OXFORD International College

A NORD ANGLIA EDUCATION SCHOOL

DATA PROTECTION POLICY

POLICY INTENDED FOR:	Students and Parents
CATEGORY:	Data Protection
POLICY IMPLEMENTED BY:	Principal and Data Protection Officer
REVIEWED BY:	NAE Global Compliance Manager
REVIEW DATE:	June 2025
FUTURE REVIEW:	June 2026

The Three Pillars

The three pillars of Oxford International College (OIC) are:

- Academic Excellence
- Personal Development
- Career and University Pathways

CONTENTS

INTRODUCTION

This policy applies to the collection, use, disclosure and destruction of Personal Data by the Oxford International College (OIC) and should be adhered to by all Staff. This policy sets the standards of data privacy compliance across OIC.

Any questions or concerns about the operation of this policy should be referred to the OIC Data Protection Officer (DPO) - dpo@oxcoll.com.

Data privacy is important to OIC not only because it is a legal requirement but also it is the right thing to do to protect staff, families, students and our stakeholders – please refer to Nord Anglia Education's (NAE) Code of Conduct and Ethics.

Failure to protect personal data may put these individuals at risk of serious harm, damage our reputation and create a loss of trust. Furthermore, it may lead to civil or criminal penalties to our staff or business and will cause increase in costs to our operations

SCOPE, AUDIENCE AND DEFINITIONS

This policy and the other policies referred to herein form the overall Data Privacy Policy which supersedes all previous OIC data protection / privacy policies. This policy is for all staff.

In this policy, when referring to policy implementation: "must" means required, "should" means strongly recommended and "may" means optional.

Definitions of data privacy terminology is set out in Appendix 1.

DATA PRIVACY PRINCIPLES

Anyone processing Personal Data must comply with eight principles of compliant processing of Personal Data. These are that Personal Data must be:

- processed fairly and lawfully and in a transparent manner ('lawfulness, fairness & transparency');
- processed for specified, explicit and legitimate purposes ('purpose limitation');
- adequate, relevant and limited to what is necessary for the purpose ('data minimisation');
- accurate and where necessary kept up to date ('accuracy');
- kept in a form which permits identification of the Data Subject for no longer than necessary for the purpose ('storage minimisation');
- kept secure using appropriate technical and organisational means ('security, integrity and confidentiality');
- not transferred to another country without appropriate safeguards ('transfer limitation'); and
- allow Data Subjects to exercise certain rights ('data subject's rights and requests')

We are responsible for and must be able to demonstrate compliance with the above data privacy principles.

RESPONSIBILITIES & KEY CONTACTS

Everyone is responsible for upholding this policy and ensuring compliance with this policy.

OIC's Group Data Protection Officer is responsible for keeping this policy up to date, liaising with regulators, and providing assurance to the NAE Central Compliance Team on compliance at OIC.

The OIC DPO is responsible for day-to-day support to staff on how to implement this policy and maintaining data privacy related documentation (e.g. current/past data privacy notices, data breach register and record of processing activities). These registers must be shared with the Central Compliance Team as required.

The Principal is accountable for data protection in OIC and is responsible for appointing the OIC Data Protection Officer and ensuring that they have sufficient time and resources to perform their tasks. Principals will update the Central Compliance Team with the relevant appointee's details.

LAWFULNESS, FAIRNESS & TRANSPARENCY

- Personal data must be processed lawfully, fairly and in a transparent manner.
- OIC must only collect, process and share personal data fairly and lawfully and for a specific purpose. Therefore, you need to ensure we have legal grounds for processing personal data. Please see Appendix 2 for further explanation on the various grounds for processing.
- If staff are collecting personal data and are uncertain on what legal grounds is the basis for the processing then please speak to the OIC Data Protection Officer - dpo@oxcoll.com.
- When processing Special Categories of Personal Data (relating to health, political or religious beliefs, ethnicity, etc.), OIC should require explicit consent. If staff are not relying on explicit consent, then they must consult with the OIC Data Protection Officer - dpo@oxcoll.com.
- When relying on Consent OIC must ensure that the Consent Protocol is adhered to as set out in Appendix 3.
- Data Subjects must be provided with a privacy notice / personal information collection statement ("PICS"), please contact the OIC Data Protection Officer to see the latest version. These should include:
    - the identity of the Data Controller(s);
    - purpose for which we are processing their personal data;
    - source of the data and legal grounds for processing;
    - categories of recipients of the personal data;
    - whether their personal data will be transferred internationally and any relevant safeguards;
    - how long we retain personal data for; and
    - what their rights are.

