Christ Centred, Child Centred, Catholic Educational Excellence

THE DIOCESE OF WESTMINSTER ACADEMY TRUST

PRIVACY NOTICE FOR STUDENTS, PARENTS AND CARERS

This Privacy Policy and Procedure has been approved and adopted by The Diocese of Westminster Academy Trust in May 2025 and will be reviewed in May 2027.

Please see School Level Privacy Policies for specific school-related information.

Signed by the Chair of The Diocese of Westminster Academy Trust: *Patrick Leeson*

THIS POLICY DOES NOT CREATE CONTRACTUAL OBLIGATIONS ON THE SCHOOL

CONTENTS

CONTENTS 2

INTRODUCTION 3

1. WHY DO WE COLLECT AND USE STUDENT INFORMATION? 3

2. THE CATEGORIES OF INFORMATION THAT WE COLLECT, HOLD AND SHARE 5

3. COLLECTING INFORMATION 6

4. STORING DATA 6

5. DATA RETENTION 7

6. WHO DO WE SHARE INFORMATION WITH? 7

7. DATA SHARING WITH THE DIOCESE OF WESTMINSTER 9

8. SAFEGUARDING 9

9. AGE 14+ QUALIFICATIONS (SECONDARY TRUST SCHOOLS ONLY) 9

10. WHY WE SHARE INFORMATION 10

11. DATA COLLECTION REQUIREMENTS 10

12. YOUTH SUPPORT SERVICES (SECONDARY TRUST SCHOOLS ONLY) 10

14. REQUESTING ACCESS TO YOUR PERSONAL DATA 12

15. CONTACT & CHANGES TO PRIVACY NOTICE 13

ADDENDUM: BIOMETRIC DATA 14

INTRODUCTION

The Diocese of Westminster Academy Trust is committed to protecting the privacy and security of your personal information.

We collect data and information about our parents/carers and students so that we can run effectively as a Trust. This privacy notice explains how and why we collect students' data, what we do with it, how long we keep it, and what rights parents and students have.

The Diocese of Westminster Academy Trust ("DoWAT") is a multi academy trust. You can find information about our schools here. DoWAT is a charitable company limited by guarantee (registration number 07944160) whose registered office is Waxwell House, 125 Waxwell Lane, Pinner, HA5 3EP. DoWAT is the Data Controller for all the academies within the Trust, Information Commissioner's Office (ICO) registration number ZA471347.

The Data Protection Officer (DPO) for DoWAT is the Trust Chief Financial Officer (CFO), named here, postal address: The Diocese of Westminster Academy Trust, Waxwell House, 125 Waxwell Lane, Pinner, HA5 3EP. The Trust DPO is supported by an External DPO Richard Maskrey. Please consult school level Privacy Notices for details of the Academy Deputy Data Protection Officer (DDPO).

The term "parent" is widely defined in education law to include the natural or adoptive parents (regardless of whether parents are or were married, whether a father is named on a birth certificate or has parental responsibility for the student, with whom the student lives or whether the student has contact with that parent), and also includes non-parents who have parental responsibility for the student, or with whom the student lives. It is therefore possible for a student to have several "parents" for the purposes of education law. This privacy notice also covers other members of students' families who we may process data about from time to time, including, for example, siblings, aunts and uncles and grandparents.

1. WHY DO WE COLLECT AND USE STUDENT INFORMATION?

1.1 We collect and use student information under the following lawful bases:

1.1.1 Where we have the consent of the data subject (Article 6 (a));

1.1.2 Where it is necessary for compliance with a legal obligation (Article 6 (c));

1.1.3 Where processing is necessary to protect the vital interests of the data subject or another person (Article 6(d));

1.1.4 Where it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6 (e)).

1.1.5 Where the personal data we collect about students is sensitive personal data, we will only process it where:

1.1.5.1 we have explicit consent;

