Randar Education
Data Protection Policy

Policy Date	**1st April 2025**
Review Date	**1st April 2027**

Version 1

REVIEW SHEET

Each entry in the table below summarises the changes to this policy and procedures made since the last review (if any).

Version Number	Version Description	Date of Revision
1	Original	1 April 2024
2	More concise language	May 2026

Everyone has rights about the way in which their personal data in handled. During our activities, we will collect, store and process personal data about our customers, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

Data users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

ABOUT THIS POLICY

The types of personal data that Randar may be required to handle include information about current, past and prospective and others that we communicate with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 (the Act) and other regulations.

This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

This policy does not form part of any employee's contract of employment and may be amended at any time.

This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

All employees at Randar are responsible for ensuring compliance with the Act and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Head of the centre/Operations Manager.

DEFINITION OF DATA PROTECTION TERMS

Data is information, which is stored electronically, on a computer, or in certain paper-based filing systems.

Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data

can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

Data controllers are the people who or organisations which determine the purposes for which, and the way, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our business for our own commercial purposes.

Data users are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

Data processors include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition, but it could include suppliers which handle personal data on Randar Education's behalf.

Processing is any activity that involves use of the 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 transferring personal data to third parties.

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

(a) Processed fairly and lawfully.

(b) Processed for limited purposes and in an appropriate way.

(c) Adequate, relevant and not excessive for the purpose.

(d) Accurate.

(e) Not kept longer than necessary for the purpose.

(f) Processed in line with data subjects' rights.

(g) Secure.

(h) Not transferred to people or organisations situated in countries without adequate protection.

FAIR AND LAWFUL PROCESSING

The Act is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

For personal data to be processed lawfully, they must be processed based on one of the legal grounds set out in the Act. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. When processing personal data as data controllers during our business, we will ensure that those requirements are met.

PROCESSING FOR LIMITED PURPOSES

During our business, we may collect and process the personal data. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

We will only process personal data for the specific purposes set out in or for any other purposes specifically permitted by the Act. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

NOTIFYING DATA SUBJECTS

If we collect personal data directly from data subjects, we will inform them about:

(i) The purpose or purposes for which we intend to process that personal data.

(j) The types of third parties, if any, with which we will share or to which we will disclose that personal data.

(k) The means, if any, with which data subjects can limit our use and disclosure of their personal data.

If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

We will also inform data subjects whose personal data we process that we are the data controller regarding that data.

Adequate, relevant and non-excessive processing

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

ACCURATE DATA

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

TIMELY PROCESSING

We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

We will process all personal data in line with data subjects' rights, in particular their right to:

(l) Request access to any data held about them by a data controller (see also clause 0).

(m) Prevent the processing of their data for direct-marketing purposes.

(n) Ask to have inaccurate data amended (see also clause 0).

(o) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

DATA SECURITY

We will process all personal data we hold in accordance with our Data Security Policy **OR** take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(p) **Confidentiality** means that only people who are authorised to use the data can access it.

(q) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

(r) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes.

Security procedures include:

(s) **Entry controls.** Any stranger seen in entry-controlled areas should be reported.

(t) **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

(u) **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.

(v) **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

We may transfer any personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

(w) The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.

(x) The data subject has given his consent.

(y) The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.

(z) The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.

The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

Subject to the requirements in clause 0 above, personal data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. That staff maybe engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

DISCLOSURE AND SHARING OF PERSONAL INFORMATION

We may share personal data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.

We may also disclose personal data we hold to third parties:

(aa) If we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets.

(bb) If we or substantially all our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.

If we are under a duty to disclose or share a data subject's personal data to comply with any legal obligation, or to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

We may also share personal data we hold with selected third parties for the purposes set out in the policy.

DEALING WITH SUBJECT ACCESS REQUESTS

Data subjects must make a formal request for information we hold about them. This must be made in writing. Employees who receive a written request should forward it to their line manager immediately.

When receiving telephone enquiries, we will only disclose personal data we hold on to our systems if the following conditions are met:

We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

We will suggest that the caller put their request in writing if we are not sure about the caller’s identity and where their identity cannot be checked.

Our employees will refer a request to their line manager for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

CHANGES TO THIS POLICY

Randar Education reserves the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or e mail.