



Christ Centred, Child Centred, Catholic Educational Excellence

THE DIOCESE OF WESTMINSTER ACADEMY TRUST

PRIVACY NOTICE FOR STAFF, DIRECTORS AND VOLUNTEERS

This Privacy notice for Staff, Directors and Volunteers has been approved and adopted by The Diocese of Westminster Academy Trust in April 2026 and will be reviewed in May 2027.

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

CONTENTS

CONTENTS	2
INTRODUCTION	3
1. DATA PROTECTION PRINCIPLES	4
2. THE TYPE OF INFORMATION WE HOLD ABOUT YOU	4
3. HOW IS YOUR PERSONAL INFORMATION COLLECTED?	5
4. PROCESSING OF DATA RELATING TO CONTRACTORS AND THIRD PARTIES	6
5. HOW WE WILL USE INFORMATION ABOUT YOU	6
6. SITUATIONS IN WHICH WE WILL USE YOUR PERSONAL INFORMATION (AS APPROPRIATE):	6
7. HOW WE USE PARTICULARLY SENSITIVE PERSONAL INFORMATION	8
8. INFORMATION ABOUT CRIMINAL CONVICTIONS	10
9. AUTOMATED DECISION-MAKING	10
10. DATA SHARING	10
11. DATA SHARING WITH THE DIOCESE OF WESTMINSTER	12
12. DATA SHARING WITH THIRD PARTIES	12
13. DATA SHARING WITH THIRD PARTIES AND SECURITY	14
14. DATA SECURITY	15
15. DATA RETENTION	15
16. RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION	16
17. RIGHT TO WITHDRAW CONSENT	16
18. DATA PROTECTION OFFICER	17
19. CHANGES TO THIS PRIVACY NOTICE	17
ADDENDUM: BIOMETRIC DATA	18



INTRODUCTION

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

Our school is an academy within the Diocese of Westminster Academy Trust (“DoWAT”), 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.

This Privacy Notice describes how we collect and use personal information about you before, during and after your working relationship with us, in accordance with the UK General Data Protection Regulation (UK GDPR).

It applies to all current and former employees, workers, contractors, directors, governors and volunteers.

DoWAT is a “data controller”. This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice does not form part of any contract of employment or other type of contract to provide services. We may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.



1. DATA PROTECTION PRINCIPLES

- 1.1 We will comply with data protection law. This says that the personal information we hold about you must be:
 - 1.1.1 Used lawfully, fairly and in a transparent way.
 - 1.1.2 Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
 - 1.1.3 Relevant to the purposes we have told you about and limited only to those purposes.
 - 1.1.4 Accurate and kept up to date.
 - 1.1.5 Kept only as long as necessary for the purposes we have told you about.
 - 1.1.6 Kept securely.

2. THE TYPE OF INFORMATION WE HOLD ABOUT YOU

- 2.1 Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).
- 2.2 There are “special categories” of more sensitive personal data which require a higher level of protection.
- 2.3 We will collect, store, and use the following categories of personal information about you may include (if applicable), but is not limited to:
 - 2.3.1 Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses;
 - 2.3.2 Date of birth;
 - 2.3.3 Gender;
 - 2.3.4 Marital status and dependants;
 - 2.3.5 Next of kin and emergency contact information;
 - 2.3.6 National Insurance number;
 - 2.3.7 Bank account details, payroll records and tax status information;
 - 2.3.8 Salary, annual leave, pension and benefits information;
 - 2.3.9 Teacher Reference Number;
 - 2.3.10 Start date;
 - 2.3.11 Location of employment or workplace;