1.1.5.2 processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; and / or

1.1.5.3 processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

1.2 Please see the ICO website here for information about sensitive personal data.

1.3 We use our data to support our statutory functions of running a school, in particular:

1.3.1 To decide who to admit to the school;

1.3.2 To maintain a waiting list;

1.3.3 To support student learning;

1.3.4 To monitor and report on student progress;

1.3.5 To provide appropriate pastoral care;

1.3.6 To assess the quality of our services;

1.3.7 To comply with the law regarding data sharing;

1.3.8 For the protection and welfare of students and others in the school;

1.3.9 For the safe and orderly running of the school;

1.3.10 To promote the school;

1.3.11 To communicate with parents / carers;

1.3.12 To respond to investigations from our regulators or to respond to complaints raised by our stakeholders;

1.3.13 In connection with any legal proceedings threatened or commenced against the school.

2. THE CATEGORIES OF INFORMATION THAT WE COLLECT, HOLD AND SHARE

2.1 Personal details (such as name, Unique Pupil Number and address), national curriculum assessment results, attendance information (such as sessions attended, number of absences and absence reasons), any exclusion information, where they go after they leave us, personal characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility), any special educational needs they may have as well as relevant medical information. Sensitive personal information may also be processed for safeguarding purposes (on the Legal Basis of Vital Interest) at any time. Explicit consent would be sought if biometric data was ever to be collected/used by the school in the future.

2.2 We collect information about students when they join the school by using data collection forms (online or physical), file transfers from local authorities and previous schools, and update this information during their time on the roll, as and when new information is acquired.

2.3 From time to time and in certain circumstances, we might also process personal data about parents/carers, some of which might be sensitive personal data, information about criminal proceedings/convictions or information about child protection/safeguarding. This information is not routinely collected about parents/carers and is only likely to be processed by the school in specific circumstances relating to particular students, for example, if a child protection issue arises or if a parent/carer is involved in a criminal matter. Where appropriate, such information may be shared with external agencies such as the child protection team at the Local Authority, the Local Authority Designated Officer and / or the Police. Such information will only be processed to the extent that it is lawful to do so and appropriate measures will be taken to keep the data secure.

2.4 For schools with a cashless catering system, we also process biometric data about students if we have received explicit consent from parents. Please see our Data Protection Policy and Breach Response Plan for more details about how we process biometric data.

3. COLLECTING INFORMATION

3.1 Whilst the majority of information we collect is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the UK General Data Protection Regulation, we will inform you whether you are required to provide certain information to us or if you have a choice in this. Where appropriate, we will ask parents or students for consent to process personal data where there is no other lawful basis for processing it, for example where we wish to use photos or images of students on our website or on social media to promote school activities or if we want to ask your permission to use your information for marketing purposes. Parents / students may withdraw consent at any time.

3.2 When students are deemed to be old enough to make their own decisions in relation to their personal data, we will also ask the student for their consent in these circumstances. This will usually be around the age of 13. Although parental consent is unlikely to be needed, we wish to take a collaborative approach so we will keep parents informed when we are approaching students for consent up to the age of 18. Students with the maturity to make their own decisions about their personal data may withdraw consent if consent has previously been given.

3.3 Schools may record phone calls for monitoring purposes. Please consult school level privacy notices for more information.

3.4 Schools may use CCTV cameras around the school site for security purposes and for the protection of staff and students. CCTV footage may be referred to during the course of disciplinary procedures (for staff or students) or to investigate other issues. CCTV footage involving students will only be processed to the extent that it is lawful to do so. Please see the relevant school's CCTV policy for more details.

4. STORING DATA

4.1 An annual sweep of the school network will be used to ensure that data is removed from general access where appropriate. We shred or destroy redundant data using a compliant provider or shred on-site.

4.2 We may hold data on USB memory devices if adequately protected, although their use is discouraged.

4.3 Photographs, videos and sound media will be captured by the school using school equipment and in line with any consent granted.

4.4 Data is backed up regularly (details can be obtained from the School Office). ARBOR and CPOMS are online services, backed up by the service providers. SIMS is backed up on school servers. Details are held within our Supplier Compliance Log. We maintain a supplier compliance log to ensure that Data Processors (our suppliers) are compliant and effectively safeguard your data.

4.5 The School and Trust has robust processes in place to minimise the risk of data breaches. In the unlikely event of a Data Breach, the Trust has an internal Data Breach Procedure and procedures which would be followed. In the event of a data breach, we would act in accordance with the UK General Data Protection Regulations.

5. DATA RETENTION

5.1 Data will be retained by the School and/or Trust for the duration of the pupil's time with us. We cannot agree to delete required safeguarding data during this time.

5.2 We will agree to remove data held on pupils, if requested, after they have left us (provided we are not required to keep it due to ratified policy or law). We will have to send their information to a new school or education establishment, if applicable.

