students are reminded to change their passwords regularly.

- Staff or students who store personal information on their devices must follow the same security procedures as for college-owned equipment.
- 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, and 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 1.

17.2 When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a college context may include, but are not limited to:

- A non-anonymised dataset being published on the college website.
- Safeguarding information being made available to an unauthorised person.
- The theft of a college laptop containing non-encrypted personal data about students.

18. Training

18.1 All staff are provided with 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.

Appendix 1: 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 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 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.
- Identify 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 risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the Principal will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- 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 data breach and mitigate any possible adverse effects on the individual(s) concerned.
- The Principal will notify any relevant third parties who can help mitigate the loss to individuals, such as the police, insurers, banks, or credit card companies.
- The Principal will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- Records of all breaches will be stored on the Google Drive Cloud.

The Principal and SLT will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

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 especially 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 being disclosed via email (including safeguarding records).

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

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

If the sender is unavailable or cannot recall the email, the Principal will ask the ICT department to recall it.

In any cases 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 being stolen or hacked

If an administrator's laptop is stolen from the college, the police, the ICO, the SLT, and the principal will be notified.

CCTV footage from when the laptop was stolen will assist the police investigation.

The laptop will be locked remotely by the network manager. Passwords will be changed.

The Principal/SLT will conduct an internet search to check if any information has been made public; if it has, we will contact the publisher/website owner or administrator to request that the information be removed from the website and deleted.

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

Audience	
Audience	Principal, college staff, parents and students

Version control	
Implementation date	September 2024
Review date	September 2026