



InPlace Network Privacy Notice

QuantumIT Solutions

© 2021 Quantum Information Technology Pty Ltd.

The smart companion to  **InPlace**
Smart Placement Solutions

Contents

Introduction.....	3
Collecting Personal Information	3
Use of Personal Information	4
Shift Information	4
Surveys.....	4
Comments	4
Auditing.....	5
Student Information	5
Transfers of data outside the EU.....	5
Cookie Policy	6
Retention policy of data	7
Security policy of data	7
Amendment clause.....	7
User Rights	7
Updating information	8
Contact details	8

Introduction

The purpose of this Privacy Notice is to inform an InPlace Network user (“User”), how QuantumIT, the InPlace Network owners, plan on using the User’s personal data.

InPlace Network is an online platform used by Placement Providers (“Agency”) to organise and track the Placements that they offer to Higher Educational Institutes (“HEI”) and their students.

In this case, the Data Controller for InPlace Network is the Agency or HEI to which a User is affiliated. QuantumIT is the Data Processor, and as such can only use InPlace Network as specified in their contracts with each Data Controller.

As defined by the GDPR, processing may include, but is not limited to, storing, organising, retrieving, using, modifying, sharing, restricting, and erasing personal data. User’s information can and will be displayed to relevant Staff & Agency users in InPlace Network. InPlace Network facilitates the following sets of operations:

- User registration process,
- Capacity Management,
- Request & Placement Management,
- Capacity & Placement Reporting,
- InSight Surveys and Campaigns,
- Costs and Payments Management,
- Integration with InPlace and Audit Tool,
- Data maintenance and security processes.

Throughout these operations, QuantumIT’s Data Controllers have prioritised protecting the interests of their InPlace Network Users. Consequently, QuantumIT always endeavours to use User personal data in a way that will benefit the data subject, as defined in their contracts with the Data Controllers.

Collecting Personal Information

There are three main user types: Administrators, Agency users and HEI users. Depending on the user type, Users will be asked to provide different information in order to create their account and successfully use InPlace Network. Please note that any information Users enter,

and most of their activity in InPlace Network, will be processed in some form or another, and most likely be retained for as long as the account remains active.

For all users to create an account, InPlace Network requires a name, work email, related HEI or Agency, Employment type and Role. This information is used to identify individuals, and understand when and how to contact them when they need to action placement related activities.

Use of Personal Information

In addition to the information requested of users in order to create an account, QuantumIT will record user interactions in InPlace Network in the following cases:

Shift Information

For Users with a Supervisor role, shift information is recorded in InPlace Network so that Staff Members and Agency Personnel know when to assign students to them for supervision.

Surveys

Responses to any InSight Surveys and Campaigns are recorded for use by the requesting HEI or Agency. Related HEI or Agency personnel will often view these answers for statistical and analytical purposes. Responses will be kept as long as the Data Controller deems necessary.

Comments

Supervisors have the opportunity to provide comments on placements, while Coordinators are asked to submit comments on requests and opportunities. These are recorded on the placement/request/opportunity entry to which they relate.

Auditing

For auditing reasons, for most entities - such as requests, placements and capacity planning - the creating user and last modifying user are recorded against them.

Student Information

Whilst most students do not have access to InPlace Network, their information is stored in InPlace Network when they are assigned to a Placement. This includes Name, DOB, Title, Contact Details, Gender and Photo (if provided). Where possible, QuantumIT strongly recommend not exporting any information from InPlace Network. If Users feel compelled to export personal information, QuantumIT recommends checking their Data Controller's Data Retention Policy prior to doing so.

In certain circumstances, GDPR allows disclosure of personal data to law enforcement agencies without the consent of the data subject. Under these circumstances, the Data Controller will be obliged to disclose personal information to the requesting law enforcement agency. QuantumIT is contractually obligated to aid them in doing so. The Data Controller will need to ensure the request is legitimate, seeking assistance from their board and from their legal advisers where necessary.

Transfers of data outside the EU

QuantumIT will only effectuate a Transfer of Data outside the EEA (according to GDPR) in the following manner:

- people/entities outside the EEA being able to access or "see" personal data held in the EEA;

Whilst personal data will normally be processed and held in the same region as the Data Controller (E.g. UK based University will have all their related information stored in the UK) in the event of a software, database or other similar data-related issue, QuantumIT may need to grant remote access to the HEI database to their head office (Melbourne, Australia) or other development teams both inside and outside the EEA. Where possible, the issue will be recreated in an instance of InPlace Network where no personal data is held.

