THE COURTYARD
General Data Protection Regulations 2018 – Recruitment & Selection

Privacy Statement
Here at The Courtyard we take your privacy seriously and will only use your personal information to administer your application for employment. This privacy statement explains what personal data we collect from you and how we use it. We encourage you to read the summaries below and if you would like more information on a particular topic please contact our Data Protection Officer.

Personal Data We Collect
We collect the following personal data relating to your employment application:
- Contact Details (Name, Address, Email Address, Telephone &/or Mobile Number)
- Employment history
- Qualifications
- Equality of Opportunity (Ethnicity, Disability Details) under Special Categories

How We Use Personal Data
Your personal data will be used to process your employment application.

How Long We Will Hold Personal Data
Successful candidate's data will be held under The Courtyard's General Data Protection Policy details of which will be made available upon the offer of employment. Full details are available in the staff handbook.

Unsuccessful candidates' data will be held of a period of 6 months whereupon it will be confidentially destroyed.

Reasons We Share Personal Data
We will not normally share personal data with anyone else, but may do so where:
- There is an issue that puts the safety of our staff at risk
- We need to liaise with other agencies or third parties (eg company pension provider). We will seek consent as necessary before doing this

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:
- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
  In connection with legal proceedings
- Where the disclosure is required to satisfy our legal obligations

How We Protect Your Personal Data
We use encrypted storage and transfer for all electronic data and have password access controls in place. If paper copies are utilised we ensure that all information is held in secure locked cabinets with controlled access by named individuals (currently the Administrator and members of the Leadership Team).

How to Access & Control Your Personal Data
Individuals have a right to make a 'subject access request' to gain access to personal information that the company holds about them. This includes:
- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing

- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or email to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary
- If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

Other data protection rights of the individual: In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

NOTE: Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.