Waltham International College

2.0 Compliance

2.5 Data Protection and Retention Policy

Version Number: 13

Reviewed by | Approved by: Compliance Review | BoG
Review date | Approved date: May 2026 | July 2026

Compliance Alignment Statement

This version of the Data Protection and Retention Policy has been aligned to current UK and Office for Students requirements as of May 2026. The substantive changes are listed below.

Version Control Statement

Version	Date	Changes	Reason	Author	Next Review
1	11/10/15		New Policy	IT Director	10/10/16
2	14/12/16	None	No changes in the Law, policy and processes	IT Director	13/12/17
3	23/05/18	Changes made to align the policy with the latest GDPR to be effective from 25th May 2018	New GDPR changes implemented	DCQ	22/05/19
4	23/01/19	Inserted statement for the College to seek express permission for learners' data to be shared for internal/external transfers (signposting)	Annual Review	Head of HE	Jul/Aug 19
5	10/08/2019	Responsibilities and data disposal are updated alongside updates from new GLA contract requirements for data retention	Annual Review	Assistant Principal	August 2020
6	27/09/2019	Minor Amendments/updates applied to make policy clearer	Updates	Director Operations FE	Sep 2020
7	July 2020	Substantial review	Annual Review	Head of HE	Jul/Aug 2020
8	Aug 2021	None	Annual Review	IT Manager	Aug 2022
9	Aug 2022	Grammar check, domain updates and minor adjustments	Annual Review	IT Manager	Aug 2023
10	September 2023	None	Annual Review	IT Manager	September 2024
11	May 2024	None	Quarter Review	IT Manager	August 2025
12	August 2025	Minor formatting changes Updated External References Added Purpose	Annual Review	IT Manager	August 2026
13	May 2026	- Textual revisions made throughout to bring the policy into compliance with applicable regulation – including UK GDPR alignment, OfS conditions, ICO guidance, updated retention schedule, DPO role formalized - Updated External Reference and Related Policies List - Added appendices 1 - 7	Compliance Alignment 2026 (OfS)	QA Compliance Review	August 2027

External Reference Points

- UK General Data Protection Regulation (UK GDPR) – as retained in UK law by the European Union (Withdrawal) Act 2018 and amended by the Data Protection Act 2018
- Data Protection Act 2018 (DPA 2018)
- Freedom of Information Act 2000 (FOIA)
- Privacy and Electronic Communications Regulations 2003 (PECR)
- Higher Education and Research Act 2017
- OfS Conditions of Registration – Conditions F3 and F4 (Provision of Information)
- OfS Transparency Conditions
- Information Commissioner's Office (ICO) Guidance and Codes of Practice
- ICO Data Retention Guidance
- Records Management Code of Practice for Health and Social Care 2021 (for health data held by the College)
- Equality Act 2010
- Limitation Act 1980
- Companies Act 2006 (where applicable to records)

Related Policies and Documents

Affects all other policy documents. This document should however be read together with the following documents:

- 1.04 Contingency and Business Continuity Plan
- 2.1 Published Information Policy
- 2.04 eSafety Policy
- 2.07 ICT Policy
- 2.08 Information Security Policy
- 2.09 Incident Response Policy
- 3.03 Information Advice and Guidance (IAG) Policy
- 5.03 Staff Handbook
- Student Handbook

Contents

Compliance Alignment Statement 2
Version Control Statement 2
External Reference Points 3
1. Purpose 5
2. Scope 5
3. Introduction 5
4. Definitions 5
4.1 Key Definitions under UK GDPR 5
5. Data Protection Principles 6
6. Policy 7
6.1 Whose personal data does the College process? 7
6.2 Lawful Bases for Processing 7
6.3 How We Use Your Personal Data 7
6.4 Privacy Notices 8
6.5 Categories of information held 8
6.6 Special category (sensitive) personal data 8
6.7 Data Subject Rights 9
6.8 Data Breaches 9
6.9 Data Sharing and Third Parties 9
6.10 Data protection Impact Assessments (DPIAs) 10
6.11 Data Retention Schedule 10
6.11.1 AEB Contractual Retention requirements 11
6.12 Destruction and Disposal of Records and Data 11
6.12.1 Paper Records 11
6.12.2 Electronic Records and Systems 11
6.12.3 Internal Correspondence and Unassigned Records 11
6.12.4 Found or unattributed storage devices 11
6.13 Responsibilities 12
6.13.1 Data Protection Officer (DPO) 12
6.13.2 Senior Leadership Team 12
6.13.3 Department Heads and Managers 12
6.13.4 All Staff 12
6.14 Compliance and Monitoring 12
7. Appendices 13
7.1 Appendix 1: Record of Processing Activities (ROPA) Template 13
7.2 Appendix 1: Data Protection Impact Assessment (DPIA) Template 13
7.3 Appendix 3: Data Subject Rights Request Form 14
7.4 Appendix 4: Data Breach Report Form and Register 16
7.5 Appendix 5: Third Party Data Processing Agreement Template 18
7.6 Appendix 6: Privacy Notice – Students 20
7.7 Appendix 7: Privacy Notice – Staff 22

1. Purpose

The purpose of this policy is to ensure that Waltham International College (WIC, “the Cpllege”) processes personal data responsibly, lawfully, securely, and transparently, in full compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). This policy establishes the principles, rights, obligations, and procedures for collecting, processing, retaining, and disposing of personal data, protecting the rights and privacy of all data subjects, maintaining data integrity, and fulfilling the College's operational, legal, and regulatory obligations, including those arising from registration with the Office for Students (OfS).

2. Scope

This policy applies to all personal data collected and processed by WIC, regardless of format (electronic, paper-based, or verbal), in the conduct of its business. It applies to all staff, students, governors, contractors, volunteers, and any other parties acting on behalf of WIC who process personal data. All persons covered by this policy are required to read, understand, and comply with it. Failure to comply may result in disciplinary action and/or referral to the ICO.

3. Introduction

WIC is registered with the Information Commissioner's Office (ICO) as a data controller under the DPA 2018. WIC is the 'controller' of personal data provided by staff, students, applicants, and other stakeholders in order to carry out its business. The College is committed to fostering a culture of transparency, accountability, and respect for individual rights in the processing of personal data.

The UK GDPR replaces the EU GDPR as retained and adapted in UK law following Brexit. The DPA 2018 supplements the UK GDPR and provides the domestic legislative framework for data protection in the United Kingdom. References in this policy to 'UK GDPR' incorporate the provisions of the DPA 2018 where applicable.

As an OfS-registered provider, WIC is additionally required to comply with transparency and information publication obligations set out in OfS Conditions F3 and F4, and to maintain accurate data submissions to the OfS and other regulatory bodies (including the Higher Education Statistics Agency (HESA)) in accordance with the Higher Education and Research Act 2017.

4. Definitions

4.1 Key Definitions under UK GDPR

Term	Definition
Personal Data	Any information relating to an identified or identifiable natural person ('data subject'). An identifiable person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, identification number, location data, an online identifier, or factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.
Special Category Data	Personal data that is particularly sensitive and requires additional protections. Under Article 9 UK GDPR, special categories include: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data processed to uniquely identify a person; data concerning health; and data concerning a person's sex life or sexual orientation.

Data Controller	The College, as the entity that determines the purposes and means of processing personal data.
Data Processor	A third party that processes personal data on behalf of WIC (e.g. cloud service providers, payroll processors).
Data Subject	The natural person to whom the personal data relates (e.g. students, staff, applicants).
Processing	Any operation performed on personal data, including collection, recording, storage, use, disclosure, erasure, or destruction.
Data Protection Officer (DPO)	The designated officer responsible for overseeing WIC's data protection compliance, advising on obligations, and acting as the point of contact for the ICO.
Consent	A freely given, specific, informed, and unambiguous indication of a data subject's agreement to the processing of their personal data, as defined in Article 7 UK GDPR.
Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed (UK GDPR Article 4(12)).

5. Data Protection Principles

WIC is committed to processing all personal data in accordance with the six data protection principles set out in Article 5 UK GDPR:

Lawfulness, Fairness, and Transparency	Personal data shall be processed lawfully, fairly, and in a transparent manner. WIC will identify and document a lawful basis for each processing activity and will provide clear privacy notices to all data subjects.
Purpose Limitations	Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
Data Minimisation	Personal data shall be adequate, relevant, and limited to what is necessary for the purposes for which it is processed.
Accuracy	Personal data shall be accurate and, where necessary, kept up to date. Every reasonable step will be taken to ensure that inaccurate personal data is erased or rectified without delay.
Storage Limitation	Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the stated purposes. WIC's Data Retention Schedule (see Section 6.10) specifies the retention periods for each category of data.
Integrity and Confidentiality (Security)	Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, and against accidental loss, destruction, or damage. WIC implements technical and organisational security measures consistent with the Information Security Policy (2.08).

6. Policy

6.1 Whose personal data does the College process?

WIC processes personal data relating to:

- Current, former, and prospective students
- Current, former, and prospective staff
- Governors and Board members
- Contractors, consultants, and agency workers
- Parents and guardians (where students are under 18)
- Alumni and donors
- External partners and suppliers
- Visitors to College premises

6.2 Lawful Bases for Processing

WIC will identify and document a lawful basis for each processing activity in its Record of Processing Activities (ROPA). Lawful bases under Article 6 UK GDPR include:

- Contract: Processing is necessary for the performance of a contract with the data subject (e.g. the student or employment contract).
- Legal Obligation: Processing is necessary for compliance with a legal obligation (e.g. statutory returns to HESA, the OfS, HMRC, or DfE).
- Vital Interests: Processing is necessary to protect the vital interests of a person.
- Public Task: Processing is necessary for the performance of a task in the public interest.
- Legitimate Interests: Processing is necessary for the legitimate interests of the College, subject to balancing against the data subject's rights.
- Consent: The data subject has given freely given, specific, informed, and unambiguous consent.

For Special Category data, WIC relies on one of the conditions in Article 9 UK GDPR (e.g. substantial public interest, employment law obligations, or explicit consent) supported by an appropriate policy document where required by Schedule 1 DPA 2018.

6.3 How We Use Your Personal Data

WIC uses the personal data it holds to carry out its educational, administrative, and regulatory functions. The main ways in which we use personal data include:

- Processing applications, enrolments, and registrations for courses and programmes
- Maintaining internal records to enable the College to provide high-quality services to students, staff, and other stakeholders
- Managing student attendance, progress, and achievement
- Responding to individual enquiries and providing Information, Advice and Guidance (IAG)
- Processing payroll, staff appraisals, and employment-related administration

- Complying with statutory reporting obligations to bodies including HESA, the OfS, DfE, HMRC, and Ofsted
- Contacting individuals about College services, events, or matters relevant to their relationship with WIC
- Conducting research, quality assurance, and service improvement activities

WIC will not use personal data for purposes that are incompatible with those for which it was collected. Where the College wishes to use personal data for a new purpose, it will assess whether this is lawfully permissible and, where required, will seek fresh consent or issue an updated privacy notice.

Where internal transfers between WIC's and HE provisions, or external referrals to other organisations, are in the interests of the student, WIC will seek the student's express permission before sharing their information for that purpose.

The lawful bases on which WIC relies for its processing activities are documented in the Record of Processing Activities (ROPA) and summarised in section 6.2.

6.4 Privacy Notices

WIC will provide a clear, accessible, and layered privacy notice to all data subjects at the point of data collection, or as soon as practicable thereafter. Privacy notices will be published on the College website and updated whenever processing activities change materially. Privacy notices will comply with Articles 13 and 14 UK GDPR and ICO transparency requirements.

6.5 Categories of information held

The College holds, among other categories, the following types of personal data:

- Identity and contact information (name, address, date of birth, National Insurance number)
- Academic records (qualifications, assessment grades, attendance, progression)
- Financial information (fee payments, bursary and hardship applications, payroll data)
- Employment records (contracts, appraisals, disciplinary and grievance records)
- Safeguarding and wellbeing records (disclosed disabilities, support plans, mental health disclosures)
- Equality and diversity monitoring data
- CCTV footage and access control records
- IT usage logs and network activity records
- References and third-party disclosures

6.6 Special category (sensitive) personal data

WIC processes special category personal data (including health data, disability status, and ethnicity monitoring data) where necessary for legitimate educational, safeguarding, or statutory purposes. All processing of special category data is documented in the ROPA with an identified Article 9 condition and, where required by DPA 2018 Schedule 1, a separate Appropriate Policy Document. Access to special category data is strictly controlled on a need-to-know basis.

6.7 Data Subject Rights

WIC respects and facilitates the following data subject rights under UK GDPR:

- Right of Access (Subject Access Request – SAR): Data subjects may request a copy of their personal data held by the College. WIC will respond within one calendar month (extensible by two further months in complex cases), free of charge, in compliance with Article 15 UK GDPR.
- Right to Rectification: Data subjects may request correction of inaccurate personal data (Article 16).
- Right to Erasure ('Right to be Forgotten'): Data subjects may request deletion of personal data where one of the Article 17 conditions applies, subject to legal retention obligations.
- Right to Restrict Processing: Data subjects may request restriction of processing in defined circumstances (Article 18).
- Right to Data Portability: Data subjects may request their data in a machine-readable format where processing is based on consent or contract and carried out by automated means (Article 20).
- Right to Object: Data subjects may object to processing based on legitimate interests or for direct marketing purposes (Article 21).
- Rights in Relation to Automated Decision-Making: WIC will not subject data subjects to solely automated decisions that produce significant legal effects without appropriate human review, unless expressly permitted by law (Article 22).

All data subject rights requests must be submitted to the Data Protection Officer (DPO). WIC will not charge a fee for responding to requests unless they are manifestly unfounded or excessive. Complaints about WIC's handling of personal data may be directed to the ICO at www.ico.org.uk or by calling 0303 123 1113.

6.8 Data Breaches

WIC maintains a Data Breach Register and follows the procedures set out in the Incident Response Policy (2.09) for all actual or suspected data breaches. In accordance with Article 33 UK GDPR, personal data breaches that are likely to result in a risk to the rights and freedoms of individuals must be reported to the ICO within 72 hours of the College becoming aware of the breach. Where there is a high risk to individuals, those individuals must also be notified without undue delay (Article 34 UK GDPR). All breaches, regardless of whether notification is required, must be logged and reviewed to prevent recurrence.

6.9 Data Sharing and Third Parties

WIC will only share personal data with third parties where there is a lawful basis and a legitimate purpose. Statutory data sharing includes returns to HESA, the OfS, DfE, HMRC, and other regulatory bodies as required by law. Where WIC engages a data processor, a Data Processing Agreement (DPA) compliant with Article 28 UK GDPR will be in place before processing commences. WIC will not sell personal data to third parties. International transfers of personal data will only occur where adequate safeguards are in place as required by Chapter V UK GDPR.

6.10 Data protection Impact Assessments (DPIAs)

WIC will conduct a DPIA before undertaking any new processing activity that is likely to result in a high risk to the rights and freedoms of individuals, consistent with Article 35 UK GDPR and ICO guidance. DPIAs will be led by the DPO and documented in the DPIA Register.

6.11 Data Retention Schedule

Personal data will be retained for no longer than is necessary for the purposes for which it was collected, as specified in the following Data Retention Schedule. Retention periods reflect statutory obligations, regulatory requirements (including OfS and HESA requirements), best practice (including ICO guidance and the JISC Records Management Toolkit), and institutional need.

Category of Record	Retention Period	Statutory / Regulatory Basis
Student academic records (transcripts, grades, qualifications)	6 years after programme end; permanent for degree-level and higher qualifications	HERA 2017; OfS Conditions; Limitation Act 1980
Student enrolment and registration records	6 years after programme end	Limitation Act 1980; OfS Conditions
Student financial records (tuition fees, bursaries, loans)	7 years after last transaction	HMRC; Limitation Act 1980
Student attendance and engagement records	3 years after programme end	OfS Conditions; Student Loan Company
Student welfare and safeguarding records	7 years from date of last action (or until the student turns 25, whichever is later)	KCSIE 2024; Local Authority guidance
Staff employment records (contracts, payroll, appraisals)	7 years after employment ends	HMRC; Employment Rights Act 1996; Limitation Act 1980
Staff DBS disclosure records	6 months (outcome recorded only after 6 months)	DBS Code of Practice
Recruitment records (unsuccessful applicants)	12 months from recruitment decision	Equality Act 2010; ICO Guidance
CCTV footage	31 days (unless evidence preservation required)	ICO CCTV Code of Practice
Financial accounting records	7 years	Companies Act 2006; HMRC
Governance records (Board minutes, policies)	Permanent	Higher Education and Research Act 2017; Charity Commission
Health and safety accident records	7 years (or until employee's 21st birthday for incidents involving minors)	RIDDOR; Limitation Act 1980
Email communications	3 years from creation (unless record of decision)	ICO Guidance

Examination and assessment records	As required by awarding body; minimum 5 years	JCQ regulations; Awarding Body requirements

Records not covered by the above schedule will be retained for a minimum of 6 years unless a shorter or longer period is specified by applicable legislation or regulatory requirement. The DPO will review and update the Retention Schedule annually.

6.11.1 AEB Contractual Retention requirements

In addition to the statutory retention periods set out above, WIC is subject to contractual data retention obligations arising from its GLA AEB (GLA Adult Education Budget) Procured Provision contract. All original invoices, delivery evidence, management information returns, and supporting documentation necessary to verify services delivered under the GLA AEB (2019–23) contract must be retained until at least 31 December 2030. This obligation applies regardless of whether the relevant records would otherwise fall due for destruction under the schedule above.

The DPO, in conjunction with the Finance and Operations leads, is responsible for ensuring that AEB related records are appropriately flagged and excluded from routine destruction cycles until this contractual retention date has passed.

6.12 Destruction and Disposal of Records and Data

6.12.1 Paper Records

Paper records containing personal data must be destroyed by cross-cut shredding using a minimum DIN 66399 Level P-4 shredder, or placed in designated confidential waste bins and collected by an approved confidential waste contractor. Certificate of destruction must be obtained and retained.

6.12.2 Electronic Records and Systems

Electronic records must be securely deleted using approved data-wiping software (meeting HMG IA Standard No. 5) or through physical destruction of media. Cloud-hosted data must be formally deleted in accordance with Data Processing Agreements and confirmation obtained from processors. Devices must be decommissioned following the procedure set out in the ICT Policy (2.07).

6.12.3 Internal Correspondence and Unassigned Records

Unless a specific retention period applies by reference to the subject matter of the correspondence (in which case the relevant period in the Retention Schedule governs), internal correspondence and memoranda, including internal emails, meeting notes, general enquiries and replies, and communications of inconsequential subject matter, should be deleted or securely destroyed once their operational purpose has been served, and in any event no later than 2 years from creation.

Where internal correspondence forms part of, or directly supports, a substantive record (such as a student file, contract, or formal decision), it should be retained and disposed of in line with the retention period applicable to that substantive record.

6.12.4 Found or unattributed storage devices

Where a portable storage device (such as a USB drive or memory card) is found on College premises and handed to the IT Manager, the device will be held securely for 28 days to allow the owner to reclaim it. If unclaimed after that period, the device will be disposed of securely in accordance with the electronic disposal procedure in section 6.11.2 above, and a record of disposal made.

