



**OXFORD**  
**SIXTH FORM COLLEGE**

Data  
Protection  
Policy

**Revised: July 2021**

**Review date: July 2022**

This policy should be read in conjunction with the OxSFC COVID-19 policy that overrides the guidelines/procedures in this policy, where appropriate. The guiding principle will always be to maintain the health and safety of all stakeholders.

## **RECRUITMENT, STAFF AND STUDENT DATA PROTECTION POLICY**

### **Scope**

This policy applies to the personal information of job applicants, current and former staff, including employees, workers, volunteers and contractors (collectively referred to as "**staff**" for the purposes of this policy). It also applies to all students studying at Oxford Sixth Form College.

Staff and students should refer to the College's privacy notices, Appendix B and in the staff handbook, where appropriate, to its other relevant policies including in relation to the use of internet, email and communications, social media and data retention, which contain further information regarding the protection of personal information in those contexts.

We will review and update this policy in accordance with our data protection obligations. It does not form part of any employee's contract of employment and we may amend, update or supplement it from time to time.

You must read and understand this policy because it gives important information about:

- the data protection principles with which the College must comply;
- your data protection obligations;
- what is meant by personal information (or data) and sensitive personal information (or data);
- how we gather, use and (ultimately) delete personal information and sensitive personal information in accordance with the data protection principles;
- where more detailed privacy information can be found, e.g., about the personal information we gather and use about you, how it is used, stored and transferred, for what purposes, the steps taken to keep that information secure and for how long it is kept;
- your rights and obligations in relation to data protection; and
- the consequences of failure to comply with this policy.

### **Introduction**

The College obtains, keeps and uses personal information (also referred to as data) about students, job applicants and about current and former employees, workers, contractors, volunteers and apprentices

for a number specific lawful purposes, as set out in the College's Staff Privacy Notice.

We also obtain, keep, and use personal information about students, their families, governors, alumni and suppliers of the College. The detail relating to how we collect and process that information is set out within separate privacy notices such as the Parent Privacy Notice and Student Privacy Notice which can be found in Appendix B, on the College's website and within the staff handbook.

This policy sets out how we comply with our data protection obligations and seek to protect personal information relating to our students and workforce. Its purpose is also to ensure that students and staff understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their studies or work.

The Data Protection Officer is responsible for data protection compliance within the College. If you have any questions or comments about the content of this policy or if you need further information, you should contact The Data Compliance Administrator - Marc Lewis by calling 01865 793333 or emailing [marc.lewis@oxfordsixthformcollege.com](mailto:marc.lewis@oxfordsixthformcollege.com).

## **Definitions**

The following definitions shall apply to this policy:

**"criminal records information"** means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures;

**"data breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;

**"data subject"** means the individual to whom the personal information relates;

**"personal information"** (sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;

**"processing information"** means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;

**"pseudonymised"** means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to

ensure that the personal information cannot be attributed to an identifiable individual; and

**"sensitive personal information"** (sometimes known as 'special categories of personal data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

### **Data protection principles**

The College will comply with the following data protection principles when processing personal information:

- we will process personal information lawfully, fairly and in a transparent manner;
- we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;
- we will only process the personal information that is adequate, relevant and necessary for the relevant purposes;
- we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay;
- we will keep personal information for no longer than is necessary for the purposes for which the information is processed; and
- we will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

### **Basis for processing personal information**

In relation to any processing activity we will, before the processing starts for the first time, and then regularly while it continues:

- review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, i.e.:
  - o that the data subject has consented to the processing;
  - o that the processing is necessary for the performance of a contract to which the data subject is party or in order to

take steps at the request of the data subject prior to entering into a contract;

- o that the processing is necessary for compliance with a legal obligation to which the College is subject;
  - o that the processing is necessary for the protection of the vital interests of the data subject or another natural person;
  - o that the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority; or
  - o that the processing is necessary for the purposes of legitimate interests of the College or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject.
- except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);
  - document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;
  - include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);
  - where sensitive personal information is processed, also identify a lawful special condition for processing that information (see '**Sensitive Personal Information**' section below), and document it; and
  - where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

When determining whether the College's legitimate interests are the most appropriate basis for lawful processing, we will:

- conduct a legitimate interest's assessment (LIA) and keep a record of it, to ensure that we can justify our decision;
- if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);
- keep the LIA under review, and repeat it if circumstances change; and

- include information about our legitimate interests in our relevant privacy notice(s).

