Tutors and Exams

DATA PROTECTION AND GDPR POLICY

2020- 2021

Issued September 2020

Approved/reviewed by	
Claire Coleman	
Date of next review	September 2021

This plan is reviewed annually to ensure compliance with current regulations

Key staff involved in this policy

Role	**Name(s)**
Data Protection Officer	**Clare-Louise Galliers**
Data Controller	**Wendy Quinney**

Contact Numbers/Emergency contacts

	Phone number
Main Number	**024 7622 1008**

Contents

Policy information	
Organisation	Tutors and Exams Ltd (the company)
Scope of policy	The Policy applies to all offices of Tutors and Exams Ltd The company has no Data Processors acting on our behalf.
Policy operational date	September 2020
Policy prepared by	Claire Coleman Data Protection Officer / Data Controller Data Protection Officer – The person on the management committee who is responsible for ensuring that it follows its data protection policy and complies with the Data Protection Act 1998. Data Controller – The person who (either alone or with others) decides what personal information Tutors and Exams will hold and how it will be held or used _____ The DPO will endeavour to ensure that all personal data is processed in compliance with this Policy and the Principles of the Data Protection Act 1998. The Freedom of Information Act 2000 and the Protection of Freedoms Act 2012 are also relevant to parts of this policy. The company recognises The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) adopted 27 April 2016, the two-year transition period and the application date of 25 May 2018 and compliance with that directive. Background on GDPR https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/
Date approved by Board/ Management Committee	September 2020
Policy review date	September 2021

<table>
<tr><td colspan="3">Introduction</td></tr>
<tr><td>Purpose of policy</td><td colspan="2">The company is required to process relevant personal</td></tr>
<tr><td rowspan="5">Types of data</td><td colspan="2">Data is processed in terms of LEGITIMATE INTEREST of members of staff, contactors, candidates, candidate parents/guardians and customers.

Personal data can be held on computers, laptops and mobile devices, or in a manual file, and includes email, minutes of meetings, and photographs.

Personal data covers both facts and opinions about an individual where that data identifies an individual. For example, it includes information necessary for employment such as the member of staff's name and address and details for payment of salary or a candidate's application, personal data and exam results.

Personal data may also include sensitive personal data as defined in the Act; for example, candidates with Special Considerations and Access Arrangements. Sensitive personal data also includes data relating to medical information, gender, religion, race, sexual orientation, trade union membership and criminal records and proceedings.</td></tr>
<tr><td>Members of Staff</td><td>name and address and details for payment of salary.</td></tr>
<tr><td>Contractors</td><td>name and address and details for payment of salary.</td></tr>
<tr><td>Candidates</td><td>name and address and details for processing examination entries.

Including data relating to Special Considerations and Access Arrangements</td></tr>
<tr><td>Candidate Parents/Guardians</td><td>name and address and details for processing examination entries of candidates</td></tr>
</table>

	Customers	Customers may be candidates or parents/guardians of candidates
Policy statement	The company shall so far as is reasonably practicable comply with the Data Protection Principles (the Principles) contained in the Data Protection Act and GDPR to ensure all data is:- • Fairly and lawfully processed • Processed for a lawful purpose • Adequate, relevant and not excessive • Accurate and up to date • Not kept for longer than necessary • Processed in accordance with the data subject's rights • Secure • Not transferred to other countries without adequate protection In addition to: • Respect individual's rights • be open and honest with individuals whose data is held • provide training and support for staff who handle personal data, so that they can act confidently and consistently • Notify the Information Commissioner voluntarily, even if this is not required It is taken that any data processing undertaken by the company is at the request and legitimate interest of the company's customers, staff and contractors. Background on individuals' rights : (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/) The company will endeavour to ensure that all personal data held in relation to all Data Subjects is accurate. Data Subjects must notify the data processor of any changes to information held about them. Data Subjects have the right in some circumstances to request that inaccurate information about them is erased. This does not apply in all cases, for example, where records of mistakes or corrections are kept, or records which must be kept in the interests of all parties to which they apply.	

Key risks	The main risks within the company lie in two key areas: • data getting into the wrong hands, through poor security • data getting into the wrong hands, through inappropriate disclosure of information • individuals being harmed through data being inaccurate or insufficient

Responsibilities	
The Board / Company Directors	Recognise that they have overall responsibility for ensuring that the company complies with its legal obligations.
Data Protection Officer	The responsibilities of the DPO include the following Data Protection/GDPR (DP/GDPR) issues: • Briefing the Board on DP/GDPR responsibilities • Reviewing DP/GDPR and related policies • Advising other staff on tricky DP/GDPR issues • Ensuring that DP/GDPR induction and training takes place • Notification to the ICO • Handling subject access requests • Approving unusual or controversial disclosures of personal data • Approving contracts with Data Processors (should this be deemed necessary in the future)
Specific Department Heads	Not applicable within the company at present. To be approved by DPO as necessary.
Employees & Volunteers	All staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work. (The term 'employees' includes both paid employees and volunteers.)
Enforcement	The company and therefore all employees and contractors are required to respect the personal data and privacy of others and must ensure that appropriate protection and security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to all personal data. Should this policy be breached, the DPO and Directors of the company will be informed. Employees or contractors will be required to undergo training (to be record by DPO)

Security	
Scope	It is noted that Data Security is not wholly a Data Protection issue. The company is developing a Business Continuity policy - backup procedures (both for data and for key employee availability) and emergency planning
Setting security levels	An appropriate level of data security must be deployed for the type of data and the data processing being performed. In most cases, personal data must be stored in appropriate systems and be encrypted when transported offsite. Other personal data (examination seating plans and candidate timetables) will be used during public examinations under controlled circumstances; therefore having a lower requirement for data security.
Security measures	Security measures: • Computers – require access key • Microsoft One Drive – require user name and password Access to examination rooms is controlled under JCQ Policies. The company will take appropriate technical and organisational steps to ensure the security of personal data. All staff will be made aware of this policy and their duties under the Act/GDPR. The company does not maintain a clear desk policy, this matter is under review by the company Directors.
Specific risks	The company does not process 'off site' or use external contractors. The company does not use external organisations to process data. All data processing is 'on site' <u>Phishing and Malware attacks</u> Employees and contractors are made aware of the treat of "vishing" and "phishing" emails. To avoid employees and contractors being tricked into giving away information over the phone or by email, staff are trained annually about current threats and how to deal with the risks arising. Specifically, employees and contractors should not give the personal information of Data Subjects to third parties.

