Data Protection Policy

Definitions

Company, "we", "us", "our": Impress the Examiner Ltd.

Company personnel, "personnel", "you", "your": All employees, tutors, contractors, consultants, directors and others working with Company personal data or Company client data on behalf of the Company.

Data subject: A living, identified or identifiable individual about whom we hold personal data. Data subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

The legislation: The Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR).

Personal data: Any information identifying a living individual (data subject) either directly or indirectly. This includes special categories and other high risk types of personal data.

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

Privacy notices or privacy policies: Separate notices setting out information that may be provided to data subjects when the Company collects information about them. These notices may take the form of general privacy or data protection statements applicable to a specific group of individuals (for example, the staff privacy policy or the website privacy notice) or they may be stand-alone, one time privacy statements covering processing related to a specific purpose (for example, the website contact form Consent notice).

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

1 Introduction

This document sets out how the Company handles the personal data of our clients and their students, suppliers, contracted tutors and staff, workers and other third parties.

It applies to all personal data that we process regardless of the media on which that data is stored or whether it relates to past or present tutors, staff, clients or supplier contacts, website users or any other data subject.

It applies to all company personnel. You must read, understand and comply with this Data Protection Policy when processing personal data on our behalf. The Company and all our personnel have a responsibility to comply with the principles and legal conditions provided by the legislation and

failure to meet those responsibilities are likely to lead to serious consequences. Firstly, any breach of this Data Protection Policy may result in the termination of your contract. Additionally, if you knowingly or recklessly disclose personal data in breach of the legislation you may be held personally legally accountable for any such breach.

The legislation contains strict principles and legal conditions which must be followed before and during any processing of any personal information. Breach of the legislation can cause distress to the individuals affected by the breach and is likely to leave the Company at risk of serious financial consequences.

If you are in any doubt about what you can or cannot disclose and to whom, do not disclose the personal information until you have sought further advice from the company's Data Protection Lead whose contact details appear at the base of this document.

This Data Protection Policy is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the Data Protection Lead.

2 What are the UK GDPR principles?

The Company and all staff must comply with the UK GDPR principles below at all times in their information-handling practices. We are committed to ensuring that these principles and rules are followed, as we take the security and protection of data very seriously.

You must inform us immediately if you become aware that any of these principles or rules have been breached or are likely to be breached.

2.1 Data Controllers

We are the controller of all personal data relating to our personnel and used in our business for our own commercial purposes.

As a controller we are required by law to ensure that everyone who processes personal data on our behalf does so in accordance with the legislation which includes the UK GDPR principles.

In brief, the principles say that:

- Personal data must be processed in a lawful, fair and transparent way.
- The purpose for which the personal information is collected must be specific, explicit and legitimate.
- The collected personal data must be adequate and relevant to meet the identified purpose.
- The information must be accurate and kept up-to-date.
- The personal data should not be kept in a form which permits identification of a data subject for longer than is necessary for the purposes for which it is used.
- The personal data must be kept confidential and secure and only processed by authorised personnel.

- The transfer of personal data to a country or organisation outside the UK should only take place if appropriate safeguarding measures are in place to protect the security of that data.
- The data subject must be permitted to exercise their rights in relation to their personal data.

2.2 Data Processors

In order to provide our services, the Company processes the student data of our clients (our clients are predominantly schools). We are, therefore, a data processor for our clients who are data controllers.

We act on behalf of our client schools and under their authority; we serve the clients' (controller's) interests rather than our own in the provision of our services to them. As such, under the legislation we are required to only process personal data in line with our clients' instructions, unless we are required to do otherwise by law.

3 Lawfulness, fairness and transparency

3.1 What are the lawful reasons under which we would expect you to process personal data?

The Company will only expect you to process personal data where the business has a lawful basis or multiple bases to process that information. These may be one or a combination of the following:

3.1.1 in order to fulfil our **contracts** either with you our staff, for example to pay you or to obtain a DBS check on your behalf; or with our clients, for example working with student data in order to fulfil our contracted tutoring obligations;

3.1.2 to comply with a **legal obligation**, for instance in Police investigations or legal cases;

3.1.3 where it is necessary for our **legitimate interests** and where the interests and fundamental rights of the data subject do not override those interests (for example using contact details to respond to queries or monitoring the quality of our services); and

3.1.4 where formal **consent** has been obtained from the data subject, for example where they consent to go on our tutor list to receive information before they have a contract with us.