### **Sensitive personal information**

The College may from time to time need to process sensitive personal information. We will only process sensitive personal information if:

- we have a lawful basis for doing so as set out above, e.g., it is necessary for the performance of the employment contract, to comply with the College's legal obligations or for the purposes of the College's legitimate interests; and
- one of the special conditions for processing sensitive personal information applies, e.g.:
  - the data subject has given explicit consent;
  - the processing is necessary for the purposes of exercising the employment law rights or obligations of the College or the data subject;
  - the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;
  - processing relates to personal data which is manifestly made public by the data subject;
  - the processing is necessary for the establishment, exercise or defence of legal claims; or
  - the processing is necessary for reasons of substantial public interest.

Before processing any sensitive personal information, staff must notify The Data Protection Officer of the proposed processing, in order that they may assess whether the processing complies with the criteria noted above.

Sensitive personal information will not be processed until:

- the assessment referred to above has taken place; and
- the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

The College's privacy notices set out the types of sensitive personal information that the College processes, what it is used for and the lawful basis for the processing.

### **Criminal Records Information**

Criminal records information will be processed in accordance with the College's Safer Recruitment Policy.

### **Data Protection Impact Assessments (DPIA)**

Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where the College is planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:

- whether the processing is necessary and proportionate in relation to its purpose;
- the risks to individuals; and
- what measures can be put in place to address those risks and protect personal information.

Before any new form of technology is introduced, the manager responsible should contact The Data Protection Officer in order that they can consider whether a DPIA should be carried out.

### **Documentation and records**

We will keep written records of processing activities which are high risk, i.e., which may result in a risk to individuals' rights and freedoms or involve sensitive personal information or criminal records information, including:

- the purposes of the processing;
- a description of the categories of individuals and categories of personal data;
- categories of recipients of personal data;
- where possible, retention schedules; and
- where possible, a description of technical and organisational security measures.

If we process sensitive personal information or criminal records information, we will keep written records of:

- the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;
- the lawful basis for our processing; and
- whether we retain and erase the personal information in accordance with our policy document and, if not, the reasons for not following our policy.

We will conduct regular reviews of the personal information we process and update our documentation accordingly.

### **Privacy notices**

The College will issue privacy notices on the College website from time to time, informing you about the personal information that we collect and hold relating to you, as well as our parents, students, alumni, and suppliers, how you can expect your personal information to be used and for what purposes.

We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.

It is important that you read and comply with the College's privacy notices.

### **Individual rights**

You have a number of rights in relation to your personal information which are set out within the Staff Privacy Notice. If you wish to exercise any of these rights, please contact The Data Protection Officer.

### **Individual obligations**

Individuals are responsible for helping the College keep their personal information up to date. You should let the Vice Principal know if the information you have provided to the College changes, for example if you move to a new house or change details of the bank or building society account to which you are paid.

You may have access to the personal information of other members of staff, students, parents, suppliers, contractors and governors of the College in the course of your employment or engagement. If so, the College expects you to help meet its data protection obligations to those individuals. For example, you should be aware that they also enjoy the rights set out above.

If you have access to personal information, you must:

- only access the personal information that you have authority to access, and only for authorised purposes;
- only allow other staff to access personal information if they have appropriate authorisation;

- only allow individuals who are not College staff to access personal information if you have specific authority to do so from the Data Protection Officer;
- keep personal information secure (e.g., by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in the College's Use of Telephone, E-mail Systems and Internet Policy;
- not remove personal information, or devices containing personal information (or which can be used to access it), from the College's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and
- not store personal information on local drives or on personal devices.

You should contact the Data Protection Officer if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

- processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the conditions set out above under the heading '**Sensitive Personal Information**' being met;
- any data breach as set out under the heading '**Data Breaches**' below;
- access to personal information without the proper authorisation;
- personal information not kept or deleted securely;
- removal of personal information, or devices containing personal information (or which can be used to access it), from the College's premises without appropriate security measures being in place; or
- any other breach of this Policy or of any of the data protection principles set out under the heading '**Data Protection Principles**' above.

Failure to comply with the above obligations could result in disciplinary action being taken.