- 2.3.12 Copy of driving licence;
 - 2.3.13 Online Search result (KCSIE);
 - 2.3.14 Recruitment information (including copies of pre-vetting recruitment and identity checks (including, where appropriate, information about your employment history, Standard or Enhanced Disclosure and Barring Service Checks, Barred Lists Checks, prohibition checks [section 128 checks] and disqualification checks, for example under the Childcare (Disqualification) Regulations 2009 and any further checks that are required if you have lived or worked outside the UK), your nationality and right to work documentation, references and other information included in a CV, application form or cover letter or as part of the application process);
 - 2.3.15 Employment records (including job titles, work history, working hours, training records and professional memberships);
 - 2.3.16 Compensation history;
 - 2.3.17 Performance information;
 - 2.3.18 Disciplinary and grievance information, including warnings issued to you;
 - 2.3.19 CCTV footage and other information obtained through electronic means such as swipecard records;
 - 2.3.20 Information about your use of our information and communications systems;
 - 2.3.21 Photographs.
- 2.4 We may also collect, store and use the following “special categories” of more sensitive personal information:
- 2.4.1 Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions;
 - 2.4.2 Trade union membership;
 - 2.4.3 Information about your health, including any medical condition, health and sickness records;
 - 2.4.4 Genetic information and biometric data;
 - 2.4.5 Information about your criminal record.

3. HOW IS YOUR PERSONAL INFORMATION COLLECTED?

- 3.1 We collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, the Local Authority or other background check agencies. For Directors and governors, your information may be added by you, using GovernorHub (or another similar online system).



- 3.2 We will also collect additional personal information in the course of job-related activities throughout the period of you working for us.

4. PROCESSING OF DATA RELATING TO CONTRACTORS AND THIRD PARTIES

- 4.1 The Trust and its schools may also process personal data relating to contractors, service providers, hirers and other third parties who engage with the school.
- 4.2 This may include contact details, identification information and, where appropriate, safeguarding or compliance-related information necessary for the safe and effective operation of the school.
- 4.3 Such information is processed in accordance with UK GDPR and the Data Protection Act 2018, and only where it is necessary to:
 - 4.3.1 manage contracts and service delivery.
 - 4.3.2 ensure safeguarding and site security.
 - 4.3.3 comply with legal and regulatory obligations.
 - 4.3.4 Personal data will only be shared where necessary and proportionate, and appropriate safeguards will be in place at all times.

5. HOW WE WILL USE INFORMATION ABOUT YOU

- 5.1 We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:
 - 5.1.1 Where we need to perform the contract we have entered into with you.
 - 5.1.2 Where we need to comply with a legal obligation.
- 5.2 We may also use your personal information in the following situations:
 - 5.2.1 Where we need to protect your interests (or someone else's interests).
 - 5.2.2 Where it is needed in the public interest or for official purposes.

6. SITUATIONS IN WHICH WE WILL USE YOUR PERSONAL INFORMATION (AS APPROPRIATE):

- 6.1 We need all the categories of information in the list above primarily to allow us to perform our contract with you, to enable us to comply with legal obligations and/or where it is needed in the public interest or for official purposes. The situations in which we will process your personal information are listed below.
- 6.2 We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:



- 6.2.1 Making a decision about your recruitment or appointment.
- 6.2.2 Determining the terms on which you work for/with us.
- 6.2.3 Complying with our responsibilities as a Catholic school under Canon Law to the Westminster Diocesan Trustees.
- 6.2.4 Checking you are legally entitled to work in the UK.
- 6.2.5 Checking the award of Qualified Teacher Status, completion of teacher induction and prohibitions, sanctions and restrictions that might prevent the individual from taking part in certain activities or working in specific positions [via the Teacher Services Online platform].
- 6.2.6 To maintain our single central record and to comply with our general safeguarding obligations.
- 6.2.7 To provide information on our website about our employees and governors.
- 6.2.8 Where appropriate, to disclose certain information in the Academy's accounts in accordance with the Accounts direction.
- 6.2.9 Paying you and, if you are an employee, deducting tax and National Insurance contributions.
- 6.2.10 Liaising with your pension provider.
- 6.2.11 Administering the contract we have entered into with you.
- 6.2.12 In order to operate as a school, which may involve us sharing certain information about our staff with our stakeholders or processing correspondence or other documents, audits or reports which contain your personal data.
- 6.2.13 Business management and planning, including accounting and auditing.
- 6.2.14 Conducting performance reviews, managing performance and determining performance requirements.
- 6.2.15 Making decisions about salary reviews and compensation.
- 6.2.16 Assessing qualifications for a particular job or task, including decisions about promotions.
- 6.2.17 Gathering evidence for possible grievance or disciplinary hearings.
- 6.2.18 Responding to complaints or investigations from stakeholders or our regulators.
- 6.2.19 Making decisions about your continued employment or engagement.
- 6.2.20 Making arrangements for the termination of our working relationship.
- 6.2.21 Providing references to prospective employers.
- 6.2.22 Education, training and development requirements.
- 6.2.23 Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- 6.2.24 Ascertaining your fitness to work.
- 6.2.25 Managing sickness absence.
- 6.2.26 Complying with health and safety obligations.



