Layered Privacy Notice

Activity/Processing being undertaken: InPlace – Nursing Student Placement Administration System

Edinburgh Napier University is providing you with this information in order for us to comply with the General Data Protection Regulation (EU) 2016/679, which requires us to tell you what we do with your personal information.

Who is collecting the information?
Edinburgh Napier University as the "Data Controller".

Who are we sharing your Personal Data with (externally)?
The Edinburgh Napier University InPlace System is used to manage your placements and as such we will be sharing some of your information held on the system to external agencies (placement providers, NES).

Please note InPlace is a 3rd party software system (their privacy notice can be found below.

The University undertakes to maintain your information securely and will restrict access to employees, our professional advisers, authorised agents and contractors on a strictly need to know basis. We will only disclose your data to external third parties (other than any specified above) where we:

- Have your consent
- Are required to do so under a statutory or legal obligation, or
- Are permitted to do so by Data Protection legislation.

Why are we collecting it/what we are doing with it (purposes)?
In order to facilitate accredited work-based learning to enhance students' learning experience and contribute to their learning and education.

What is the legal basis for processing?
As part of the University's stated objects of providing education, research and general scholarship, as per the University's Statutory Instruments and to enable the University to fulfil any contractual obligations. General Data Protection Regulation Article 6. 1. (b) & (e) and 9 .2. (i) refer.

How are we collecting this information?
Part of the data will be transferred across from the University's student database (SITs) and part will be entered directly onto the InPlace system yourself.

What information are we collecting (whose information and what type of personal data)?
Nursing students:
Contact details, programme, status, health data (relating to compatibility to placements)

Who can see your information within the University?
Placements Team and relevant Academic staff

How long is your information kept?
Information will be held as per requirement for all Nursing Student records – 35 years after graduation.
Further information can be found online at:
https://staff.napier.ac.uk/services/governance-compliance/governance/records/Pages/RecordsRetentionSchedules.aspx

How secure is your information?
For services provided locally by Information Services, information is stored on servers located in secure University datacentres. These datacentres are resilient and feature access controls, environmental monitoring, backup power supplies and redundant hardware. Information on these servers is backed up regularly. The University has various data protection and information security policies and procedures to ensure that appropriate organisational and technical measures are in place to protect the privacy or your personal data.

The University makes use of a number of third party, including “cloud”, services for information storage and processing. Through procurement and contract management procedures the University ensures that these services have appropriate organisational and technical measures to comply with data protection legislation.

You can view InPlace’s Privacy Notice below.

Who keeps your information updated?
You can update your information yourself via SITs for contact details and directly on the InPlace system for health data.

Will your information be used for any automated decision making or profiling?
No

Is information transferred to a third country? Outside the EEA and not included in the adequate countries list.
No

Is any other information available?
You can access all the University’s privacy notices using the following link: https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Pages/statement.aspx