### **Information security**

The College will use appropriate technical and organisational measures in accordance with the College's policies to keep personal information

secure, and in particular, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

These may include:

- making sure that, where possible, personal information is pseudonymised or encrypted;
- ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Where the College uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:

- the organisation may act only on the written instructions of the College;
- those processing the data are subject to a duty of confidence;
- appropriate measures are taken to ensure the security of processing;
- sub-contractors are only engaged with the prior consent of the College and under a written contract;
- the organisation will assist the College in providing subject access and allowing individuals to exercise their rights under the GDPR;
- the organisation will assist the College in meeting its GDPR obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;
- the organisation will delete or return all personal information to the College as requested at the end of the contract; and
- the organisation will submit to audits and inspections, provide the College with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the College immediately if it is asked to do something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the Data Protection Officer.

### **Storage and retention of personal information (Appendix A)**

Personal information (and sensitive personal information) will be kept securely in accordance with the College's Data Protection Policy.

Personal information (and sensitive personal information) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Staff should follow the College's records retention policy, which sets out the relevant retention period, or the criteria that should be used to determine the retention period. Where there is any uncertainty, staff should consult the Data Protection Officer .

Personal information (and sensitive personal information) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely. We may retain personal data for archiving purposes where it is necessary to do so in the public interest, for scientific or historical research purposes or statistical purposes subject to appropriate safeguards being put in place to protect the rights and freedoms of the data subject.

### **Data breaches**

A data breach may take many different forms, for example:

- loss or theft of data or equipment on which personal information is stored;
- unauthorised access to or use of personal information either by a member of staff or third party;
- loss of data resulting from an equipment or systems (including hardware and software) failure;
- human error, such as accidental deletion or alteration of data;
- unforeseen circumstances, such as a fire or flood;
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
- 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

If you become aware of a data breach, you must follow the Data Breach Policy and Procedure and you must report it to the Data Protection Officer as soon as possible. Failure to comply with this obligation could result in disciplinary action being taken.

The College will:

- make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and
- notify the affected individuals, if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

### **International transfers**

In most cases the College will not transfer personal information outside the European Economic Area (EEA), which comprises the countries in the European Union and Iceland, Liechtenstein and Norway. If staff wish to transfer personal information outside the EEA they must consult with the Data Protection Officer before doing so. The Data Protection Officer will only permit the transfer to happen on the basis that either; (i) the country, territory or organisation is designated as having an adequate level of protection or (ii) the organisation receiving the information has provided adequate safeguards by way of standard data protection clauses or by compliance with an approved code of conduct.

### **Training**

The College will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

### **Consequences of failing to comply**

The College takes compliance with this policy very seriously. Failure to comply with the policy:

- puts at risk the individuals whose personal information is being processed;
- carries the risk of significant civil and criminal sanctions for the individual and the College; and

- may, in some circumstances, amount to a criminal offence by the individual.

Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the Data Protection Officer.

## Appendix A

<b>Data Protection - Disposing of Records (Appendix to Data Protection Policy)</b>	
<b>Agreements and related correspondence Periods</b>	<b>Retention</b>
Major agreements of historical significance	permanently
Contracts with customers	6 years after expiry
Contracts with suppliers	6 years after expiry
Contracts with agents	6 years after expiry
Licensing agreements	6 years after expiry
Rental and hire purchase agreements	6 years after expiry
Indemnities and guarantees	6 years after expiry
Other agreements/contracts	6 years after expiry
<b>Property documents</b>	
Deeds of title	permanently or until delivered to a purchaser on disposal
Leases	12 years after lease has terminated and all terminal queries (e.g., dilapidations) settled
Agreements with architects, builders, etc.	6 years after completion of the contract
<b>Accounting records</b>	
Complying with Companies Acts 1948, 1967 and 1976 at least 6 years (3 years if private company)	