6.13 Responsibilities

6.13.1 Data Protection Officer (DPO)

- Oversee and monitor WIC's compliance with UK GDPR and DPA 2018
- Maintain the Record of Processing Activities (ROPA) and DPIA Register
- Provide advice and training to staff on data protection obligations
- Act as the primary point of contact with the ICO
- Manage data breach reporting and the Data Breach Register
- Review and update this policy annually
- Report to the OMC and Board of Governors on data protection matters at least annually

6.13.2 Senior Leadership Team

- Ensure data protection is embedded as a governance priority
- Allocate adequate resources to support the DPO and data protection compliance
- Ensure that data protection considerations are incorporated into new projects and service developments (Privacy by Design)

6.13.3 Department Heads and Managers

- Ensure staff within their teams receive appropriate data protection training
- Maintain awareness of the personal data processed within their areas and ensure compliance with this policy
- Report suspected data breaches to the DPO immediately

6.13.4 All Staff

- Process personal data only as necessary for their role and in accordance with this policy
- Complete mandatory data protection training as part of induction and annually thereafter
- Report suspected data breaches or non-compliance to the DPO without delay
- Not share personal data with unauthorised individuals or organisations

6.14 Compliance and Monitoring

The DPO will conduct annual data protection audits and report findings to the OMC. The ROPA will be reviewed at least annually. Staff compliance with mandatory training will be monitored by the DPO and HR. Any material non-compliance or data breach with significant risk will be escalated to the Board of Governors. This policy will be reviewed annually or sooner in the event of legislative changes (including any updates to UK GDPR via the Data Protection and Digital Information Act or equivalent legislation).

7. Appendices

7.1 Appendix 1: Record of Processing Activities (ROPA) Template

This template must be completed and maintained by the Data Protection Officer. A separate row should be completed for each distinct processing activity. The ROPA must be reviewed at least annually and updated whenever a new processing activity commences or an existing activity changes materially.

Field	Details
Processing Activity Reference	
Name of Processing Activity	
Department / Function responsible	
Description of processing activity	
Categories of data subjects	e.g. students / staff / applicants / governors / visitors
Categories of personal data processed	e.g. identity, contact, academic, financial, health
Special category data involved? (Y/N)	If yes, state Article 9 condition relied upon
Appropriate Policy Document required? (Y/N)	Required where Schedule 1 DPA 2018 condition applies
Purposes of processing	
Lawful basis (Article 6 UK GDPR)	e.g. Contract / Legal Obligation / Legitimate Interests / Consent
Article 9 condition (if special category data)	
Is data shared with third parties?	If yes, list recipients and basis for sharing
Data Processing Agreement in place? (Y/N)	
Is data transferred outside the UK?	If yes, state transfer mechanism (adequacy / SCCs / other)
Retention period	Cross-reference to Retention Schedule (Section 6.11)
Security measures in place	e.g. encryption, access controls, pseudonymisation
Date record created / last reviewed	
Reviewed by (DPO)	

Completed ROPA entries are held securely by the DPO and are not appended to this policy in their entirety. This template is provided for reference and for use when establishing new processing activities.

7.2 Appendix 2: Data Protection Impact Assessment (DPIA) Template

A DPIA must be completed before commencing any new processing activity likely to result in a high risk to the rights and freedoms of individuals (Article 35 UK GDPR). It must be led by the DPO and approved before processing begins. If the DPIA identifies a high residual risk that cannot be mitigated, the ICO must be consulted prior to processing.

Section 1 – Project / Processing Activity Overview

Field	Details
Project / activity name	
Department / lead officer	
Date of assessment	
DPO name	
Description of the new processing activity	
Purposes of processing	
Categories of personal data to be processed	
Categories of data subjects affected	
Volume / scale of processing	
Is special category data involved?	If yes, specify categories and Article 9 condition
Technology / systems to be used	
Is data to be shared with third parties?	If yes, identify recipients and legal basis

Section 2 – Necessity and Proportionality

Question	Response
Is the processing necessary for the stated purpose?	
Could the purpose be achieved with less data or less intrusive processing?	
Is the lawful basis clearly identified and documented?	
Have data subjects been / will they be informed via a privacy notice?	
Are data subject rights adequately provided for?	
What is the planned retention period? Is it justified?	

Section 3 – Risk Identification and Assessment

Risk identified	Likelihood (H/M/L)	Severity (H/M/L)	Overall risk (H/M/L)	Proposed mitigation measure	Residual risk after mitigation

Section 4 – Outcome and Sign-off

Field	Details
Overall risk rating (prior to mitigation)	
Overall residual risk rating (after mitigation)	
Is ICO consultation required? (High residual risk = yes)	
DPO recommendation	Approved to proceed / Approved with conditions / Do not proceed
Conditions / actions required before processing commences	
DPO signature and date	
Senior Leadership sign-off (where required)	
Date of next review	

7.3 Appendix 3: Data Subject Rights Request Form

Use this form to submit any request relating to your personal data rights under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Completed forms should be submitted to the Data Protection Officer at dataprotection@wic.ac.uk or by post to: Data Protection Officer, Waltham International College, Glebe House, Vicarage Drive, Barking, IG11 7NR. WIC will respond within one calendar month of receipt of a valid request.