PURPOSE LIMITATION

Privacy notices must be provided to Data Subjects every time OIC collect personal data from them or when OIC first communicates with them. Any revisions should be brought to their attention appropriately.

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be processed in any manner which is incompatible with those purposes.

DATA MINIMISATION

Personal Data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

Staff may only collect Personal Data that they require for their job duties and must not process Personal Data for any reason unrelated to their job duties; do not collect excessive data.

Staff must ensure any Personal Data collected is adequate and relevant for the intended purpose.

Staff must ensure that when Personal Data is no longer needed for a specific purpose, it is deleted or anonymised in accordance with the relevant Data Retention Schedule – Please refer to the Data Retention Policy for further information.

ACCURACY

Personal Data must be accurate and kept up to date. It must be corrected or deleted without delay when inaccurate.

Steps must be taken to check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. Staff must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data in respect of any system, register or other process for which processes Personal Data that they are responsible.

STORAGE MINIMISATION

Personal Data must not be kept longer than is necessary for the purposes for which that data was collected and is processed.

Staff must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate purpose or purposes for which OIC originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

OIC will maintain a data retention schedule and associated procedures to ensure Personal Data is deleted after an appropriate time unless a law requires that data to be kept for a minimum period. This must be regularly reviewed (at a minimum annually).

Each database owner must conduct regular audits and erasures in line with the relevant data retention schedule. System owners must ensure their system can facilitate data retention periods and allow in certain circumstances to hold-off deletion of data.

Staff must take all reasonable steps to destroy or erase from OIC's systems all Personal Data that OIC no longer requires in accordance with all the applicable records retention schedules and policies. This includes requiring third parties to delete the data where applicable. Staff should obtain certification or formal confirmation of the destruction from any third party.

SECURITY, INTEGRITY & CONFIDENTIALITY

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing and against accidental loss, destruction, or damage.

Staff must adhere to the Nord Anglia Education IT Security Policy. IT will ensure that the policy is maintained with appropriate safeguards proportionate to our size, scope and business, the amount of Personal Data that OIC own or maintain and identified risks (including use of encryption and pseudonymisation, where applicable). OIC will regularly evaluate and test the effectiveness of those safeguards to ensure security of its processing of Personal Data.

Staff are responsible for protecting the Personal Data we hold. Staff must implement reasonable and appropriate security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data.

Staff must follow all procedures and technologies OIC put in place to maintain security of all Personal Data from the point of collection to the point of destruction.

Staff may only transfer Personal Data to a third-party service provider who agrees to comply with the required policies and procedures and who have and/or agree to put in place adequate measures (e.g.

appropriate data processing agreement or clauses), as requested.

Staff must maintain data security by protecting the confidentiality, integrity, and availability of Personal Data, defined as follows:

- Confidentiality: only people who have a need to know and are authorised to use the Personal Data can access it on a least privilege basis;
- Integrity: Personal Data is accurate and suitable for the purpose for which it is processed; and
- Availability: authorised users can access the Personal Data when they need it for authorised purposes.

Staff must not attempt to circumvent the administrative, physical and technical safeguards implemented by OIC.

REPORTING A PERSONAL DATA BREACH

It is essential that any suspected or actual breach is reported to the OIC Data Protection Officer **immediately** - dpo@oxcoll.com.

OIC have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where it is legally required to do so. This will only be done with the prior authorisation as set out in the Data Breach Policy.

TRANSFER LIMITATION

An international data transfer of Personal Data occurs when that data is transmitted, sent, viewed, or accessed in or to a different country other than the UK.