Periodic internal financial reports, e.g., to Board file copies for 5 years. Taxation returns and records permanently.	
<b>Banking Records, including GIRO</b>	
Cheques, bills of exchange and other negotiable instruments	6 years
Bank statements & instructions to banks	6 years
Patent and trade mark records	Permanently
Reports and opinions	10 years
<b>Personnel Records</b>	
Staff personal records	6 years after employment ceases
Personal records of company's senior executives	6 years after employment ceases
Applications for jobs - unsuccessful	up to 1 year
Payrolls	6 years from the financial year end in which payment made
Salary registers	6 years from the financial year end in which payment made
Salary revision schedules	6 years from the financial year end in which payment made
Expenses accounts	6 years from the financial year end in which payment made
Tax returns	6 years after lodgement date
Staff Group minutes	Permanently
Records of hours worked	3 years beginning on the day upon which the pay reference period immediately following that to which they relate ends
Salary records (including overtime details)	6 years from the financial year end in which payments made
Medical records	12 years
Training records	6 years after employment ceases
Accident books	3 years from date of report
<b>Pension Records</b>	
All trust deeds and rules	permanently
Trustees' minute book	permanently
Fund annual accounts and Inland Revenue approvals	permanently
Investment records	permanently
Actuarial valuation records	permanently
Contribution records	permanently
Records of ex-pensioners	6 years after cessation of benefit
Pension scheme investment policies	12 years after final cessation of any benefit payable under the policy

Group health policies	12 years after final cessation of benefit
<b>Insurance</b>	
Group personal accident policies	12 years after final cessation of benefit
Public liability policies	permanently
Product liability policies	permanently
Employer's liability policies	permanently
Other policies	3 years after lapse
Claims correspondence	3 years after settlement
Accident reports and related correspondence	3 years after settlement
Insurance schedules	10 years
Medical records	12 years
Other policies	3 years after lapse
Claims correspondence	3 years after settlement
<b>Safeguarding and Child Protection documents</b>	
Child Protection	88 years from the date the first incident was reported
Safeguarding	On the 25 <sup>th</sup> birthday of the student concerned
<b>Parental Permission slips for school trips</b>	Where there has been <b>no</b> major incident Until conclusion of the trip Where there <b>has been</b> a major incident DOB of the student involved + 25 Years Permission slips for all students on the trip need to be retained to show that all rules have been followed for all students.
Any other records created in the course Current year	3 years of contact with the student
<b>Alumni Files</b>	Life of Alumni
<b>Admission Registers</b>	Date of last entry in the register + 6 years
<b>Attendance Registers</b>	Date of register + 3 years
<b>Correspondence Relating to Authorised Absence and Issue</b>	Date of absence + 3 years
<b>Examination Results Public</b>	
School's copies Year of examinations	+ 4 years
Students Copies Uncollected certificates	Returned to the Examination Board or destroyed after 4 years
Exam papers relating to appeals	Kept until any appeal/validation process is

	complete
Examination results of internal exams	Current year + 4 years
<b>Returns made to Central Government (e.g. Census)</b>	Current year + 6 years
<b>Accessibility Strategy</b>	Student DOB + 25 Years
<b>Sponsorship Licence and Related Permissions</b>	The duration of the period covered by the licence
<b>Copies of admission information</b>	If the Migrant is sponsored for one year or longer
<b>For students sponsored under tier 4 PBS</b>	The documents must be kept for one Year or until a compliance Officer has examined and approved them, whichever is the longer period
<b>Reports and correspondence with The Home Office made in relation to a Current student</b>	To the end of the sponsorship + 2 years

Updated: May 2019

## Appendix B

### Privacy Statements

#### CONTACT US

If you have any questions, concerns or would like more information about anything mentioned in our privacy notices, please contact our Data Protection Officer at [marc.lewis@oxfordsixthformcollege.com](mailto:marc.lewis@oxfordsixthformcollege.com)

#### PRIVACY NOTICE FOR JOB APPLICANTS

This privacy notice explains how we collect, store and use personal data about agents. Oxford Sixth Form College is the data controller, and for the purposes of data protection law, this privacy notice applies to Oxford Sixth Form College.

The table below shows the data that we process about applicants, the reasons for processing this data and the lawful bases for processing this data.

The data or type of data we process	The purpose of processing that data	The lawful bases for processing this data
Details that appear on CVs and cover letters such as names, address and date of birth, education/professional qualifications	To assess your suitability for the role you have applied for and for progressing your application	To perform an employment contract with you, in the event you are successful
Interview notes/results from assessments	To assess your suitability for the role you have applied for	Necessary for our legitimate interests (to make recruitment decisions)