Part A – Your Details

Field	Your response
Title	
Surname	
Forename(s)	
Date of birth (to assist identification)	
Address	
Email address	
Telephone number	
Any other name(s) by which you have been known	
Your relationship to the College	e.g. current student / former student / current staff / former staff / applicant / other
Student / staff ID number (if known)	

Part B – Nature of Request

Please indicate the right(s) you wish to exercise (tick all that apply):

Right	Select	UK GDPR Article
Right of Access (Subject Access Request – copy of my personal data)	☐	Article 15
Right to Rectification (correct inaccurate personal data)	☐	Article 16
Right to Erasure ('Right to be Forgotten')	☐	Article 17
Right to Restrict Processing	☐	Article 18
Right to Data Portability	☐	Article 20
Right to Object to Processing	☐	Article 21
Right relating to Automated Decision-Making	☐	Article 22

Part C – Description of Request
Please describe your request in as much detail as possible to enable us to locate your data and respond accurately. If you are making a Subject Access Request, please indicate the type of records or time period you are interested in.

Details of request (continue on a separate sheet if necessary)

Part D – Proof of Identity
The Data Protection Act 2018 requires the College to verify the identity of the person making a request before responding. Please attach a scanned or clear photographic copy of one form of photographic identification (e.g. passport, photo card driving licence). If supply of this documentation is problematic, please contact dataprotection@wic.ac.uk to discuss alternative arrangements.

Identity document provided	
Type of document	e.g. passport / driving licence / other
Document reference number (optional)	

Part E – Declaration
I confirm that the information provided in this form is accurate and that I am the data subject named in Part A (or am authorised to act on their behalf). I understand that providing false information may constitute an offence under the Data Protection Act 2018.

Field	
Signature	
Date	
If acting on behalf of another person, state authority	e.g. parent / guardian / power of attorney

WIC will acknowledge receipt of your request within five working days and will respond in full within one calendar month. We may extend this period by up to two further months for complex or multiple requests, in which case we will notify you within one month of receipt. There is no charge for submitting a request unless it is manifestly unfounded or excessive.

7.4 Appendix 4: Data Breach Report Form and Register

This form must be completed for all actual or suspected personal data breaches, regardless of severity. All breaches must be reported to the DPO immediately upon discovery. Where the breach is likely to result in a risk to the rights and freedoms of individuals, the ICO must be notified within 72 hours (Article 33 UK GDPR). Where there is a high risk, affected individuals must also be notified without undue delay (Article 34 UK GDPR).

Section 1 – Initial Notification

Field	Details
Date and time breach discovered	
Date and time breach occurred (if known)	
Reported by (name and role)	
Department	
Date and time reported to DPO	
Brief description of the incident	

Section 2 – Nature of Breach

Field	Details
Type of breach	Confidentiality / Integrity / Availability (select all that apply)
How did the breach occur?	e.g. lost device / unauthorised access / misdirected email / system failure / theft / human error
Categories of personal data affected	e.g. identity, contact, financial, health, academic
Does the breach involve special category data?	Yes / No. If yes, specify categories.
Approximate number of data subjects affected	
Approximate volume of records affected	
Has the data been recovered or contained?	Yes / No / Partially – provide details
Is the breach ongoing?	Yes / No

Section 3 – Risk Assessment

Question	Response
What is the potential impact on affected individuals?	e.g. identity theft / financial loss / reputational harm / discrimination / physical harm / distress
Likelihood of harm materialising	High / Medium / Low
Overall risk level	High / Medium / Low
Is ICO notification required? (likely risk to individuals = yes)	Yes / No / Under assessment
Is individual notification required? (high risk = yes)	Yes / No / Under assessment

Section 4 – Actions Taken

Field	Details
Immediate containment actions taken	
Date / time ICO notified (if applicable)	
ICO reference number (if notified)	
Date / time affected individuals notified (if applicable)	
Method of individual notification	e.g. email / letter / telephone
Remedial / preventive actions identified	
Target completion date for remedial actions	
Person responsible for remedial actions	

Section 5 – DPO Sign-off

Field	Details
DPO name	
Date of sign-off	
Breach reference number (for Register)	
Outcome / lessons learned	
Escalated to Board of Governors?	Yes / No. If yes, date escalated:

Data Breach Register – Summary Log

The DPO maintains a full Breach Register. The table below provides a summary log format. A separate detailed form (above) must be held for each breach.

Ref	Date discovered	Date occurred	Nature of breach	Data categories affected	No. of subjects	Risk level	ICO notified?	Individuals notified?	Status

7.5 Appendix 5: Third Party Data Processing Agreement Template

This template sets out the minimum provisions required in any Data Processing Agreement (DPA) between Waltham International College ("the Controller") and a third party processing personal data on its behalf ("the Processor"). It must be completed and signed before any processing commences. The DPO must retain a copy of all executed agreements. This template should be reviewed by legal counsel for complex or high-risk arrangements.

