CARDINAL CLINIC
Better Mental Health for a Brighter Future

Cardinal Clinic Employee & Self Employed Practitioner Privacy Notice

Cardinal Clinic is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect, use and disclose personal information about you during and after your working relationship with us, in accordance with the General Data Protection Regulation (GDPR).

It applies to all employees, workers and those with practising privileges.

Cardinal Clinic is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under the GDPR to notify you of the information contained in this privacy notice.

This notice applies to current and former employees, workers and those with practising privileges. This notice does not form part of any contract of employment or other contract to provide services.

We may update this Privacy Notice from time to time and will publish an up to date copy of the Privacy Notice on the Staff Notice Board and staff accessible area of the website.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

Data Protection Principles
We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

If you fail to provide personal information
If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of purpose
We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Lawful basis for data processing:
Processing takes place as part of your employment with the organisation. The lawful basis is in order to fulfil our contract with you and in order to meet our legal obligations.

Purposes for which we need your personal information and examples: (please note that these are illustrative and non-exhaustive)

Recruitment	To assess your suitability to work for or at the Clinic To conduct screening, assessments & interviews To maintain a library of correspondence To make offers and provide contracts of employment & practising privileges To conduct pre-employment checks, including determining your legal right to work and carrying out criminal records checks.
Human Resources (HR), finance and other business administration purposes	Staffing, including resource planning, recruitment, termination and succession planning Budgetary and financial planning and administration Payroll, including salary, salary reviews, tax, insurance & pensions To liaise with your pension provider Workforce development, education, training and certification Performance management Problem resolution, including carrying out internal review, grievances, audits To conduct business reporting and analytics Work related injury & illness, including the management of employee Health & Safety and disabilities Managing absence including sickness absence To communicate with you and facilitate communication between you and other people Risk management Training and quality purposes Use of consulting rooms & staff hours in relation to your practice
Security Access	Physical access control Authorising, granting, administering, monitoring and terminating access to the use of Cardinal Clinic facilities, records, property and infrastructure including communication services such as telephone, email and internet use CCTV Prevention and detection of crime
Information Technology (IT) administration purposes	IT systems access control and use monitoring IT fault reporting, management & resolution Systems administration, support, development, management and maintenance.
Legal purposes	To comply with our legal obligations, including criminal record checks.

What personal information do we collect from and about you?

Information about you	Name, address, date of birth, marital status, nationality, race, gender, religion, details of any disabilities and work restrictions.
Information to contact you at work or home	Name, address, telephone and e-mail addresses.
Information about who to contact in case of emergency	Name, address, telephone, e-mail address and their relationship to you.
Information to identify you	Photographs, passport and/or driving licence details, electronic signatures.
Information about your suitability to work for us	References, interview notes, work visas ID information such as passport details and driving licence information, records/results of pre-employment checks including criminal record, credit and fraud checks.
Information about your skills and experience	CVs, resumes and/or application forms, references, records of qualifications, skills, training and other compliance requirements.
Information about your terms of employment	Letters of offer and acceptance of employment, your employment contract or practising privilege contract.
Information that we need to pay you	Bank account details, national insurance or social security numbers (where applicable).
Information to provide you with benefits and other entitlements	Length of service information, health information, leave requests.
Information for you to access our buildings and systems	Computer or facilities access and authentication information, passwords, photographs (where applicable).
Information relating to your performance at work	Performance reviews, appraisals, records and/or notes of 1:1 and other meetings, personal development and/or improvement plans, revalidation documents, correspondence & reports.
Information relating to discipline, grievance and other employment related processes	Interview/meeting notes, correspondence.

How do we protect your personal information?
We have security arrangements in place to guard against unauthorised access, improper use, alteration, destruction or accidental loss of your personal information. We take extra care to protect particularly sensitive information. You are required to help with this by ensuring that your own personal information and that of your colleagues is kept secure.

How we use particularly sensitive personal information
"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal obligations or exercise rights in connection with employment or contracts.
3. Where it is needed in the public interest, such as for equal opportunities monitoring [or in relation to our occupational pension scheme].

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public

Our obligations as an employer
We will use your particularly sensitive personal information in the following ways:
We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.
We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, to ensure meaningful equal opportunity monitoring and reporting.

Do we need your consent?
We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions
We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us.

When do we share information?
We may have to share your personal data with third parties, including third-party service providers, such as professional advisors and providers of pensions and medical insurance and where we are under a legal obligation to do so, for example to prevent fraud or another criminal offence or because of a Court Order.

We require third parties to respect the security of your data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

We will use your records to be able to respond to reference requests after you have left the company.

Data Security

We have put in place measures to protect the security of your personal information. Details of these measures are available upon request.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Transferring personal data outside of the EEA
In some cases we may transfer your personal data to countries outside the European Economic Area, for example we may use cloud computer programmes where the servers are outside of the EEA.

Where we do so we will ensure that such transfers are compliant with GDPR and that appropriate measures are put in place to keep your Personal Data secure.

Your duty to inform us of changes
It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights
You can request access to or a copy of the information that we hold about you at any time by contacting the HR department.

You can request correction of the personal information that we hold about you, where it is incomplete or inaccurate.

You can request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. Legislation and good practice demands that we retain certain information (payroll, tax, HR records) for six years after the end of the financial year to which they relate. This also allows us to respond to reference requests after you have left the company. After this time records are destroyed confidentially.

You can object to/or restrict the processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

If you have any queries or concerns please address them to:

Chief Privacy Officer
Bishops Lodge Limited T/A Cardinal Clinic
Oakley Green
Windsor SL4 5UL