- 6.2.27 To prevent fraud.
- 6.2.28 To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- 6.2.29 To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- 6.2.30 To conduct data analytics studies to review and better understand employee retention and attrition rates.
- 6.2.31 In connection with the Transfer of Undertaking (Protection of Employment) Regulations 2006, for example, if a service is outsourced or in connection with an academy conversion.
- 6.2.32 To maintain and promote equality in the workplace.
- 6.2.33 To comply with requirements of the Diocese of Westminster to share personal data about employees to the extent that they require it to fulfil their functions – further details are available on the Diocese’s privacy notice.
- 6.2.34 To receive advice from external advisors and consultants.
- 6.2.35 In appropriate circumstances to liaise with regulatory bodies, such as the TRA, the Department for Education, the DBS and the Local Authority about your suitability to work in a school or in connection with other regulatory matters.
- 6.2.36 Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.
- 6.3 If you fail to provide certain information when requested, we may not be able to perform any contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers) or we may be unable to discharge our obligations which may be in the public interest or for official purposes.
- 6.4 We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.
- 6.5 Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

7. HOW WE USE PARTICULARLY SENSITIVE PERSONAL INFORMATION

- 7.1 “Special categories” of particularly sensitive personal information require us to ensure higher levels of data protection. We need to have further justification for collecting, storing and using this type of



personal information. We may process special categories of personal information in the following circumstances:

- 7.1.1 In limited circumstances, with your explicit written consent.
- 7.1.2 Where we need to carry out our legal obligations and in line with our Data Protection Policy and Breach Response Plan.
- 7.1.3 Where it is needed in the public interest, such as for equal opportunities monitoring [or in relation to our occupational pension scheme], and in line with Data Protection Policy and Breach Response Plan.
- 7.1.4 Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.
- 7.2 Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.
- 7.3 We will use your particularly sensitive personal information in the following ways:
 - 7.3.1 We will use information relating to leaves of absence including the reasons for the leave, which may include sickness absence or family-related leave, sabbaticals, to comply with employment and other laws.
 - 7.3.2 We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to comply with the Equality Act 2010, to monitor and manage sickness absence and to administer benefits.
 - 7.3.3 We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.
 - 7.3.4 We will use trade union membership information to pay trade union subscriptions, register the status of a protected employee and to comply with employment law obligations.
 - 7.3.5 As we are a Catholic school, we will hold information about the religious beliefs of some employees so that we can assess their suitability to hold certain posts.
- 7.4 We do not need your consent if we use your particularly sensitive information in accordance with our written policy where processing is necessary:
 - 7.4.1 To carry out our legal obligations or exercise specific rights in the field of employment law;
 - 7.4.2 For the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;



7.4.3 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 we provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

7.5 In other circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract of employment with us that you agree to any request for consent from us.

8. INFORMATION ABOUT CRIMINAL CONVICTIONS

8.1 We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our Safeguarding and Recruitment responsibilities and our Data Protection Policy and Breach Response Plan.

