



36 Washington Street, Glasgow, G3 8AZ. Tel. 0141 303 8430

## **Privacy Policy**

### **Including GDPR Considerations**

**April 2020**

**Glasgow Training Rooms ("GTR")**

**Request to withdraw from communications or delete any personal data held by us can be made by contacting [ian.mccallum@glasgowtrainingrooms.co.uk](mailto:ian.mccallum@glasgowtrainingrooms.co.uk) by email, or through website contact details found on [www.glasgowtrainingrooms.co.uk](http://www.glasgowtrainingrooms.co.uk).**

## GTR Privacy Policy Summary

<b>Purpose of policy</b>	<p>The purpose of this policy is to :</p> <ul style="list-style-type: none"> <li>• protect clients, staff and other individuals</li> <li>• follow good operational practice</li> <li>• comply with the appropriate legal requirements</li> <li>• protect the organisation</li> </ul>
<b>Types of data</b>	<p>GTR may as part of our business conversations record:</p> <p>Email address and contact information          Name and job title          Demographic information such as postcode          Other information relevant to enquiries</p> <p>We require this information to understand client and enquiry needs and provide an acceptable level of service, and in particular for the following reasons:</p> <p>Internal record keeping.          From time to time, we may also use information to contact previous contacts for the purpose of feedback, additional information provision, or to determine if our services are still relevant.          If attending one of our events we ask for a responsible individual's mobile number for the explicit purpose of allowing communication during unexpected circumstances (e.g. heavy snowfall). We are clear that this is optional and is intended to allow communications in everyone's interests in unusual circumstances and will only be used for this purpose.</p> <p>The types of data which could be considered personal data held by the company consist of data or details held on staff and also data supplied by clients or enquiries through standard business operations. GTR does not control or process sensitive data as we understand it as defined under current or known upcoming legislation. The information obtained from clients, or information requestors who have previously requested information or services, is retained where the information has been required in order to provide those services, or answer requests, in order to maintain business records required by law, or where this is suggested by good customer and prospective customer business practice</p>
<b>Policy statement</b>	<p>As fundamental guiding principles, GTR aims to:</p> <ul style="list-style-type: none"> <li>• respect individuals' rights</li> <li>• be open and honest with individuals whose data is held</li> <li>• comply with both the law and good practice</li> <li>• provide training and support for staff who handle personal data, so that they can act confidently and consistently</li> <li>• notify the Information Commissioner voluntarily, even if this is not required, when any potential breach may become evident.</li> </ul> <p>Particularly, GTR holds as essential to all ongoing operations, that the rights of individuals are upheld as both a specific aim and also as a standard part of normal and expected operating practice.</p>

## GTR Privacy Policy Detailed

<b>Organisations</b>	<p><b>Kingston Clyde Ltd / Etopia Solutions Ltd</b>          Trade as Glasgow Training Rooms          Company Registration: SC504197 / SC232988          36 Washington Street          Glasgow          G3 8AZ</p>
<b>Scope of policy</b>	<p>This policy applies to the business and operations of GTR and where appropriate the processing of data where this undertaken by a supplier or subcontractor. The scope includes data or details of information held on staff and clients or others who have requested information or services.</p> <p>The policy has been updated to reflect GTR's responsibilities under new legislation regarding personal data. The GDPR applies to personal data meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.</p> <p>This definition provides for a wide range of personal identifiers to constitute personal data, and this may include, for information supplied to GTR, name and location data.</p> <p>The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria.</p> <p>Under examinations, currently any external processor to GTR is identified as situations where billing is sent to an individual person as an individual and where name, email address and location address may feature in invoices (necessarily involved in business practice) and where payment facilities have been requested. This may also apply where an individual's name features in any supplied email address upon invoicing an organisation. Current processors may, for particular occasions, be either individually or collectively Microsoft, Sage or PayPal, who have readily available Privacy Policy statements available.</p>
<b>Policy operational date</b>	<p>This policy becomes operational on 2<sup>nd</sup> April 2020 and is subject to review every 3 years forward from this point.</p>
<b>Policy prepared by</b>	<p>This policy has been prepared by GTR's Commercial Director and responsibility lies with that individual and position. This is currently as of April 2020, Ian C McCallum BA. GTR does not process sensitive data and has not at this point appointed a Data Protection Officer.</p>
<b>Date approved by Board/ Management Committee</b>	<p>This policy has been approved by GTR's Board of directors on 2<sup>nd</sup> April 2020.</p>
<b>Policy review date</b>	<p>This policy will be in review during February and March 2023, with changes required initiated by latest on 2<sup>nd</sup> April 2023.</p>

<b>Key risks</b>	<p>The main identified risks have been determined to be:</p> <ul style="list-style-type: none"> <li>• information about data getting into the wrong hands, through poor security or inappropriate disclosure of information</li> <li>• to a lesser extent, individuals being harmed through data being inaccurate or insufficient</li> <li>• In both cases above GTR has identified potential risk situations and sought to minimise the possibilities through allocating responsibility, control procedures and staff training and operational practices</li> </ul>
------------------	--

<b>Responsibilities</b>	
<b>Company Directors</b>	Have overall responsibility for ensuring that the organisation complies with its legal obligations and for responsible and defensible business practice.
<b>Employees &amp; Volunteers</b>	All staff and any 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. (From now on, where 'employees' is used, this includes both paid employees and volunteers.)
<b>Enforcement</b>	Any potential, or actual, infringing of Data Protection and related policies is an automatic issue to be raised and discussed at (initially) an internal review meeting held for the purpose with line management. Employees are encouraged to advise of or report any situation, practice or non-compliance that could potentially lead to any situation where data security could be compromised for any reason.

<b>Security</b>	
<b>Scope</b>	Data Security is a business issue in addition to being something that is covered by legal and professional requirements - and all employees are actively encouraged to maintain best practice for data held for any reason.
<b>Security measures</b>	All information held by the organisation on any computer system is subject to individually named logon and password protection. Work being processed on paper on desks will be restricted to tasks, requests and information provision that have a current requirement for that being processed.
<b>Business continuity</b>	Backups (these are internal) of information that we hold - is subject to the same security requirement as above.
<b>Specific risks</b>	<p>While GTR may allow remote working of employees, this is subject to the same password and login requirements as when working at an GTR office.</p> <p>Requests for information held are subject to validity challenge and multi-factor authentication and identification. In addition staff are actively encouraged to treat any information as they would their own – e.g. non provision to any potentially unauthenticated request.</p>

## **Data recording and storage**

<b>Updating</b>	Customer data is maintained for as long as this is useful to be held, under standard and regular commercial requirements to know your customer. Information on quotes and communications to organisations (and occasionally individuals) whom have enquired regarding services or with whom we have had service provision discussion of any form - may be kept on record for the time that is may be useful to both parties to have records of prior conversations for continuity purposes. Staff data is maintained on a continuing basis. Any legitimate request to remove held information is acted upon as a matter of high business priority under best efforts with available resources.
<b>Storage</b>	Information is held electronically however paper copies may exist such as invoices which contain information that makes people identifiable – e.g. email addresses. Records are filed within offices that as standard practice are locked when no appropriate company personnel are present within the relevant room.
<b>Retention periods</b>	Data is retained subject to being useful to identify previous customers and enquirers, suppliers and employees and other business contacts. Our field of operations is business-to-business sales in addition to supply to public sector organisations. GTR does not hold mass or collated records of information on individuals. There are no specific periods currently when any personal data component of our business information is systematically culled or destroyed - these are contained within records of the customer or enquiry maker.

<b>Right of Access</b>	
<b>Responsibility</b>	All Directors are individually and severally responsible for ensuring that any right of access requests of which they are aware of - are handled within one month.
<b>Procedure for making request</b>	Rights of access refer to a data subject (someone whose information may be held) asking for information to be copied to themselves or another party, or be deleted. Right of access requests must be in writing. All employees have a clear responsibility to pass on anything which might be a subject access request directly to the appropriate person or Director without delay. GTR understands that individuals have a right to complain to the ICO if they think there is a problem with the way any organisation is handling their data.
<b>Provision for verifying identity</b>	Where the person managing the access procedure does not (without any room for any doubt) know the individual personally, then entirely appropriate and suitable provision should be made for checking of their identity before handing over any information.
<b>Charging</b>	Information held is provided free of charge. However employees should be aware that under legislation an organisation can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive or for further copies of the same information. The fee must be based on the administrative cost of providing the information.
<b>Procedure for granting access</b>	If the request is made electronically, we provide the information in a commonly used electronic format like PDF.  GDPR includes a best practice recommendation that, where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information. This is not currently appropriate for GTR's operations.

<b>Transparency</b>	
<b>Commitment</b>	Through business necessity, GTR captures information when it is either offered or requested as part of a form of service provision request, to or from the company. We aim that everyone holding discussions with us through email, telephone conversation, discussion in person, or any other means - is fully aware that we may retain the information provided in order to meet with aim of our being able to provide continuity with continuing conversations in the future.

<b>Lawful Basis</b>	
<b>Underlying principles</b>	GDPR states you must record the lawful basis for the personal data held by an organisation, which for GTR is under legitimate interests.
<b>Opting out</b>	GTR will treat any and every legitimate notification to opt out of anyone's data being held or processed as a priority under best available efforts.
<b>Withdrawing consent</b>	GTR appreciates that, once given, consent can be withdrawn, but not necessarily retrospectively. There may be occasions (such as the company maintaining appropriate VAT records) where the organisation has no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn.

<b>Employee training &amp; Acceptance of responsibilities</b>	
<b>Induction</b>	All employees who have access to any kind of personal data will have their responsibilities outlined during their induction procedures.
<b>Continuing training</b>	Any changes to Data Protection requirements are discussed during employee training or team awareness meetings as appropriate.

<b>Policy review</b>	
<b>Responsibility</b>	Commercial Director to review c. March 2023.
<b>Procedure</b>	While responsibility lies with GTR's Commercial Director, it is expected that other customer-facing, administrative and operational employees will be consulted in the review.
<b>Timing</b>	The review will be initiated in February 2023 in order to be completed by April 2023.