DATA PROTECTION POLICY

Reviewed April 2021

CONTENTS

EDUCATIONAL COMPETENCIES CONSORTIUM LIMITED

DATA PROTECTION POLICY

1 POLICY STATEMENT

Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities Educational Competencies Consortium Limited will collect, store and process personal data about our registered members (**Members**), potential and existing clients (**Clients**), suppliers, employees and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in Educational Competencies Consortium Limited and will provide for successful business operations.

We are each obliged to comply with this policy when processing any such personal data. Any breach of this policy may result in disciplinary action.

2 ABOUT THIS POLICY

The types of personal data that Educational Competencies Consortium Limited (**We**) may be required to handle include information about current, past and prospective suppliers, employees, Members, Clients 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 and other regulations (which, from 25th May 2018, will include the General Data Protection Regulation) (the **Act**).

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.

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

If a data subject has any questions about this policy, please contact the Business Manager via contactus@ecc.ac.uk.

3 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 manner in which, 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 Educational Competencies Consortium Limited'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.

4 DATA PROTECTION PRINCIPLES

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

1. Processed fairly and lawfully.
2. Processed for limited purposes and in an appropriate way.
3. Adequate, relevant and not excessive for the purpose.
4. Accurate.
5. Not kept longer than necessary for the purpose.
6. Processed in line with data subjects' rights.
7. Secure.

8. Not transferred to people or organisations situated in countries without adequate protection.

5 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 on the basis of 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 in the course of our business, we will ensure that those requirements are met.

6 PROCESSING FOR LIMITED PURPOSES

In the course of our business, we may collect and process the personal data set out in the 0. 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 and others).

We will only process personal data for the specific purposes set out in the 0 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. We will only use personal data 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 personal information for an unrelated purpose, we will notify the relevant data subject and we will explain the legal basis which allows us to do so.

7 NOTIFYING DATA SUBJECTS

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

1. The purpose or purposes for which we intend to process that personal data.

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

3. 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 with regard to that data.

8 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.

9 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.

10 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.

11 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:

1. Request access to any data held about them by a data controller (see also clause 16). This enables a data subject to receive a copy of the personal information we hold about them and to check that we are lawfully processing it.

2. Prevent the processing of their data for direct-marketing purposes.

3. Ask to have inaccurate data corrected (see also clause 9).

4. Ask to have their data transferred to a third party (sometimes referred to 'data portability').

5. Prevent processing that is likely to cause damage or distress to themselves or anyone else.

6. Ask to have their data deleted. This enables a data subject to ask us to delete or remove personal information where there is no good reason for us continuing to process it.

7. Request the restriction of processing. This enables a data subject to suspend the processing of personal information about them, for example if they want us to establish the accuracy or the reason for processing it.

It is important that the personal information we hold about a data subject is accurate and current. Data subjects should keep us informed if their personal information changes during their working relationship with us.

12 DATA SECURITY

We will 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:

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

2. **Integrity** means that personal data must be accurate and suitable for the purpose for which it is processed.

3. **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data must therefore be stored on Educational Competencies Consortium Limited's central computer system instead of individual PCs.

Security procedures include:

1. **Entry controls.** Any stranger seen in entry-controlled areas must be reported.

2. **Secure lockable desks and cupboards.** Desks and cupboards must be kept locked if they hold confidential information of any kind. Personal information is always considered confidential.

3. **Methods of disposal.** Paper documents must be shredded. Digital storage devices must be physically destroyed when they are no longer required.

4. **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.

13 TRANSFERRING PERSONAL DATA TO A COUNTRY INSIDE THE EU

Under the UK and EU Trade and Cooperation Agreement (TCA) data transfers from the EU to UK can continue for a period of four months after Brexit whilst the EU considers the UK's application for adequacy (the usual mechanism used by the EU to

allow for continued data flow with third countries). This policy will be reviewed once further information is available. You should refer to the ICO website if you have any urgent queries – www.ico.org.uk

14 TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

The personal data that we hold is currently held on our, or third party, secure servers within the European Economic Area (**EEA**).

We will only transfer any personal data we hold to a country outside the EEA provided that one of the following conditions applies:

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

2. The data subject has given his consent.

3. 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.

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

5. 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 14.2 above, personal data we hold may from time to time need to 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. We will ensure that we comply with the requirements in clause 14.2 before making such transfer outside of the EEA.

15 DISCLOSURE AND SHARING OF PERSONAL INFORMATION

If applicable, 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:

1. In the event that 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.

2. If we or substantially all of 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 in order to comply with any legal obligation, or in order 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.

We may also share personal data we hold with selected third parties for the purposes set out in the 0.

Business contacts - Details of business contacts obtained during an employee's employment are considered confidential information and remain the property of the Company. Business contact details includes the contacts records in computer software installed on an employee's computer as well as maintained in third party websites including social media.

16 RIGHT TO WITHDRAW CONSENT

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

17 DEALING WITH SUBJECT ACCESS REQUESTS

Data subjects must make a formal request for information we hold about them. This must be made in writing to the Business Manager. 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 our systems if the following conditions are met:

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

2. 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.

18 RIGHT TO MAKE A COMPLAINT

A data subject has the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

19 CHANGES TO THIS POLICY

We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or email.

20 POLICY REVIEW

This policy will be reviewed by the ECC's Audit and Quality Assurance Committee annually or more frequently as required.

Agreed: **4 January 2018, revised 14 April 2021**

Next review date: **Spring 2022**

SCHEDULE 1 – DATA PROCESSING ACTIVITIES

Type of data	Type of data subject	Type of processing	Legitimate interests and purpose of processing	Type of recipient to whom personal data is transferred	Retention period
Personal Member and Client data (such as contact names, email addresses and telephone numbers)	Members and Clients	Internal (admin, business operations, for the provision of services and monitoring of provision and marketing) and external (if we subcontract any services or marketing)	To deliver our services to our members and clients. A valid email address is required for all ECC Online users.	Likely to remain internal. Will be external if we subcontract the delivery of our services or marketing, or where we subcontract ICT maintenance, support or development.	Until such time as the data is no longer reasonable required, or for 5 years after termination of membership.
Personal data relating to employees	Employees	Internal (admin, business operations, for the provision of services and monitoring of provision (and external (if we subcontract any services or business processes).	To deliver our services to our members and clients. To conduct business processes. To check whether our employees are legally entitled to work in the UK. To monitor equal opportunities. To make a decision about an employee's recruitment, appointment or continued employment with us.	Likely to remain internal. Will be external if we subcontract delivery of services or business processes such as payroll or engage professional advisers including legal and financial.	Until such time as the data is no longer reasonable required.
Personal data relating to suppliers and subcontractors	Suppliers' employees	Internal (admin, business operations, for the provision of services and monitoring of provision)	To deliver our services to our members and clients. To conduct business processes.	Likely to remain internal.	Until such time as the data is no longer reasonable required.

Type of data	Type of data subject	Type of processing	Legitimate interests and purpose of processing	Type of recipient to whom personal data is transferred	Retention period
Personal data relating to partner organisations	Partner organisations ' employees	Internal (admin, business operations, for the provision of services and monitoring of provision and strategic development)	To deliver our services to our members and clients. To conduct business processes. To enable strategic planning and development.	Likely to remain internal.	Until such time as the data is no longer reasonable required.
Personal data relating to potential clients and members	Potential clients' and potential members' employees	Internal (admin, business operations, for the provision of services and monitoring of provision and marketing) and external (if we subcontract any services or marketing)	To develop our services. To promote services to potential clients and members. Business to business marketing based on legitimate interests	Likely to remain internal. May be external if we subcontract marketing or research.	Until such time as the data is no longer reasonable required.