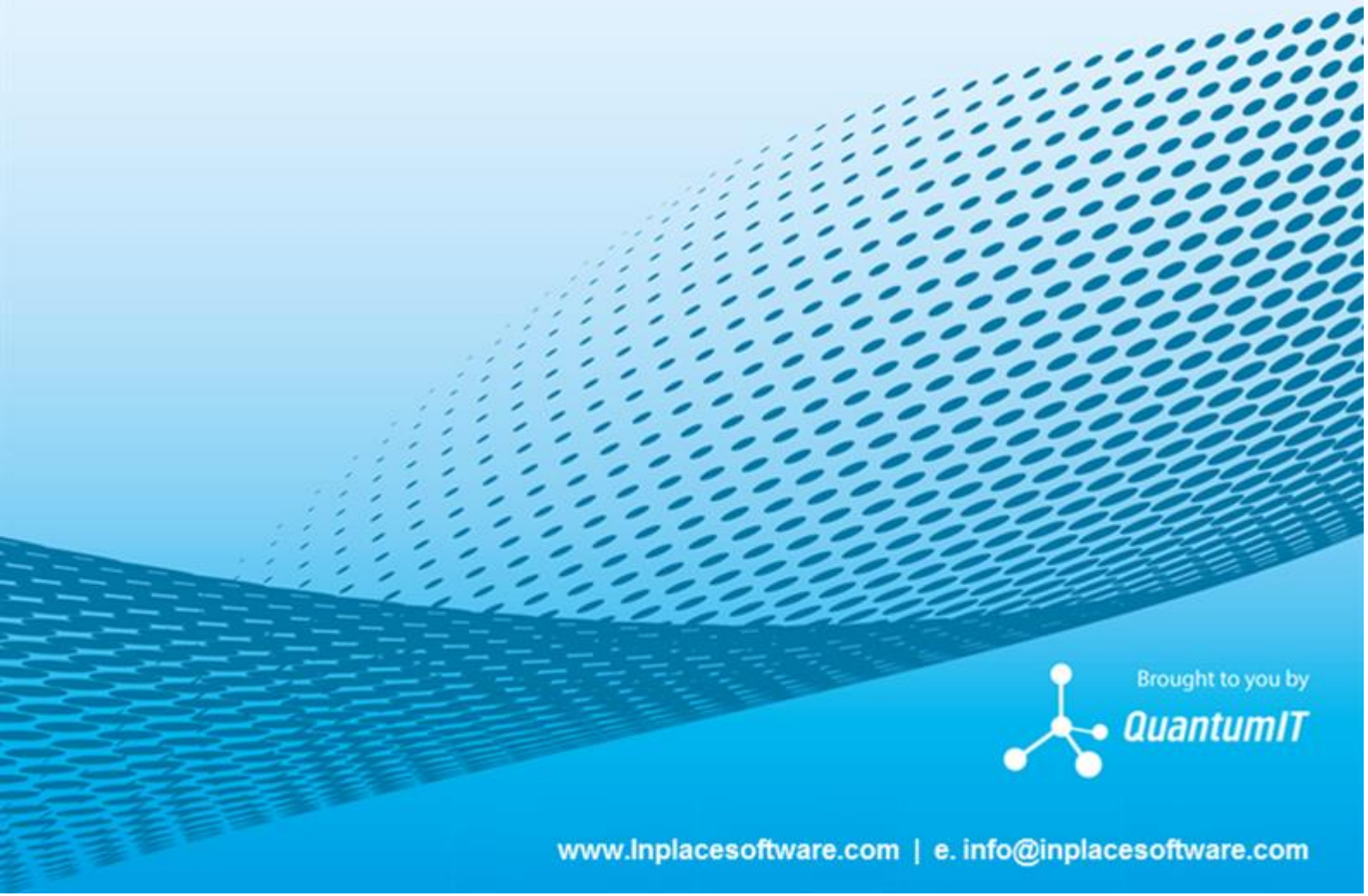
You have a number of rights available to you with regards to what personal data of yours is held by the University and how it is processed – to find out more about your rights, how to make a request and who to contact if you have any further queries about Data Protection please see the information online using the following URL: https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Pages/default.aspx

InPlace
Smart Placement Solutions

Quantum IT Solutions

InPlace Network Privacy Notice

Updated: May 2018



Quantum Information Technology Pty Ltd
100 Drummond Street
Carlton, Victoria, Australia 3053
+61 (03) 8650 9800

www.inplacesoftware.com
info@inplacesoftware.com

Contents

Introduction

The purpose of this Privacy Notice is to inform an InPlace Network user (“User”), how Quantum IT, 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. Quantum IT 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, Quantum IT’s Data Controllers have prioritised protecting the interests of their InPlace Network Users. Consequently, Quantum IT 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, Quantum IT 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, Quantum IT strongly recommend not exporting any information from InPlace Network. If Users feel compelled to

export personal information, Quantum IT 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. Quantum IT 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

Quantum IT 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, Quantum IT 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 Quantum IT to transfer student data to medical boards, government agencies or other organisations. When transferring data, Quantum IT 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 Quantum IT's Data Controllers, or when within the scope of Quantum IT'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). Quantum IT 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**
__StickyCientSessionId	InPlace Network 1.2+	Opens a session after validation confirmed.	Yes	Browser Session ends
__QuantumNetworkId	InPlace Network 1.2+	Confirms that __StickyCientSessionId is not a forgery.	Yes	Browser Session ends

Retention policy of data

As part of the Quantum IT Data Retention Policy, Quantum IT 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

Quantum IT 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 Quantum IT Security Policy.

Amendment clause

Quantum IT retain the right to amend this Privacy Notice at any time. As Quantum IT 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 Quantum IT fall within their chosen basis and within the confines of the agreed contract.

User Rights

As a Data Processor, Quantum IT processes User information based on the lawfulness of processing applied by the respective Data Controller. Quantum IT 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 Quantum IT, 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 Quantum IT 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, Quantum IT recommends contacting the supervisory authority listed in the Data Controller's Privacy Notice.

Updating information

Whilst Quantum IT 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 Quantum IT 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 Quantum IT's Data Protection Officer, please use email: dataprocessing@quantumit.com.