Staff must adhere to the international data transfer restrictions and compliance requirements for international data transfers. If staff are unsure of the rules, then you should consult with the OIC Data Protection Officer - dpo@oxcoll.com and Legal Team to assess the requirements and advise.

Staff must comply with any international data transfer procedures issued by OIC.

The UK has restrictions to transfer Personal Data outside of the UK and EEA, except to countries which have been deemed adequate by the UK's Information Commissioner's Office – a list can be found on their website.

Staff must also ensure that the transfer is necessary, and you have assessed the adequacy of the protections to where you are transferring the data and ensure that there are the appropriate contractual protections in place (using the International Data Transfer Agreement ("IDTA") in your data processing / supplier contract/agreement). If you need support in these please reach out to the OIC Data Protection Officer - dpo@oxcoll.com.

DATA SUBJECT'S RIGHTS & REQUESTS

A Data Subject has rights when it comes to how we handle their Personal Data. These may include rights to:

- withdraw consent to processing at any time;
- receive certain information about our processing activities;
- request access to their Personal Data that we hold;
- prevent our use of their Personal Data for direct marketing purposes;
- ask to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or rectify inaccurate data or to complete incomplete data;
- restrict processing in specific circumstances;

- challenge processing which has been justified on the basis of legitimate interest or in the public interest;
- request a copy of an agreement which covers the international transfer of Personal Data;
- object to any automated decision making;
- be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- make a complaint to the supervisory authority; and
- in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

Staff must verify the identity of the individual requesting data under any of the rights above. Do not allow third parties to persuade you to disclose Personal Data without proper authorisation.

Staff must immediately forward any Data Subject request you receive to the OIC Data Protection Officer - dpo@oxcoll.com.

ACCOUNTABILITY

OIC must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles.

OIC must have adequate resources and controls in place to ensure and to document data privacy compliance, including:

- appointing a suitable (and qualified) Data Protection Officer;
- implementing Privacy by Design and completing Data Protection Impact Assessment ("DPIA") where processing presents a high risk to the rights and freedoms of Data Subjects;
- integrating data privacy into other internal documents/policies and procedures;
- regularly training and improving awareness of data privacy – using NAE training resources and completing any and all mandatory training; and
- regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance.

RECORD KEEPING

OIC must keep an accurate record of all our data processing activities. The DPO will maintain the data processing register to record this.

OIC must keep and maintain accurate records reflecting our processing including records of Data Subject consents and the procedures for obtaining consents.

Any processing registers should include, at a minimum, clear description of:

- the Personal Data types;
- the Data Subject types;
- the processing activities;
- the processing purposes;
- third-party recipients of the Personal Data;
- Personal Data storage locations;
- Personal Data transfers;

- Personal Data retention periods; and
- security measures in place.

Staff should create data maps which should include the above details with appropriate data flows.

TRAINING AND AUDIT

OIC requires all OIC staff to undergone adequate training to enable them to comply with data privacy laws.

OIC must regularly test our systems and processes to assess compliance.

Staff must undertake all mandatory data privacy and cyber security training and ensure all teams maintain good awareness of data privacy and cyber security.

Staff must regularly review all systems and processes under their control to ensure they comply with this Data Privacy Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data. They should refer to the OIC Data Protection Officer for further information if necessary.

PRIVACY BY DESIGN & DEFAULT AND DATA PROTECTION IMPACT ASSESSMENT

OIC is required to implement Privacy by Design as a default when processing Personal Data by implementing appropriate technical and organisational measures (e.g. pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

Staff must assess what Privacy by Design measures can be implemented on all programmes, systems or processes that process Personal Data by taking into account the following:

- The state of the art.
- The cost of implementation
- The nature, scope, context and purposes of processing.
- The risks on the rights and freedoms of Data Subject posed by the processing (with due regard for the impact and likelihood of the risk).