5.3 The pupil's educational record is held as follows:

5.3.1 Primary schools – the pupil file is retained whilst the child remains at the primary school. The file should follow the pupil when they leave the primary school. This will include moving to another primary school, a secondary school, a pupil referral unit. If the pupil transfers to an independent school, transfers to home schooling, dies or leaves the country, the file may be returned to the LA to be retained for the statutory retention period.

5.3.2 Secondary schools - the pupil file is retained until the pupil reaches 25 years of age. Data will be securely deleted in the academic year of their 25th birthday.

5.4 Some school data will be kept for 6 years plus the current year – this includes financial accounting information (legal reasons) and Data Breach Logs. Emails will usually be retained within school for a period of two years, unless the information contained needs to be kept longer than this (professional judgement/SLT discretion).

6. WHO DO WE SHARE INFORMATION WITH?

6.1 We routinely share student information with:

6.1.1 Parents / carers (as defined in the Education Act 1996).

6.1.2 Schools that students attend after leaving us.

6.1.3 Our local authorities within the geographical area of the Trust (Hillingdon, Hertfordshire, Brent and Hounslow).

6.1.4 A student's home local authority (if different).

6.1.5 The Department for Education (DfE).

THIS POLICY DOES NOT CREATE CONTRACTUAL OBLIGATIONS ON THE SCHOOL

6.1.6 The Education and Skills Funding Agency

6.1.7 School local governors / trustees.

6.1.8 The central team at DoWAT.

6.1.9 Trust and DPO approved web-based learning platforms.

6.1.10 Exam boards including exam boards including AQA, OCR, Edexcel, WJEC, BTEC.

6.2 From time to time, we may also share student information other third parties including the following:

6.2.1 The Police and law enforcement agencies.

6.2.2 NHS health professionals including the school nurse, educational psychologists.

6.2.3 Education Welfare Officer.

6.2.4 Courts, if ordered to do so.

6.2.5 The National College for Teaching and Learning.

6.2.6 The Joint Council for Qualifications.

6.2.7 The Standards Testing Agency.

6.2.8 Prevent teams in accordance with the Prevent Duty on schools.

6.2.9 The Local Safeguarding Board relevant to the Academies location.

6.2.10 Other schools, for example, if we are negotiating a managed move and we have your consent to share information in these circumstances.

6.2.11 The Catholic Education Service.

6.2.12 Diocesan Officers at the Diocese of Westminster for the purposes of receiving educational support.

6.2.13 OfSTED.

6.2.14 The school chaplain.

6.2.15 Our HR providers, for example, if we are seeking HR advice and a student is involved in an issue.

6.2.16 UCAS

6.2.17 our legal advisors

6.2.18 our insurance providers / the Risk Protection Arrangement

6.2.19 our school Parents' Association (with your consent)

6.3 The above organisations will either be Data Processors or Data Controllers in their own right. We would inform you of any sub-processor data breaches, once informed, in line with the Data Protection Act and UK GDPR.

6.4 In the event that we share personal data about students with third parties, we will provide the minimum amount of personal data necessary to fulfil the purpose for which we are required to share the data.

7. DATA SHARING WITH THE DIOCESE OF WESTMINSTER

7.1 The Diocesan Education Commission of the Diocese of Westminster is responsible for all areas relating to education in schools and colleges set out in canon law and English law. It is responsible to the Diocesan Trustees for the financial aspects of providing and maintaining Catholic education in the Diocese of Westminster. The Trust and its academies as Catholic schools within the diocese share information with the Diocese of Westminster to allow them to meet these requirements. Examples of the data provided:

7.1.1 Personal information (such as name, unique student number, date of birth, address, gender, year group, admissions data).

7.1.2 Characteristics (such as ethnicity, religion, language, medical conditions, nationality, Special Education Needs information and free school meal eligibility).

7.1.3 Standards data for the Diocesan Inspection of Catholic Schools.

7.1.4 Continued Professional Development (Training data, Inset days).

7.1.5 Information requested by the Bishop.

7.1.6 Financial Benchmarking data.

8. SAFEGUARDING

8.1 UK GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards will still be in place.

9. AGE 14+ QUALIFICATIONS (SECONDARY TRUST SCHOOLS ONLY)

9.1 For students enrolling for post 14 qualifications, the Learning Records Service will give us a student's unique learner number (ULN) and may also give us details about the student's learning or qualifications.

