



Policies and Procedures

GDPR PRIVACY POLICY

Introduction

This policy applies to all Wise Origin College employees and all third parties responsible for the processing of personal data on behalf of Wise Origin College. It is intended to notify you, whether you are an employee, learner, worker or contractor, about the personal data that we hold relating to you in the course of your work for us. The document also explains how we can use your personal data and for what purposes.

Purpose

We are committed to conducting business in accordance with all applicable data protection laws and regulations and in line with the highest standards of ethical conduct.

We are deemed to be a "data controller" for the purposes of the GDPR. This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this Policy.

This Policy applies to current and former employees, learners, workers and contractors. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time but if we do so, we will provide you with an updated copy of this notice as soon as reasonably practical. It is important that you read and retain this notice, together with any other Privacy Notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information and what your rights are under the data protection legislation.

Data protection principles

Data protection law says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

We will comply with our obligations listed above.

The kind of information we hold about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are "special categories" of more sensitive personal data which require a higher level of protection, such as information about a person's health or sexual orientation.

We will collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email
- addresses.
- Date of birth.
- Gender.
- Marital status and dependants.
- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Start date and, if different, the date of your continuous employment.
- Leaving date and your reason for leaving.
- Location of employment or workplace.
- Copy of any driving licence used in the course of your work for us.
- 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).
- Employment records (including job titles, work history, working hours, holidays, training records and professional memberships).
- Performance information.
- Disciplinary and grievance information.
- Any CCTV footage and other information obtained through electronic means.
- Information about your use of our information and communications systems.
- Photographs obtained in connection with your work for us.

We may also collect, store and use the following "special categories" of more sensitive personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.
- Trade union membership.
- Information about your health, including any medical condition, health and sickness records, including:
- details of any absences (other than holidays) from work including time on statutory parental leave and sick leave; and where you leave employment and the reason for leaving is related to your health, information about that condition needed for pensions and permanent health insurance purposes.

- Information about criminal convictions and offences.

How is your personal information collected?

We collect personal information about employees, workers and contractors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies.

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

How will we use information about you

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with you.
2. Where we need to comply with a legal obligation.
3. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

1. Where we need to protect your interests (or someone else's interests).
2. Where it is needed in the public interest or for official purposes.

We need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below:

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Paying you and, if you are an employee or deemed employee for tax purposes, deducting tax and National Insurance contributions (NICs).
- Enrolling you in a pension arrangement in accordance with our statutory automatic enrolment duties.
- Administering the contract we have entered into with you.
- Business management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.

- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention and attrition rates.
- Equal opportunities monitoring.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

How we use particularly sensitive personal information

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal obligations or exercise rights in connection with employment.
3. Where it is needed in the public interest, such as for equal opportunities monitoring.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.

We will use your particularly sensitive personal information in the following ways:

- We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits including statutory maternity pay, statutory sick pay and pensions.
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.
- We will use any trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations.

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Data Subject Consent

Wise Origin College will obtain personal data only by lawful and fair means and, where appropriate with the knowledge and consent of the individual concerned. Where a need exists to request and receive the consent of an individual prior to the collection, use or disclosure of their personal data, Wise Origin College is committed to seeking such consent. We acknowledge that consent must be freely given, specific, informed and unambiguous. In order to obtain freely given consent, it must be given on a voluntary basis. The element “free” implies a real choice by the data subject. The Data Protection Officer, in cooperation with other relevant business representatives, shall establish a system for obtaining and documenting data subject consent for the collection, processing, and/or transfer of their personal data. These collection methods ensure that consent is obvious and requires a positive action to opt in. Consent requests are prominent, unbundled from other terms and conditions, concise and easy to understand, and user-friendly. All new systems and processes that are introduced are audited to confirm they apply to this standard.

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy. Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. We will use information about criminal convictions only when necessary and in compliance with relevant legislation.

Automated Decision Making

Automated decision-making takes place when an electronic system, such as a computer programme, uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

Where we have notified you of the decision and given you 21 days to request a reconsideration.

1. Where it is necessary to perform the contract with you and appropriate measures are in place to
2. safeguard your rights.
3. In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

Data Sharing

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

The following activities may be carried out by third-party service providers: payroll, pension administration, benefits provision and administration, IT services All our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. In this situation we will, so far as possible, share anonymised data with the other parties before the transaction completes. Once the transaction is completed, we will share your personal data with the other parties if and to the extent required under the terms of the transaction.