Data Processing Agreement

Field	Details
Agreement reference	
Date of agreement	
Controller	Waltham International College, Glebe House, Vicarage Drive, Barking, IG11 7NR
Controller contact / DPO	dataprotection@wic.ac.uk
Processor (company name)	
Processor registered address	
Processor contact for data protection matters	
ICO registration number of Processor (if applicable)	

Schedule 1 – Details of Processing

Field	Details
Subject matter of processing	
Duration of processing	
Nature of processing	e.g. storage / analysis / transmission / support services
Purpose of processing	
Categories of personal data to be processed	
Special category data involved?	Yes / No. If yes, specify categories and Schedule 1 DPA 2018 condition.
Categories of data subjects	
Permitted sub-processors (if any)	List names or state 'None'. Sub-processor changes require prior written consent.
Location(s) of processing (countries)	
International transfer mechanism (if outside UK)	e.g. UK adequacy decision / International Data Transfer Agreement (IDTA) / other

Schedule 2 – Processor Obligations

The Processor agrees to:

1. Process personal data only on documented instructions from the Controller, unless required to do so by applicable law.
2. Ensure that persons authorised to process personal data are subject to appropriate confidentiality obligations.
3. Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (Article 32 UK GDPR), including as appropriate: pseudonymisation and encryption; ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems; and the ability to restore data following an incident.
4. Not engage sub-processors without prior specific or general written authorisation from the Controller.
5. Assist the Controller in responding to data subject rights requests and in meeting obligations under Articles 32–36 UK GDPR (security, breach notification, DPIAs, prior consultation).
6. At the Controller's election, delete or return all personal data at the end of the processing relationship, and delete existing copies unless storage is required by applicable law.
7. Provide the Controller with all information necessary to demonstrate compliance with Article 28 UK GDPR and allow for and contribute to audits and inspections.
8. Notify the Controller immediately upon becoming aware of a personal data breach.

Signatures

	Controller (WIC)	**Processor**
Signed by		
Name and title		
Date		

7.6 Appendix 6: Privacy Notice – Students

Waltham International College – Student Privacy Notice

This privacy notice explains how Waltham International College (WIC, "we", "us", "our") collects and uses your personal data. It applies to all current, former, and prospective students. This notice is issued in accordance with Articles 13 and 14 of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Who we are

Waltham International College Limited is registered as a data controller with the Information Commissioner's Office (ICO). Our ICO registration number is available on request. Our registered address is: Glebe House, Vicarage Drive, Barking, IG11 7NR. You can contact our Data Protection Officer at dataprotection@wic.ac.uk.

What personal data we collect

We collect and hold the following categories of personal data about you:

Category	Examples
Identity and contact information	Name, date of birth, address, email, telephone number, National Insurance number
Academic records	Qualifications, assessment grades, attendance records, progression data, prior learning
Financial information	Tuition fee payments, bursary or hardship applications, Student Loan Company records
Welfare and safeguarding information	Disclosed disabilities, learning support plans, mental health disclosures, safeguarding records
Equality and diversity data	Ethnicity, gender, disability status (for statutory reporting purposes)
CCTV and access control data	Images captured on campus CCTV systems and access control logs
IT usage data	College network activity and usage logs
Application and admissions data	Application forms, references, prior qualifications

Special category data

In some circumstances we collect special category data, including health data, disability information, and ethnicity monitoring data. We only do so where necessary for a legitimate educational, safeguarding, or statutory purpose, and where we have identified an appropriate condition under Article 9 UK GDPR.

Why we collect your data and our lawful basis

Purpose	Lawful basis (Article 6 UK GDPR)
Processing your application and enrolment	Contract (performance of the student contract)
Managing your attendance, progress, and achievement	Contract; Legal Obligation
Providing learning support and welfare services	Vital Interests (where relevant); Legal Obligation; Consent

Statutory returns to HESA, OfS, DfE, HMRC, and Ofsted	Legal Obligation
Providing Information, Advice, and Guidance (IAG)	Contract; Legitimate Interests
Equality and diversity monitoring	Legal Obligation; Substantial Public Interest
Operating campus CCTV for safety and security	Legitimate Interests
Communicating with you about your studies and College services	Contract; Legitimate Interests
Referring you internally between FE and HE provision (where relevant)	Consent
Conducting quality assurance, research, and service improvement	Legitimate Interests; Legal Obligation

Who we share your data with

We share your personal data only where there is a lawful basis and legitimate purpose. Recipients include: awarding bodies and academic partners (e.g. Leeds Trinity University, NCC Education, NCFE/JCQ); the Higher Education Statistics Agency (HESA); the Office for Students (OfS); the Department for Education (DfE); the Education and Skills Funding Agency (ESFA); HMRC; the Student Loans Company; local authorities (where safeguarding or statutory obligations apply); and other statutory bodies as required by law. We do not sell your personal data.