10. WHY WE SHARE INFORMATION

10.1 Whilst we share information as an ongoing School/Trust management requirement, which would include non-standard operational activity such as complaints and legal proceedings as required, we do not share information about our pupils with anyone without your consent unless the law and our policies allow us to do so.

10.2 We share data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

10.3 We are required to share information about our students with the (DfE) under regulation 5 of The Education (Information About Individual Students) (England) Regulations 2013.

11. DATA COLLECTION REQUIREMENTS

11.1 To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

11.2 If you require more information about how our local authority and/or DfE collect and use your information, please visit the DfE website at https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

12. YOUTH SUPPORT SERVICES (SECONDARY TRUST SCHOOLS ONLY)

12.1 Once our students reach the age of 13, we also pass student information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

12.2 This enables them to provide services as follows:

12.2.1 youth support services.

12.2.2 careers advisers.

12.3 A parent / guardian can request that only their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / student once he/she reaches the age 16.

12.4 We will also share certain information about students aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

THIS POLICY DOES NOT CREATE CONTRACTUAL OBLIGATIONS ON THE SCHOOL

12.5 This enables them to provide services as follows:

12.5.1 post-16 education and training providers;

12.5.2 youth support services;

12.5.3 careers advisers.

12.6 For more information about services for young people, please visit our local authority website.

13. THE NATIONAL PUPIL DATABASE (NPD)

13.1 The NPD is owned and managed by the Department for Education and contains information about students in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

13.2 We are required by law, to provide information about our students to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Students) (England) Regulations 2013.

13.3 To find out more about the NPD, go to https://www.gov.uk/government/publications/national-student-database-user-guide-and-supporting-information.

13.4 The department may share information about our students from the NPD with third parties who promote the education or well-being of children in England by:

13.4.1 Conducting research or analysis.

13.4.2 Producing statistics.

13.4.3 Providing information, advice or guidance.

13.5 To be granted access to student information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

13.6 For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

13.7 For information about which organisations the department has provided student information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-student-database-requests-received

13.8 To contact DfE: https://www.gov.uk/contact-dfe

14. REQUESTING ACCESS TO YOUR PERSONAL DATA

14.1 You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is manifestly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

14.2 We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

14.3 For primary schools within the Trust:

14.3.1 Under data protection legislation, parents and students have the right to request access to information about them that we hold ("Subject Access Request"). Where a child does not have the maturity to make their own requests for personal data, parents may do so on their behalf in a primary school setting. To make a request for your child's personal data, or be given access to your child's educational record, contact the Academy internal DDPO, although you can also make this request directly to the school office.

14.4 For secondary schools within the Trust:

14.4.1 : Under data protection legislation, students, and in some circumstances, parents, have the right to request access to information about them that we hold ("Subject Access Request"). From the age of 13, we generally regard students as having the capacity to exercise their own rights in relation to their personal data. This means that where we consider a student to have sufficient maturity to understand their own rights, we will require a Subject Access Request to be made by the student and not their parent(s) on their behalf. This does not affect any separate statutory right parents might have to access information about their child (e.g. Education Record).

14.4.2 Subject to the section below, the legal timescales for the School to respond to a Subject Access Request is one calendar month, although this can be extended by a further 60 days in certain circumstances. As the School has limited staff resources outside of term time, we encourage parents / students to submit Subject Access Requests during term time and to avoid sending a request during periods when the School is closed or is about to close for the holidays. where possible. This will assist us in responding to your request as promptly as possible. For further information about how we handle Subject Access Requests, please see our Data Protection Policy and Breach Response Plan.

14.4.3 Parents of students who attend academies have a separate statutory right to receive an annual written report setting out their child's attainment for the main subject areas which are taught. This is an independent legal right of parents rather than a student's own legal right which falls outside

of the UK GDPR, therefore a student's consent is not required even a student is able to make their own decisions in relation to their personal data, unless a court order is in place which states otherwise.