We may also need to share your personal information with a regulator or to otherwise comply with the law. This may include making returns to HMRC and disclosures to shareholders such as directors' remuneration reporting requirements.

Data Transfer (including outside of the UK)

Wise Origin College may transfer personal data to internal or third party recipients located in another country where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant data subjects. Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. third countries), they must be made in compliance with an approved transfer mechanism. Wise Origin College may only transfer personal data where one of the transfer scenarios list below applies:

- The data subject has given Consent to the proposed transfer.
- The transfer is necessary for the performance of a contract with the data subject
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the data subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded with a third party in the interest of the data subject.
- The transfer is legally required on important public interest grounds.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the data subject

Data Security

We have put in place measures to protect the security of your information. Details of these measures are available upon request to a director or senior manager.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data Retention

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with applicable laws and regulations.

Rights of access, correction, erasure and restriction

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Under certain circumstances, by law you have the right to:

- Request access to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing.
- Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- Request the transfer of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact a director or senior manager in writing.

You will not have to pay a fee to access your personal information (or to exercise any of the other rights).

However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive.

Alternatively, we may refuse to comply with the request in such circumstances.

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

Right to withdraw consent

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

Data Protection, confidentiality and Integrity

Wise Origin College will adopt physical, technical, and organisational measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment. A summary of the personal data related security measures is provided below:

- Prevent unauthorised persons from gaining access to data processing systems in which personal data are processed.
- Prevent persons entitled to use a data processing system from accessing personal data beyond their needs and authorisations.
- Ensure that personal data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation.
- Ensure that access logs are in place to establish whether, and by whom, the personal data was entered into, modified on or removed from a data processing system.
- Ensure that in the case where processing is carried out by a Data Processor, the data can be processed only in accordance with the instructions of the Data Controller.
- Ensure that personal data is protected against undesired destruction or loss.
- Ensure that personal data collected for different purposes can and is processed separately.
- Ensure that personal data is not kept longer than necessary

Data Protection Officer

We have appointed a data protection officer to oversee compliance with this policy. If you have any questions about this policy or how we handle your personal information, please contact the data protection officer.

The Data Protection Officer's duties include:

- Informing and advising wise Origin College and its employees who carry out processing pursuant to data protection regulations, national law or European Union based data protection provisions;
- Ensuring the alignment of this policy with data protection regulations, national law or European Union based data protection provisions;
- Providing guidance with regards to carrying out Data Protection Impact Assessments (DPIAs);
- Acting as a point of contact for and cooperating with Data Protection Authorities (DPAs);
- Determining the need for notifications to one or more DPAs as a result of Wise Origin College's current or intended personal data processing activities;
- Making and keeping current notifications to one or more DPAs as a result of Wise Origin College's current or intended personal data processing activities;
- The establishment and operation of a system providing prompt and appropriate responses to data subject requests;
- Informing senior managers, officers, and directors of Wise Origin College of any potential corporate, civil and criminal penalties which may be levied against the organisation and/or its employees for violation of applicable data protection laws.
- Ensuring establishment of procedures and standard contractual provisions for obtaining compliance with this Policy by any third party.

Record Management

Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognised Wise Origin College recordkeeping system.

All records relevant to administering this policy and procedure will be maintained for a period of 5 years.

Training

All employees that have access to personal data will have their responsibilities under this policy outlined to them as part of their staff induction training. In addition, each we will provide regular Data Protection training and procedural guidance for staff.

Complaints

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues. Please ask a senior manager or a director for the contact details of the ICO.

Evaluating effectiveness and Review

Wise Origin College ensure that all employees responsible for the processing of personal data are aware of and comply with the contents of this policy. In addition, we will make sure all third parties engaged to process personal data on their behalf (i.e. their data processors) are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all third parties, whether companies or individuals, prior to granting them access to personal data controlled by Wise Origin College.

The effectiveness of these measures will be subject to an annual assessment completed by the data protection officer and renewed / additional measures imposed as required.

This policy will be reviewed by the Data Protection Officer every three years, unless there are any changes to regulations or legislation that would enable a review earlier.

Review of the Policy

The GDPR Policy will be revised annually by the Senior Management Team and Director.

Policy Review	Review Date	Next Review Date	Approved by
Annually	26 July 2023	25 July 2024	Asif Khan