8.2 Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

8.3 We envisage that we will hold information about criminal convictions, for example, if information about criminal convictions comes to light as a result of our recruitment and Disclosure and Barring Service checks, or if information about criminal convictions comes to light during your employment with us.

8.4 We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. We will use information about criminal convictions and offences to assess your suitability to work in a school setting, as required by Keeping Children Safe in Education.

9. AUTOMATED DECISION-MAKING

9.1 We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

10. DATA SHARING



- 10.1 We may have to share your data with third parties, including third-party service providers and other organisations.
- 10.2 In particular, we may share your data with organisations including, but not limited to, the following:
- 10.2.1 Local Authorities;
 - 10.2.2 The Department for Education;
 - 10.2.3 The Catholic Education Service;
 - 10.2.4 The Education & Skills Funding Agency;
 - 10.2.5 The Diocese of Westminster;
 - 10.2.6 The Disclosure and Barring Service;
 - 10.2.7 The Local Safeguarding Board relevant to the Academies location;
 - 10.2.8 The Teaching Regulation Agency;
 - 10.2.9 The Teachers' Pension Service.
 - 10.2.10 The Local Government Pension Scheme which is administered by Hertfordshire, Hillingdon, Hounslow and Brent Pension Scheme Administrators for our academies depending on their location;
 - 10.2.11 Our external HR providers;
 - 10.2.12 OfSTED;
 - 10.2.13 Our external auditors;
 - 10.2.14 Our external payroll providers;
 - 10.2.15 Our external IT Provider;
 - 10.2.16 HMRC;
 - 10.2.17 The Police or other law enforcement agencies;
 - 10.2.18 Our legal advisors and other consultants;
 - 10.2.19 Insurance providers / the Risk Protection Arrangement;
 - 10.2.20 Occupational health advisors;
 - 10.2.21 Exam boards including AQA, OCR, Edexcel, WJEC, BTEC;
 - 10.2.22 the Joint Council for Qualifications;
 - 10.2.23 the Standards and Testing Agency;
 - 10.2.24 NHS health professionals including educational psychologists and school nurses;
 - 10.2.25 Education Welfare Officers;
 - 10.2.26 Courts, if ordered to do so;
 - 10.2.27 Prevent teams in accordance with the Prevent Duty on schools;
 - 10.2.28 Other schools, for example, if we are requested to provide a reference.



- 10.3 We require third parties to respect the security of your data and to treat it in accordance with the law. Some of the organisations referred to above are joint data controllers. This means we are all responsible to you for how we process your data.
- 10.4 We may transfer your personal information outside the UK or EU. If we do, you can expect a similar degree of protection in respect of your personal information.

11. DATA SHARING WITH THE DIOCESE OF WESTMINSTER

- 11.1 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:
- 11.1.1 Personal information (such as name, date of birth, address, gender, TRN).
 - 11.1.2 Characteristics (such as ethnicity, religion, language, medical conditions, nationality).
 - 11.1.3 Standards data for the Diocesan Inspection of Catholic Schools.
 - 11.1.4 Continued Professional Development (Training data, Inset days).
 - 11.1.5 Information requested by the Bishop.
 - 11.1.6 Financial Benchmarking data.

12. DATA SHARING WITH THIRD PARTIES

- 12.1 We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you, where it is needed in the public interest or for official purposes, or where we have your consent.
- 12.2 Which third-party service providers process your personal information?
- 12.3 “Third parties” includes third-party service providers (including contractors and designated agents). The following activities are carried out by third-party service providers:

SIMS / Arbor	School Information Management System
EduPay TES	Outsourced payroll provider
The Disclosure and Barring Service	Criminal convictions check



HMRC	Tax purposes
The Teachers Pension Service	Pension details for Teachers
The Local Government Pension Scheme for Hillingdon, Hertfordshire, Brent and Hounslow	Pension details for Support Staff
Parentpay Limited	On line school payment system
Cunninghams Catering System	Cashless catering
Google Classroom	Cloud service
Microsoft Office 365	Email and cloud services
Paxton Security System	School entry system
Signin	Entry system
BACs Bureau	Enables payment of payroll via BACs

12.4 Department for Education:

12.4.1 We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding/expenditure and the assessment educational attainment.