How long we keep your data

We retain your personal data in accordance with our Data Retention Schedule (Section 6.11 of the Data Protection and Retention Policy). For example, student academic records are retained for a minimum of 6 years after programme end (permanently for degree-level qualifications). Attendance and engagement records are retained for 3 years after programme end.

Your rights

Under UK GDPR you have the right to: access your personal data (Subject Access Request); request correction of inaccurate data; request erasure of your data in certain circumstances; restrict or object to processing; and request data portability where processing is based on consent or contract. To exercise any of these rights, please contact us at dataprotection@wic.ac.uk or use the Data Subject Rights Request Form (Appendix 3).

Complaints

If you have a concern about how we handle your personal data, you may raise this through our Complaints Procedure (Policy 4.06) or contact the ICO directly at www.ico.org.uk or 0303 123 1113.

Changes to this notice

This privacy notice is reviewed annually and updated whenever our processing activities change materially. The current version is available on our website at www.wic.ac.uk/about/wic-policies.

7.7 Appendix 7: Privacy Notice – Staff

Waltham International College – Staff Privacy Notice

This privacy notice explains how Waltham International College (WIC) collects and uses the personal data of its employees, workers, contractors, governors, and volunteers. It is issued in accordance with Articles 13 and 14 of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This notice supplements your contract of employment and any applicable collective agreements.

Who we are

Waltham International College Limited is registered as a data controller with the ICO. You can contact our Data Protection Officer at dataprotection@wic.ac.uk.

What personal data we collect

Category	Examples
Identity and contact information	Name, address, date of birth, National Insurance number, contact details, next of kin
Employment records	Contract of employment, job title, start date, salary, working hours, annual leave, employment history
Payroll and financial data	Bank account details, tax code, pension information, expense claims, salary sacrifice arrangements
Performance and development records	Appraisal records, professional development, training records, disciplinary and grievance records
Recruitment records	Application forms, interview notes, references, right to work documentation
DBS disclosure records	Outcome of Disclosure and Barring Service checks
Absence and health records	Sickness absence records, fit notes, occupational health referrals, adjustments for disability
Equality and diversity data	Ethnicity, gender, disability status, age (for monitoring and statutory reporting)
CCTV and access control data	Images and access records on College premises
IT usage data	College network and device usage logs

Special category data

We process special category data including health information (for sickness absence management and occupational health purposes), disability data (for reasonable adjustments), and equality monitoring data. We do so on the basis of employment law obligations (Article 9(2)(b) UK GDPR; Schedule 1 DPA 2018) or explicit consent where required.

Why we collect your data and our lawful basis

Purpose	Lawful basis (Article 6 UK GDPR)
Managing your employment and contract	Contract; Legal Obligation
Payroll processing and pension administration	Contract; Legal Obligation
Tax and National Insurance reporting to HMRC	Legal Obligation
Managing performance, development, and appraisal	Contract; Legitimate Interests
Managing sickness absence and occupational health	Legal Obligation; Substantial Public Interest
Statutory returns (e.g. HESA staff data, DfE workforce census)	Legal Obligation
DBS checking and safeguarding compliance	Legal Obligation
Right to work verification	Legal Obligation
Equality and diversity monitoring	Legal Obligation; Substantial Public Interest
Campus security (CCTV and access control)	Legitimate Interests
Disciplinary, grievance, and complaints investigations	Contract; Legal Obligation; Legitimate Interests
Emergency contact use (next of kin)	Vital Interests

Who we share your data with

We share your personal data only where there is a lawful basis. Recipients include: HMRC (payroll and tax); pension providers; the Department for Education (workforce census); HESA (staff data return); Disclosure and Barring Service; occupational health providers; HR advisors and legal counsel; and statutory authorities where required by law (e.g. regulatory investigations, law enforcement). We do not sell your personal data.

How long we keep your data

Retention periods are set out in the Data Retention Schedule (Section 6.11 of the Data Protection and Retention Policy). For example, staff employment records are retained for 7 years after employment ends. DBS disclosure records are retained for 6 months (outcome only retained thereafter). Recruitment records for unsuccessful applicants are retained for 12 months from the recruitment decision.

Your rights

Under UK GDPR you have the right to: access your personal data (Subject Access Request); request correction of inaccurate data; request erasure in certain circumstances; restrict or object to processing; and request data portability where processing is based on consent or contract. To exercise any of these rights, contact dataprotection@wic.ac.uk or use the Data Subject Rights Request Form (Appendix 3).

Automated decision-making

WIC does not subject staff to solely automated decisions that produce significant legal or similarly significant effects.

Complaints

If you have a concern about how we handle your personal data, you may raise this via our internal grievance procedure or contact the ICO directly at www.ico.org.uk or 0303 123 1113.

Changes to this notice

This notice is reviewed annually. The current version is available on the staff intranet and from the Data Protection Officer on request.