Staff must conduct a Data Protection Impact Assessment ("DPIA") when implementing a major system or business change programme involving the processing of Personal Data including:

- Use of new technology or changing technologies.
- Automated processing including profiling, biometric technologies or automated decision making.
- Large-scale processing of Special Categories or Personal Data or Criminal Convictions Data or children's data.
- Large-scale, systematic monitoring of a publicly accessible area.

You should use the OIC DPIA template to complete your assessment and it must be carried out prior to the implementation of the new system and/or change. These must be submitted to the OIC Data Protection Officer for review prior to completion.

AUTOMATED PROCESSING AND AUTOMATED DECISION-MAKING

Generally, this activity is prohibited when a decision based on the automated process has a legal or similar significant effect on an individual unless the Data Subject has consented, the processing is authorised by law or is necessary for the performance of or entering into a contract.

This type of processing includes the use of AI (artificial intelligence) and is automatically considered a

high-risk form of processing. This means that staff must ensure that a Data Privacy Impact Assessment is carried out prior to this processing taking place.

Special Categories of Personal Data or Criminal Convictions Data may only be processed in this way with explicit consent, and only where there is a substantial public interest (e.g. fraud prevention).

If you are planning on incorporating any automated processing or automated decision-making, Staff must contact the OIC Data Protection Officer, who should inform the Central Compliance Team.

DIRECT MARKETING

OIC is subject to certain rules and regulations when marketing to current and prospective families particularly where that marketing is done electronically.

Consent is required for electronic direct marketing (e.g., by email, text or automated call).

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from the other information. Staff should keep any electronic 'opt-out' mechanism simple.

OIC must honour objections to direct marketing promptly and ensure the Data Subject is placed on its suppression list to ensure it respects their marketing preferences in the future.

The Marketing and Admissions team is responsible for ensuring their procedures adhere to these rules.

SHARING PERSONAL DATA

OIC cannot share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

Staff may only share Personal Data with another employee, agent, or representative of NAE or OIC if the recipient has a job-related need to know the information.

Staff may only share Persona Data OIC holds with a third party, such as our service provider, if:

- they need to know the information for the purposes of providing the contracted services;
- sharing the Personal Data complies with our privacy notices provided to the Data Subject and, if relevant, the Data Subject's consent has been obtained;
- the third-party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- the transfer complies with any applicable cross-border transfer restrictions; and
- a fully executed contract containing the necessary data privacy clauses (as contained in NAE's data processing templates) has been obtained.

OIC may receive requests for Personal Data from law enforcement agencies, regulators, local authorities or other public bodies, and we may receive requests as part of civil litigation (e.g. family disputes). OIC must verify that the sharing is lawful and ensure that we comply with local legal requirements in sharing that data – please speak to OIC's Data Protection Officer or the Legal Team. In these circumstances, OIC are unlikely to be able to give notice to individuals of the data sharing and may be barred from doing so. Where possible, notice of these requests must be provided to the Central Compliance Team.

OIC may be requested to provide data based on a public interest, in which case, OIC must assess whether there is a genuine public interest balancing with individual rights. The OIC Data Protection Officer is responsible for carrying out this assessment. These decisions must be recorded in writing and prior

notification must be provided to the Central Compliance Team.

FURTHER INFORMATION

For further information about Data Protection and Privacy at OIC please speak with OIC Data Protection Officer.

dpo@oxcoll.com

Oxford International College

1 London Place

OX4 1BD

APPENDIX 1 - DEFINITIONS

Automated Decision-Making: when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual.

Automated Process: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Consent: agreement which must be freely given, specific, informed and be unambiguous indication of the Data Subject's wishes by which they, by a statement or a clear positive action, signify agreement to the processing of Personal Data relating to them.

Controllers: the person or organisation that determines when, why and how to process Personal Data It is responsible for establishing practices and policies in line with relevant legislation. We are the Controller of all Personal Data relating to our staff, and Personal Data used in our business for our won commercial purposes.

Criminal Convictions Data: personal data relating to criminal convictions and offences, including personal data relating to criminal allegations and proceedings.