Data recording and storage	
Accuracy	The company will endeavour to ensure that all personal data held in relation to all Data Subjects is accurate. Data Subjects must notify the data processor of any changes to information held about them. Data Subjects have the right in some circumstances to request that inaccurate information about them is erased. This does not apply in all cases, for example, where records of mistakes or corrections are kept, or records which must be kept in the interests of all parties to which they apply.
Updating	The company may retain data for differing periods of time for different purposes as required by statute or best practices. The fundamental requirement of the company is to ensure the identification of candidates. This may require the company holding photographs and personal information over several examination sessions. This this is to identify candidates and for the convenience of candidates. Individual data requirements are incorporate these retention times. For example, CVs cannot be kept for more than 6 months without the express permission of the data subject. The company may store some data such as examination administration material, photographs, exam results and examination certificates awaiting collection indefinitely. Subject to legal requirements. To date, the company has not introduced a regular cycle of checking, updating or discarding old data. This is to be reviewed by the DPO and the Directors of the company, with regard to the number of returning customers and candidates.
Storage	This is to be reviewed by the DPO and the Directors of the company
Retention periods	This is to be reviewed by the DPO and the Directors of the company
Archiving	This is to be reviewed by the DPO and the Directors of the company

Right of Access	
Responsibility	Examination Officers are responsible for ensuring that right of access requests are handled within the legal time limit of one month
Procedure for making request	Right of access requests must be in writing to the appropriate Exam Centre. All employees or contractors are required to pass on anything which might be a subject access request to the appropriate Examination Officer without delay. Further information about Rights of Access is available on the following link: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/
Provision for verifying identity	Provision for checking their identity before handing over any information. Exams Officers should use data subject information to verify the identity of an individual making a Right of Access Request.
Charging	Information is provided free of charge. A charge ('reasonable fee') may be made when a request is manifestly unfounded or excessive, particularly if it is repetitive. The company may also charge a reasonable fee to comply with requests for further copies of the same information. The fee is based on the administrative cost of providing the information.
Procedure for granting access	If the request is made electronically, the information will be provided in a commonly used electronic format. It is noted that the GDPR best practice recommendation, is to provide remote access to a secure self-service system to provide individuals with direct access to their information. This is not appropriate for the nature of the company's business model

Operational Guidance	
E Mail	All staff should consider whether an email (both incoming and outgoing) will need to be kept as an official record. If the email needs to be retained it should be saved into the appropriate folder or, printed and stored securely. The original email should then be deleted from the personal mailbox and any "deleted items" box, either immediately or when it has ceased to be of use. Remember, emails that contain personal information which is no longer required for operational use, should be deleted from the personal mailbox and any "deleted items" box.
Phone Calls	Phone calls can lead to unauthorised use or disclosure of personal information and the following precautions should be taken: • If you receive a phone call asking for personal information to be checked or confirmed, • Be aware that the phone call may come from someone pretending to be the data subject, or impersonating someone with a right of access. • Personal information should not be given out over the telephone unless you have no doubts as the caller's identity and the information requested is innocuous. If you have any doubts, ask the caller to put their enquiry in writing.
Passwords	The company passwords should not be easy to guess. Make sure all your passwords contain both upper and lower-case letters and preferably contain some numbers. Ideally passwords should be 6 characters or more in length.

Transparency	
Commitment	The company is committed to ensuring that Data Subjects are aware that their data is being processed and • for what purpose it is being processed • what types of disclosure are likely, and • how to exercise their rights in relation to the data
Procedure	• This information is available on the company website • Reference to data subject information within the DPA/GDPR legislation is identified on the candidate application form.
Responsibility	All employees and contractors are responsible for transparency in relation to Data Subjects.

Lawful Basis	
Underlying principles	Data is processed in terms of LEGITIMATE INTEREST of members of staff, contactors, candidates, candidate parents/guardians and customers. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/
Opting out	It is difficult to envisage the potential for employees, contractors or candidates to opt out of the company's data processing system. To opt out would render JCQ candidate verification invalid and contravene their rules.
Withdrawing consent	Once given, consent can be withdrawn, but not retrospectively. In such a situation, it will be taken that a candidate wishes to withdraw from their examination entry. The company cannot guarantee that fees can be refunded. Given the nature of the company's business, there may be occasions where the company has no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn

Employee training & Acceptance of responsibilities	
Induction	All employees who have access to any kind of personal data, have their responsibilities outlined during their induction procedures
Continuing training	If there are opportunities to raise Data Protection issues during employee training, team meetings, supervisions, etc. this may be worth mentioning
Procedure for staff signifying acceptance of policy	This DPA/GDPR Policy is supplementary to the company handbook. This Policy is available on the company's Document storage facility (Company Policies)

Policy review	
Responsibility	The next Policy review will be completed by the DPO.
Procedure	All employees and contractors may be consulted during this review.
Timing	It is expected that the Policy review will be completed by September of the year of review.

For more information, please visit the ICO website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

When using a third party data processor, please read the guidelines here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/