Where this is not possible, access will be restricted to a need-only basis, and will be revoked as soon as the issue has been resolved. No copies of any data will be made or otherwise transferred elsewhere. Personal information will continue to be protected to the same standard as always, and data subjects will continue to have the same rights over their personal data as they would under normal circumstances.

The Data Controller might also ask QuantumIT to transfer student data to medical boards, government agencies or other organisations. When transferring data, QuantumIT always ensures that all personal data is adequately protected throughout the transfer process. These, and all other transfers, will only ever take place under direct instruction from QuantumIT’s Data Controllers, or when within the scope of QuantumIT’s contract with the Data Controller.

Finally, any user that is created for an EEA based Data Controller will have access to InPlace Network regardless of their geographic location. As such, if a user were to login to InPlace Network from outside the EEA, they would be able to see the same data as if they had logged in from within the EEA (effectively carrying out a Transfer of Data outside the EU). QuantumIT cannot take any responsibility for the actions of users that they do not employ.

Cookie Policy

InPlace Network uses (session) cookies to allow users to open a session after successfully authenticating their access. After the cookies reach their expiration, they are no longer valid, and will be deleted by the User’s internet browser. Here’s a list of the cookies InPlace Network uses and their purpose:

Name	Origin	Purpose	Mandatory	Expiration
StickyClientSessionId	InPlace Network 1.2+	Opens a session after validation confirmed.	Yes	Browser Session ends
QuantumNetworkId	InPlace Network 1.2+	Confirms that __StickyClientSessionId is not a forgery.	Yes	Browser Session ends

Retention policy of data

As part of the QuantumIT Data Retention Policy, QuantumIT deletes all inactive personal data after a 10 year period. Data subjects have increased rights over the retention period if they so wish to utilise them. These are detailed in the section labelled User Rights.

Security policy of data

QuantumIT Security Policy covers the following areas:

- Access control
- Network and Server security
- Application and Database security
- Cloud Services security
- Data Transfer security
- Penetration testing

Please contact the Data Controller's Data Protection Officer to obtain a copy of the QuantumIT Security Policy.

Amendment clause

QuantumIT retain the right to amend this Privacy Notice at any time. As QuantumIT inherits the Data Controller's basis for Lawfulness of Processing via its contract, it is the Data Controller's responsibility to ensure any changes in processing asked of QuantumIT fall within their chosen basis and within the confines of the agreed contract.

User Rights

As a Data Processor, QuantumIT processes User information based on the lawfulness of processing applied by the respective Data Controller. QuantumIT inherits this from the Data Controller as a result of being a contracted Data Processor. Where this Lawfulness of Processing is based on consent, the Data Controller - the User's HEI or Agency - will have recorded consent when the User initially signed up to their services.

If the User wishes to withdraw their consent, either from QuantumIT, or their Data Controller entirely, they would need to contact their Data Controller's Data Protection Officer or system administrator directly. These contact details can be found in the Data Controller's Privacy Notice.

Furthermore, a user can also ask what information the Data Controller has asked QuantumIT to hold about them, request a copy of this information, or ask to rectify or erase it (partially or in full) as part of their Right of Access, Right of Rectification and Right of Transparency as defined within the GDPR. A request for complete erasure will be treated as a user utilising their Right to be Forgotten, and all their personal data will be purged from InPlace Network. To use any of these rights, please contact the Data Controller's Data Protection Officer.

If a user wishes to raise a concern or complaint with a supervisory authority, QuantumIT recommends contacting the supervisory authority listed in the Data Controller's Privacy Notice.

Updating information

Whilst QuantumIT will make every effort to process accurate information about the User, please note that it is within the User's control to update the information QuantumIT hold when and where there is a discrepancy. If there is any incorrect information that the User is unable to modify directly, please contact the Data Controller, or raise a DSAR as described in the User Rights section.

Contact details

Please refer to the Data Controller's Privacy Notice for their Data Protection Officer's contact details.

To contact QuantumIT's Data Protection Officer, please use email:
dataprocessing@quantumit.com.au

To find out how InPlace Network can help you,
reach out to us today.

AU +61 (3) 8650 9800 | UK +44 (0) 207 0962 152
USA +1704 966 2100 | Asia/Middle East +60 173507677

info@inplacesoftware.com | www.inplacenet.com

© 2021 Quantum Information Technology Pty Ltd. ® All rights reserved.