The data or type of data we process	The purpose of processing that data	The lawful bases for processing this data
References from former employers	A pre-employment check to assess your suitability for the role you have applied for	Necessary for our legitimate interests (to make recruitment decisions)
Right to work information	To assess your eligibility for the role you have applied for	Compliance with a legal obligation
Pre-employment checks such as criminal record checks	A pre-employment check to assess your suitability for the role you have applied for	Compliance with a legal obligation; to fulfil regulatory checks
Salary, benefits and bonus information	For the purposes of making an offer of employment	To perform an employment contract with you, in the event you are successful
We may also collect data about 'special categories' of sensitive personal information such as your race or ethnicity, religious beliefs, disability, sexual orientation	For equal opportunities monitoring	Compliance with a legal obligation
If we need to make reasonable adjustments as part of the recruitment process	For the purposes of ensuring a fair selection process	Compliance with a legal obligation

Where we have obtained consent to use applicant data, this consent can be withdrawn at any time. We will make this clear when we ask for consent and explain how consent can be withdrawn.

#### **WHEN DO WE SHARE JOB APPLICANT DATA?**

When it is legally necessary, or allowed under data protection law, we may need to share information about you with the organisations listed in the table below, for the listed reasons.

<b>Organisation Name</b>	<b>The Reason for Sharing</b>
Regulatory bodies, such as Ofsted or the British Council	To comply with regulatory inspections
Service providers	For running surveys
Financial organisations	For processing payments
Our auditors	For carrying out legal audits of company accounts
Professional advisers and consultants	To assist us in developing our business
Police forces, courts, tribunals	For dealing with legal issues

In addition, your personal data may be shared internally with other employees who are involved in the recruitment process, employees in HR who have responsibility for recruitment and on-boarding, employees in IT for setting up systems and permissions, and employees in security for access to our premises.

#### **TRANSFERRING JOB APPLICANT DATA INTERNATIONALLY**

Your personal information may be stored and processed outside of the country where it is collected, including outside of the European economic area.

We will only transfer personal data to a country or territory outside the European economic area:

- where the transfer is to a place that is regarded by the European commission as providing adequate protection for your personal information; or
- where we have put in place appropriate safeguards to ensure that your personal information is protected (for example where both parties involved in the transfer have signed standard data protection clauses adopted by the European commission); or
- the above does not apply but we are still legally permitted to do so, for example if the transfer is necessary for the establishment, exercise or defence of legal claims.

You can request further detail about the safeguards that we have in place in respect of transfers of personal information outside of the EEA and where applicable a copy of the standard data protection clauses that we have in place, by contacting us at [marc.lewis@oxfordsixthformcollege.com](mailto:marc.lewis@oxfordsixthformcollege.com)

#### **STORING JOB APPLICANT DATA**

We will keep personal information about you while you are an active applicant. We create and maintain files for each applicant. The information contained in these files is kept secure and is only used for purposes directly relevant to your position as an applicant. Once the application process is finished, we will retain this file if your application is successful in accordance with our Staff Privacy Notice, or delete it after 12 months, in accordance with our Data Retention Policy.

**PRIVACY NOTICE FOR EMPLOYEES**

This privacy notice explains how we collect, store and use personal data about employees. Oxford Sixth Form College is the 'data controller' for the purposes of data protection law.

The table below shows the data that we process about employee and agencies, the reasons for processing this data and the lawful bases for processing this data.

The data or type of data we process	The purpose of processing that data	The lawful bases for processing this data
Name, date of birth, gender	To administer our relationship with you	Fulfilment of a contract with you
Telephone number, email address, postal address	To administer our relationship with you	Necessary for our legitimate interests (to manage the workforce)
Next of kin and emergency contact numbers	To contact family or close friends in the event of an emergency	To protect your vital interests
Bank account details, payroll records, National Insurance number, tax status information, salary, annual leave, pension & benefits information, marital status	To process salary payments	Fulfilment of a contract with you
	To provide tax and related data to HMRC	Compliance with a legal obligation

The data or type of data we process	The purpose of processing that data	The lawful bases for processing this data
Recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process	To administer the business	Compliance with a legal obligation
	To facilitate safe recruitment, as part of our safeguarding obligations towards students	Necessary for our legitimate interests (recruitment)
Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships	To administer our business	Necessary for our legitimate interests (to manage the workforce)
Performance information; outcomes of any disciplinary and/or grievance procedures; absence data	To administer our business	Fulfilment of a contract with you
		Necessary for our legitimate interests (to support effective performance management)
Copy of driving licence	To ensure legal, insured use of vehicles	Compliance with a legal obligation
Images	For maintaining security	Compliance with a legal obligation
	For marketing our services	Where you have given us consent
CCTV footage	For security management	Compliance with a legal obligation

The data or type of data we process	The purpose of processing that data	The lawful bases for processing this data
Data about your use of the organisations information and communications systems, including Internet use	To meet our safeguarding obligations	Compliance with a legal obligation
	To administer and protect the business	Necessary for our legitimate interests (to secure our buildings)
Criminal record information	To meet our safeguarding obligations	Compliance with a legal obligation
Medical and disability information	To meet the requirements of our accrediting bodies	Necessary for our legitimate interests (to meet the requirements of accrediting bodies)

Where we have obtained consent to use employee data, this consent can be withdrawn at any time. We will make this clear when we ask for consent and explain how consent can be withdrawn.

#### WHEN DO WE SHARE EMPLOYEE DATA?

When it is legally necessary, or allowed under data protection law, we may need to share information about you with the organisations listed in the table below, for the listed reasons.

Organisation Name	The Reason for Sharing
The Department for Education	To meet our obligations for sharing data with the government

Organisation Name	The Reason for Sharing
The Local Education Authority	To meet our obligations for sharing data with the government
Government departments	To meet our legal obligations on matters such as tax and social security
Regulatory bodies, such as Ofsted or the British Council	To comply with regulatory inspections
Service providers	Such as companies that run surveys for us or provide travel or insurance services or venues that are hosting events for Oxford Sixth Form College including seasonal programmes or conduct criminal record checks
Financial organisations	For processing payments, administering pensions
Our auditors	For carrying out legal audits of company accounts
Police forces, courts, tribunals	For dealing with legal issues
Other education providers	Where we have partnerships
Security providers	For DBS checking services
Other employers	To provide an employment reference on your behalf and where you have given your consent to the prospective employer to contact Oxford Sixth Form College

## **TRANSFERRING EMPLOYEE DATA INTERNATIONALLY**

Your personal information may be stored and processed outside of the country where it is collected, including outside of the European economic area.

We will only transfer personal data to a country or territory outside the European economic area:

- where the transfer is to a place that is regarded by the European commission as providing adequate protection for your personal information; or
- where we have put in place appropriate safeguards to ensure that your personal information is protected (for example where both parties involved in the transfer have signed standard data protection clauses adopted by the European commission); or
- the above does not apply but we are still legally permitted to do so, for example if the transfer is necessary for the establishment, exercise or defence of legal claims.

You can request further detail about the safeguards that we have in place in respect of transfers of personal information outside of the EEA and where applicable a copy of the standard data protection clauses that we have in place, by contacting us at [marc.lewis@oxfordsixthformcollege.com](mailto:marc.lewis@oxfordsixthformcollege.com)

## **STORING EMPLOYEE DATA**

We will keep personal information about you while you are an active employee. We create and maintain records for each member of staff. The information contained in these records is kept secure and is only used for purposes directly relevant to your position as an employee of Oxford Sixth Form College. Once your time as an employee with us has ended, we will retain this file and delete the information in it in accordance with our Data Retention Policy.

## **PRIVACY NOTICE FOR STUDENTS, PARENTS AND GUARDIANS**

This privacy notice explains how we collect, store and use personal data about agents. Oxford Sixth Form College is the data controller, and for the purposes of data protection law, this privacy notice applies to Oxford Sixth Form College.

The table below shows the data that we process about students, the reasons for processing this data and the lawful bases for processing this data. Cells marked with an asterisk (\*) indicate that parent or guardian data may also be processed in the same way, where a student requires parental consent.

The data or type of data we process	The purpose of processing that data	The lawful bases for processing this data
<b>Your name, date of birth, gender, addresses, email addresses and phone numbers. Your relationship to the student.*</b>	To identify you to communicate with you	Fulfilment of a contract with you
		Compliance with a legal obligation
<b>Your nationality, ethnic background, any special educational needs, special requirements or disabilities</b>	To provide appropriate information and assistance for you	Fulfilment of a contract with you
		Compliance with a legal obligation
<b>Next of kin and emergency contact numbers</b>	To contact your family or close friends in the event of an emergency	To protect your vital interests
<b>Your passport, BRP and visa details</b>	To meet government immigration regulations	Compliance with a legal obligation