14.5 In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the relevant school. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

14.6 If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/

15. CONTACT & CHANGES TO PRIVACY NOTICE

15.1 If you would like to discuss anything in this privacy notice, please contact: DoWAT DPO (CFO), contact name here, The Diocese Of Westminster Academy Trust, Waxwell House, 125 Waxwell Lane, Pinner, London, HA5 3EP

15.2 We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

ADDENDUM: BIOMETRIC DATA

1. PURPOSE

1.1. This addendum supplements the existing privacy notices used by the school, academy, trust or setting. It explains how biometric data will be approached if a biometric recognition system is used, or proposed for use. It does not replace the existing privacy notices and should be read alongside them.

1.2. Biometric data means personal data resulting from specific technical processing relating to a person's physical, physiological or behavioural characteristics. Examples include fingerprints, facial recognition data, iris or retina scans, palm vein data, voice recognition data and similar identifiers. Where biometric data is used for the purpose of uniquely identifying a person, it is special category data.

2. WHO THIS APPLIES TO

2.1. This addendum applies where biometric data is processed about pupils or students, parents or carers, staff, volunteers, governors, trustees, committee members, visitors or other individuals who may use or be affected by a biometric recognition system operated by, or on behalf of, the school, academy, trust or setting.

3. WHEN BIOMETRIC SYSTEMS MAY BE USED

3.1. The school, academy, trust or setting will only use biometric systems where there is a clear, necessary and proportionate reason for doing so. Examples may include cashless catering, library access, access control, attendance systems or similar education management purposes. Before introducing or materially changing any biometric system, the relevant data controller will consider whether a less intrusive alternative can achieve the same purpose.

4. LEGAL BASIS AND SAFEGUARDS

4.1. Before using biometric data for identification, the relevant data controller will identify an appropriate lawful basis under Article 6 UK GDPR and a separate condition for processing special category data under Article 9 UK GDPR. In most education biometric recognition contexts, explicit consent is likely to be required.

4.2. For pupils and students under 18, the school, academy, trust or setting will also comply with the Protection of Freedoms Act 2012. This means parents or carers will be notified before the child's biometric information is processed, the required written parental consent will be obtained, any written parental objection or withdrawal of consent will be respected, and a pupil's or student's own objection or refusal will also be respected.

5. DATA PROTECTION IMPACT ASSESSMENT

5.1. A Data Protection Impact Assessment will be completed before introducing, or materially changing, a biometric recognition system. The assessment will consider the purpose of the system, whether the processing is necessary and proportionate, the risks to individuals, the supplier arrangements, security measures, retention arrangements and the availability of reasonable alternatives.

5.2. If a Data Protection Impact Assessment identifies a high risk that cannot be mitigated, the processing will not begin until the appropriate further steps have been taken, including consultation with the Information Commissioner's Office where required.

6. CONSENT, REFUSAL AND ALTERNATIVES

6.1. Where consent is used, it must be freely given, specific, informed and capable of being withdrawn.

6.2. For pupils and students under 18, the written consent of at least one parent or carer with parental responsibility is required, unless a statutory exception applies, and no parent or carer has objected or withdrawn consent.

6.3. A pupil or student may refuse or object to the use of their biometric data. Their objection does not need to be in writing and will override parental consent.

6.4. A reasonable non-biometric alternative will be provided so that individuals are not disadvantaged because they do not use the biometric system.

6.5. Where consent is withdrawn, or the individual ceases to use the system, the relevant biometric data will be securely deleted unless there is a lawful reason to retain it.

7. HOW BIOMETRIC DATA WILL BE HANDLED

7.1. Where biometric data is used, separate information will be provided explaining the specific system being used, the type of biometric data collected, the purpose of the processing, who will have access

to the data, whether a processor or supplier is involved, how the information will be secured, how long it will be retained and how it will be deleted.

7.2. Biometric data will only be used for the purpose explained at the point consent is sought or information is provided. It will not be used for unrelated purposes without further assessment and, where required, fresh consent and updated privacy information.

8. LIVE FACIAL RECOGNITION

8.1. Live facial recognition will not be used in a school, academy, trust or education setting. Live facial recognition is different from a controlled biometric recognition system and involves the real-time and potentially indiscriminate capture of biometric data from people passing within range of a camera. Current DfE guidance states that live facial recognition is not appropriate in school and college settings.

9. REVIEW

9.1. This addendum should be reviewed when the school, academy, trust or setting introduces or changes any biometric system, when supplier arrangements change, or when relevant legislation or national guidance is updated.