Data Privacy Champion: a person designated to champion data privacy in a Business Unit / School fulfilling a similar role to a Data Protection Officer while not appointed under a specific data privacy law with the same restrictions.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activities. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the processing of Personal Data.

Data Protection Officer: either of the following:

- The person appointed in specific circumstances under data privacy law (e.g., GDPR); or
- Where a mandatory Data Protection Officer has not been appointed, a data privacy manager or other voluntary appointment of a Data Protection Officer or Data Privacy Champion.

Data Subject: a living, identified, or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

EEA: European Economic Area which includes all EU countries and also Iceland, Liechtenstein and Norway

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data along or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and pseudonymised Personal Data but excludes anonymous data that has had the identity of an individual permanently removed. Personal data can be factual or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss or unauthorised access, disclosure or acquisition of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the relevant data privacy laws (e.g. GDPR, PDPA, PIPL, etc) to any new system / data processing / database prior to implementation.

Privacy notice: separate notices setting out information that may be provided to Data Subjects when NAE collects information about them. These notices may take the form of:

- general privacy statement applicable to a specific group of individuals (e.g. employee privacy notice or website privacy notice); or
- standalone, onetime privacy statement covering processing related to a specific purpose.

Processing or process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties or within NAE.

Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure.

Special Categories of Personal Data / Special Category Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

APPENDIX 2 - GROUNDS FOR PROCESSING

Use of Personal Data must be justified under one legal basis and we are required to set out the legal basis in our privacy notices. Please note there are different grounds for general Personal Data, Special Categories of Personal Data and Criminal Convictions Data.

Please note that these are general Grounds for processing and can differ between jurisdictions – therefore speak to the OIC Data Protection Officer.

General

Contract performance: where the Personal Data is necessary to enter into or perform our contract with the Data Subject.

Legal obligation: where we need to use Personal Data to comply with our legal obligations.

Legitimate interests: where we use Person Data to achieve a legitimate interest and our reasons for using it outweigh any prejudice to the Data Subject data privacy rights. Note that to rely on this we will need to document our assessment. Reach out the OIC Data Protection Officer, if you need assistance.

Legal claims: where Personal Data is necessary for us to defend, prosecute or make a claim against Data Subjects, us or a third party.

Public Interest/Task: process Personal Data in the exercise of official authority or to perform a specific task in the public interest that is set out in law. For example, at OIC this could be tasks that a public school authority would undertake which OIC is obliged to also perform.

Consent: where a Data Subject has consented to the processing of their Personal Data for one or more specified purposes.

Vital interest: where we need to process Personal Data in an emergency to protect someone's life and they are incapable of consenting.

Special Categories of Personal Data

Employment, social security and social protection: where processing is necessary for the obligations in employment, social security and social protection law.

Vital Interest: Processing is necessary to protect the vital interests of the Data Subject or of another, where the Data Subject is physically or legally incapable of consenting.

Legal claims: Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

Substantial public interest: Processing is necessary for reasons of substantial public interest, on the basis

of a local law.

Health or Social care: to assess Data Subjects working capacity, assist in making medical diagnoses, or provision of health/social care and treatment. Social care includes social work, personal care and social support services. Includes school nurses, speech language therapists, child psychologist, etc.

Made public by the Data Subject: where the Data Subject has manifestly made public the Personal Data. E.g. a Parent is a member of a national Parliament for a specific political party ('political beliefs').

Public Health: processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health.

Explicit consent: Data Subject has given explicit consent to the processing of their Personal Data for one or more specified purposes.

Criminal Convictions Data

Processing is only allowed under the control of official authority or when the processing is authorised by local laws. Please speak to the OIC DPO to understand when we can process Criminal Convictions Data.

APPENDIX 3 - CONSENT PROTOCOL

- A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly by a statement or positive action to the Processing.
- Consent requires affirmative action, so silence, pre-ticked boxes or activity are unlikely to be sufficient.
- If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.
- A Data Subject must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured.
- Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which as not disclosed when the Data Subject first consented.
- You must evidence Consent captured and keep records of all Consents – you need to design your processes to enable us to capture and use evidence of Consent as and when necessary