The data or type of data we process	The purpose of processing that data	The lawful bases for processing this data
<b>Bank account details*</b>	To manage payments and refunds	Fulfilment of a contract with you
		Compliance with a legal obligation
<b>Your educational records and test or exam results from previous schools</b>	To offer you the most appropriate courses	Fulfilment of a contract with you
<b>Your medical information, including medications you take, allergies and dietary requirements</b>	To help you manage your health while you are with us	Fulfilment of a contract with you
		Compliance with a legal obligation
<b>Your educational records and test or exam results from Oxford Sixth Form College</b>	To manage your progress while studying with us	Fulfilment of a contract with you
	To meet government immigration and safeguarding regulations	Fulfilment of a contract with you

The data or type of data we process	The purpose of processing that data	The lawful bases for processing this data
Your attendance records and booking in/out records for school and residence		Compliance with a legal obligation
Details of your welfare such as how you are getting on at Oxford Sixth Form College safeguarding or child protection records and any problems or issues you may have had	To look after your wellbeing and meet government safeguarding regulations	Fulfilment of a contract with you
		Compliance with a legal obligation
Details of any behaviour issues or exclusions	To manage discipline in the College	Necessary for our legitimate interests (to manage college discipline)
Images	For maintaining security	Compliance with a legal obligation
	For marketing our services	Where you have given us consent
CCTV footage*	For security management	Compliance with a legal obligation

The data or type of data we process	The purpose of processing that data	The lawful bases for processing this data
		Necessary for our legitimate interests (to maintain building and personal security)
<b>Data about your use of information and communications systems, including Internet use</b>	To meet our safeguarding obligations	Compliance with a legal obligation
	To administer and protect the College	Necessary for our legitimate interests (to secure our buildings)

Where we have obtained consent to use student data, this consent may be withdrawn at any time. We will make this clear when we ask for consent and explain how consent can be withdrawn.

#### **WHEN DO WE SHARE STUDENT, PARENT OR GUARDIAN DATA?**

When it is legally necessary, or allowed under data protection law, we may need to share information about you with the organisations listed in the table below, for the listed reasons.

Organisation Name	The Reason for Sharing
The Department for Education	To provide data on international students

Organisation Name	The Reason for Sharing
The Local Education Authority	To provide data on international students
Regulatory bodies, such as Ofsted or the British Council	To comply with regulatory inspections
Service providers	For running surveys, providing taxi or excursion services, providing security services
Financial organisations*	For processing payments
Our auditors	For carrying out legal audits of company accounts
Health and social welfare organisations	To manage student wellbeing
Professional advisers and consultants	To assist us in developing our business
Police forces, courts, tribunals*	For dealing with legal issues
Your family and representatives	To share details of your academic progress or to tell them about attendance or behaviour issues

Organisation Name	The Reason for Sharing
Exam Boards	To enter you for exams
UCAS	To enable you to apply to universities in the UK
The Taylor Partnership (TTP)	To provide data on International students to comply with our duties as a Tier 4 sponsor *
Marketing services, such as those offered by Facebook	To identify other students who may be interested in studying with Oxford Sixth Form College. No decisions will be taken about you based on this profiling.
WCBS	To enable our database to be maintained and supported by WCBS
Corbett Engineering Limited, trading as Celcat (CEL)	Limited data when timetabling, held on a web-based platform supplied by CEL
Fresh Student Living	To facilitate student enquiries for those who wish to reside in Between Towns Court accommodation. Personal information may be shared, for example in a safeguarding situation.
REACH Boarding	Database held by REACH boarding and used by students, parents, guardians and staff for the security and wellbeing of the students whilst in boarding.

Organisation Name	The Reason for Sharing
Endsleigh	Insurance purposes

\*If your child is not of British nationality, we have to make sure that your child has the right to study in the UK. This process is managed by The Taylor Partnership (TTP), with whom the College has a legally binding contract regarding management of data. We may provide information about you to UK Visas and Immigration to comply with our duties as a Tier 4 sponsor.

#### **TRANSFERRING STUDENT, PARENT AND GUARDIAN DATA INTERNATIONALLY**

Your personal information may be stored and processed outside of the country where it is collected, including outside of the European economic area.