There are other rare occasions where you may need to process a data subject's personal information. These include:

3.1.5 protecting the data subject's **vital interests**, for example if they are taken seriously ill you may need to provide their personal information to a doctor or paramedic in order to save their life; or

3.1.6 where it is needed in the **public interest** or for official purposes, this generally refers to tasks carried out by official bodies such as councils and government departments.

You must always be sure to identify and document the legal basis or bases being relied on in respect of each processing activity which you perform and that you communicate this legal basis to the data subject. Privacy notices are generally used for this purpose.

3.2 Consent

A Controller must only process personal data on the basis of one or more of the lawful bases set out in the legislation. Most often the Company will be working under the Contract and Legitimate Interest legal bases with individuals and organisations with whom we share legal agreements or who have specifically requested (for example via recruitment) to be in contact with us.

Occasionally, however, we will use the Consent legal basis, for instance where individuals who are not under contract with us appear on any tutoring or marketing contact lists.

A data subject consents to processing of their personal data if they clearly indicate agreement to the processing either by a statement or through positive action. Consent requires affirmative action, so data processing based on non-actions such as silence, pre-ticked boxes or a lack of response will not be sufficient.

Data subjects must be easily able to withdraw Consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to process personal data for a different and incompatible purpose which was not disclosed when the data subject first consented.

You will need to evidence Consent captured and keep records of all Consents so that the Company can demonstrate compliance with Consent requirements.

3.3 Privacy Notices (transparency)

The legislation requires Controllers to provide detailed, specific information to data subjects depending on whether the information was collected directly from them or from elsewhere.

Such information must be provided through appropriate Privacy Notices which must provide accurate, transparent and unambiguous details of:

- the lawful and fair reasons why we are processing the data;
- how, when and for how long we propose to process the data;

We must include all the information required by the legislation including:

- the identity of the Controller;
- the Data Protection Lead or Data Protection Officer (DPO) and any other key data protection staff member;
- how and why we will use, process, disclose, protect and retain that personal data.

Privacy Notices must be presented when the data subject first provides the personal data.

When personal data is collected indirectly, for example from a third party or publicly available source, you must provide the data subject with all the information required by the legislation as soon as possible after collecting/receiving the data.

Personal data collected by third parties must be collected on a basis which reflects our purposes in the processing of that data. The data subject must be aware when they provide their data how it is going to be used all along the processing line.

You must only use data collected indirectly if you have evidence that it has been collected in accordance with the UK GDPR principles.

4 Data integrity and confidentiality

Company personnel must maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- *Confidentiality* means that only people who have a need to know and are authorised to use the personal data can access it.
- *Integrity* means that personal data is accurate and suitable for the purpose for which it is processed.
- *Availability* means that authorised users are able to access the personal data when they need it for authorised purposes.

4.1 Only collect and keep the data you need

The collected personal data must be adequate and relevant to meet the identified purpose.

Personnel must only process personal data where they have been authorised to do so and because it relates to their work or they have been delegated temporary responsibility to process the information.

Personnel must not collect, store or use unnecessary personal data and must ensure that personal data is deleted, erased or removed within the Company's retention guidelines (see our Data Retention Policy).

Personnel must not process or use personal data for non-work related purposes.

The Company will review its records on a regular basis to ensure we do not contain a backlog of out-of-date or irrelevant information and to check there are lawful reasons requiring information to continue to be held.

4.2 Keep data accurate and up-to-date

Company personnel will ensure that the personal data we use and hold is accurate, complete, kept up-to-date and relevant to the purpose for which we collected it.

Personnel will check the accuracy of personal data when it is collected and at regular intervals afterwards. Make sure you take all reasonable steps to destroy or amend inaccurate or out-of-date personal data.

5 Data security

5.1 Technological safeguards

The Company will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of personal data that we own or maintain on behalf of others and to identify risks.

This includes the use of encryption and pseudonymisation where pseudonymisation is the process of replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is kept separate and secure.

We will regularly evaluate and test the effectiveness of all safeguards to ensure the security of our processing of personal data.

5.2 Responsibilities of Personnel

Company personnel are responsible for protecting the personal data we hold. We require all personnel working with our data and our Clients' data to:

- Read, understand and follow our Staff Data Protection Protocol.
- Implement reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss of or damage to personal data and to exercise particular care in protecting special category and other sensitive personal data from loss and unauthorised access, use or disclosure.
- Follow all procedures and technologies put in place by us to maintain the security of personal data from the point of collection to the point of destruction.
- Comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the legislation and relevant standards to protect personal data.
- Not establish Company accounts with any third-party service provider for the purpose of processing personal data without the direct permission of the Data Protection lead.
- Only transfer personal data to third-party service providers who agree to comply with the required policies and procedures and who agree to put or have already put adequate data protection measures in place.