12.4.2 We are required to share information about our students with the Department for Education (DfE) under regulation 7 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 as amended.

12.5 The following is information provided by the DfE concerning the reason it collects data about school employees:

12.5.1 The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Student Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

12.5.2 To find out more about the data collection requirements placed on us by the DfE including the data that we share with them, go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.



12.5.3 The DfE may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff by:

12.5.3.1 Conducting research or analysis;

12.5.3.2 Producing statistics; and / or

12.5.3.3 Providing information, advice or guidance

12.5.4 The DfE has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

12.5.4.1 Who is requesting the data;

12.5.4.2 The purpose for which it is required;

12.5.4.3 The level and sensitivity of data requested;

12.5.4.4 The arrangements in place to securely store and handle the data

12.5.5 To be granted access to school workforce information, organisations must comply with the DfE's strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

12.5.6 For more information about the DfE's data sharing process, please visit: <https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>. To contact the department, please visit: <https://www.gov.uk/contact-dfe>.

13. DATA SHARING WITH THIRD PARTIES AND SECURITY

13.1 All our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

13.2 What about other third parties?

13.2.1 We may share your personal information with other third parties, for example if there was a TUPE transfer of staff in future. We may also need to share your personal information with a regulator or to otherwise comply with the law.

13.2.2 From time to time, we may disclose your personal data in response to a request for information pursuant to the Freedom of Information Act 2000 or following a data subject access request. We may approach you for your consent but, in any event, we will only disclose your personal data if



we are satisfied that it is reasonable to do so in all the circumstances. This means that we may refuse to disclose some or all of your personal data following receipt of such a request.

- 13.3 We may sometimes transfer your personal data outside of the UK or EU if, for example, we are arranging a school trip and we are booking transport, accommodation or activities. In these circumstances, we will obtain your consent for us to process your data in this way.

14. DATA SECURITY

- 14.1 We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.
- 14.2 Third parties who are processing personal data on our behalf will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.
- 14.3 We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

15. DATA RETENTION

- 15.1 We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, insurance or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements. Usually we will hold data for 7 years after you have left us, in line with financial record-keeping requirements. Personal data is retained in line with the Department for Education (DfE) Data Retention Schedule (2025).
- 15.2 In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information.



16. RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION

- 16.1 It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.
- 16.2 Under certain circumstances, by law you have certain rights, please see this [link](#) for further information.
- 16.3 If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Academy Data Protection Lead in writing.
- 16.4 The legal timescales for the school / trust to respond to a Subject Access Request is one calendar month, though sometimes a 60 day extension to this timescale may be added, depending on certain criteria; you would be informed if this extension was necessary. As the school/trust has limited staff resources outside of term time, we encourage staff 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.
- 16.5 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.
- 16.6 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.

17. RIGHT TO WITHDRAW CONSENT

- 17.1 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 Academy



Data Protection Lead. 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, or for safeguarding purposes.

18. DATA PROTECTION OFFICER

- 18.1 We have appointed a data protection officer (DPO) to oversee compliance with this privacy notice. The Data Protection Officer (DPO) for DoWAT is the Trust Chief Financial Officer (CFO), named [here](#), contactable via dpo@dowat.co.uk, 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. The Academy Deputy Data Protection Officer (DDPO) Emma Gritten
- 18.2 You can contact the Information Commissioners Office on 0303 123 1113 or via email <https://ico.org.uk/global/contact-us/email/> or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF.

19. CHANGES TO THIS PRIVACY NOTICE

- 19.1 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.