We will only transfer personal data to a country or territory outside the European economic area:

- where the transfer is to a place that is regarded by the European commission as providing adequate protection for your personal information; or
- where we have put in place appropriate safeguards to ensure that your personal information is protected (for example where both parties involved in the transfer have signed standard data protection clauses adopted by the European commission); or
- the above does not apply but we are still legally permitted to do so, for example if the transfer is necessary for the establishment, exercise or defence of legal claims.

You can request further detail about the safeguards that we have in place in respect of transfers of personal information outside of the EEA and where applicable a copy of the standard data protection clauses that we have in place, by contacting us at [marc.lewis@oxfordsixthformcollege.com](mailto:marc.lewis@oxfordsixthformcollege.com)

#### **STORING STUDENT, PARENT AND GUARDIAN DATA**

We will keep personal information about you while you are an active student. We create and maintain records for each individual student. The information contained in these records is kept secure and is only used for purposes directly relevant to your position as a student with Oxford Sixth Form College. Once your time as a student with us has ended, we will retain these records and delete them in accordance with our Data Retention Policy.

#### **PRIVACY NOTICE FOR AGENTS**

This privacy notice explains how we collect, store and use personal data about agents. Oxford Sixth Form College is the data controller, and for the purposes of data protection law, this privacy notice applies to Oxford Sixth Form College.

The table below shows the data that we process about agents and agencies, the reasons for processing this data and the lawful bases for processing this data.

<b>The data or type of data we process</b>	<b>The purpose of processing that data</b>	<b>The lawful bases for processing this data</b>
Names, address, email addresses, phone numbers	To communicate with you about students you have sent to Oxford Sixth Form College; to ensure you have up-to-date information so you can provide accurate information to potential students	Fulfilment of a contract with you

The data or type of data we process	The purpose of processing that data	The lawful bases for processing this data
Bank account details	To process commission payments	Fulfilment of a contract with you
Joining information, references	To register your agency with Oxford Sixth Form College	Necessary for our legitimate shared interests
Details of students you have sent to us	To administer our business, to manage agreed recruitment targets	Fulfilment of a contract with you
Images	For marketing our services	Where you have given us consent
CCTV footage	For security management if you have visited our schools	Compliance with a legal obligation
		Necessary for our legitimate interests (to maintain building and personal security)
Financial details, bank account information, commission agreements, payment records	To administer our business, to make commission payments	Fulfilment of a contract with you

Where we have obtained consent to use agent data, this consent can be withdrawn at any time. We will make this clear when we ask for consent and explain how consent can be withdrawn.

#### **WHEN DO WE SHARE AGENT DATA?**

When it is legally necessary, or allowed under data protection law, we may need to share information about you with the organisations listed in the table below, for the listed reasons.

<b>Organisation Name</b>	<b>The Reason for Sharing</b>
The Department for Education	To provide data on international students
Regulatory bodies, such as Ofsted or the British Council	To comply with regulatory inspections
Service providers	For running surveys
Financial organisations	For processing payments
Our auditors	For carrying out legal audits of company accounts
Health and social welfare organisations	To manage student wellbeing
Professional advisers and consultants	To assist us in developing our business

Organisation Name	The Reason for Sharing
Police forces, courts, tribunals	For dealing with legal issues

### **TRANSFERRING AGENT DATA INTERNATIONALLY**

Your personal information may be stored and processed outside of the country where it is collected, including outside of the European economic area.

We will only transfer personal data to a country or territory outside the European economic area:

- where the transfer is to a place that is regarded by the European commission as providing adequate protection for your personal information; or
- where we have put in place appropriate safeguards to ensure that your personal information is protected (for example where both parties involved in the transfer have signed standard data protection clauses adopted by the European commission); or
- the above does not apply but we are still legally permitted to do so, for example if the transfer is necessary for the establishment, exercise or defence of legal claims.

You can request further detail about the safeguards that we have in place in respect of transfers of personal information outside of the EEA and where applicable a copy of the standard data protection clauses that we have in place, by contacting us at [marc.lewis@oxfordsixthformcollege.com](mailto:marc.lewis@oxfordsixthformcollege.com)

### **STORING AGENT DATA**

We will keep personal information about you while you are an active agent. We create and maintain records for each agent. The information contained in these records is kept secure and is only used for

purposes directly relevant to your position as an agent for Oxford Sixth Form College. Once your time as an agent with us has ended, we will retain this file and delete the information in it in accordance with our Data Retention Policy.