6 Transferring data to another country

The transfer of personal data to countries or organisations outside the UK should only take place if appropriate safeguarding measures are in place to protect the security of that data.

You must speak to the Data Protection Lead before you send personal data outside the UK.

7 Reporting a personal data breach

The legislation requires Controllers to notify any data security incidents severe enough to be deemed a personal data breach to the applicable regulator – in the UK this is the Information Commissioner's Office (ICO) – and, in certain instances, the data subject.

See our Data Breach Procedure for our procedure to deal with any suspected personal data breach.

Any personnel that knows or suspects that a personal data breach has occurred, should not attempt to investigate the matter themselves but immediately inform the Data Protection Lead. Preserve all evidence relating to the potential personal data breach.

8 The data subject rights and requests

Under the legislation, subject to certain legal limitations, data subjects have a number of rights regarding how their personal data is processed. At any time a data subject can request that the Company should take any of the following actions with regard to their personal data:

- Allow access to the personal data
- Request corrections to be made to data
- Request erasure of data
- Object to the processing of data
- Withdraw their consent if consent was the legal basis for processing
- Request that processing restrictions be put in place
- Request a transfer of personal data
- Object to automated decision making
- Right to be notified of a data security breach

Note that Data Subject Access Requests (SAR) can be verbal, they do not need to be in writing.

All SARs should be directed to **Fatima Hajnal, admin@impresstheexaminer.com 03332 12 05 75**. Do not allow third parties to persuade you into disclosing personal data without proper authorisation.

The process for dealing with SARs is set out in our Subject Access Request Procedure.

9 Privacy By Design and Data Protection Impact Assessments (DPIA)

The Company is required to implement Privacy by Design measures when processing personal data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

'Privacy by design' means incorporating data protection into the planning and exercising of all data processing activities and business practices from the design stage right through the data lifecycle, and being able to demonstrate this.

The Company must assess what Privacy by Design measures can be implemented on all programs, systems and processes that process personal data by taking into account the following:

a. the state of the art;

b. the cost of implementation;

c. the nature, scope, context and purposes of processing; and

d. the risks of varying likelihood and severity for rights and freedoms of data subjects posed by the processing.

Data protection impact assessments (DPIAs) are used to assess the risks to data subjects when processing their personal data, particularly if their data is sensitive or 'special category'.

You should conduct a DPIA (and discuss your findings with the Data Protection Lead) when implementing major system or business change programs involving the processing of personal data including:

a. use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

b. automated processing including profiling and automated decision making;

c. large scale processing of special categories of personal data or criminal convictions data; and

d. large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

a. a description of the processing, its purposes and the Controller's legitimate interests if appropriate;

b. an assessment of the necessity and proportionality of the processing in relation to its purpose;

c. an assessment of the risk to individuals; and

d. the risk mitigation measures in place and demonstration of compliance.

10 Sharing personal data

We may share personal data internally as necessary. Personnel must always ensure that personal Data is only shared with authorised persons and is shared in accordance with the purposes stated in any privacy notice or consents.

Extra care and security must be taken when sharing special categories of data or transferring data outside the Company to a third party.

11 Direct Marketing

We are subject to specific rules under the legislation in relation to marketing our services. Data subjects have the right to reject direct marketing and we must ensure that they are given this option at first point of contact. When a data subject exercises their right to reject marketing you must desist immediately from sending further communications.

12 Complaints

If you believe that this policy has been breached by a colleague or to exercise all relevant rights, queries or complaints please in the first instance contact:

Data Protection Lead
Tamara Caldwell
E-mail: tcaldwell@impresstheexaminer.com
MOB: 03332 12 05 75

13 Changes to this policy

We reserve the right to change this policy at any time so please always check this document regularly to ensure you are following the correct procedures.

This policy was last updated on 11 October 2021.

Compliance with the UK GDPR is everyone's responsibility.

By signing this policy you confirm that you have read and understood the content of this policy and that you agree to adhere to the content and that you understand that breach of any aspect of this policy may lead to serious disciplinary action.

Signed by: Date:

Print name of employee/worker/contractor: