

Privacy Notice

Candidate

1: WHAT IS THE PURPOSE OF THIS DOCUMENT?

Ulster Independent Clinic is committed to protecting the privacy and security of your personal data.

You have received a copy of this privacy notice because you have applied to work with us, whether as an Employee, Worker or independent contractor as a Consultant or GMP member with practicing privileges (all Candidates). This privacy notice describes how we collect and use a Candidates personal data during any recruitment or membership application exercise. This privacy notice also provides information in respect of your privacy rights and how the law protects you.

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

If you are successful in your application, please see our Employee and Worker Privacy Notice or Consultant with Practising Privileges and Non-Consultant Grade Doctors Practising Privileges Privacy Notice (whichever applicable) for further information in respect of how the Clinic processes your personal data.

2. WHO WE ARE AND GENERAL INFORMATION

CONTROLLER

Ulster Independent Clinic is the “data controller” and is responsible for any of your personal data we hold (collectively referred to as the “Clinic”, “we”, “us” or “our” in this privacy notice). This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection law to notify you of the information contained in this privacy notice.

CONTACT DETAILS

If you have any questions about this privacy notice, including how we handle your personal data or if you wish to exercise your legal rights or make a complaint about how we have handled your data, please contact our Data Protection Officer (**DPO**), in one of the following ways:

Email: secretary@uic.org.uk.

Postal Address: Data Protection Officer
Ulster Independent Clinic
245 Stranmillis Road
Belfast
BT9 5JH.

Telephone: 028 9066 1212.

You are required to raise any complaint or concern with us directly in the first instance, however, if you remain dissatisfied you have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk).

CHANGES TO THIS PRIVACY NOTICE AND YOUR DUTY TO INFORM US OF CHANGES

We keep our privacy notice under regular review. This version was last updated on 19/06/2026. We ensure that any updates to this privacy notice shall be circulated to you by email to the email address you have supplied.

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your application process.

3: DATA PROTECTION PRINCIPLES

We will comply with data protection law, which says that the personal data 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.

4: THE KIND OF DATA WE HOLD ABOUT YOU

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the person's identity has been permanently removed (anonymous data).

There are certain types of more sensitive personal data which require a higher level of protection, such as information about a person's health, religion or race, which are called "special category data".

We will collect, store, and use the following categories of your personal data:

- **Contact Data** - personal contact details such as name, title, addresses, telephone numbers, personal and work email addresses.
- **Identity Data** - personal details such as date of birth, gender and marital status.
- **Application Data** – information collected during the application process including your curriculum vitae, reference statements, details of your education and qualifications, professional records, employment history, previous job titles, training history and professional membership information together with any further application documentation completed and submitted by you.
- **Image Data** – visual images, personal appearances and behaviour of individuals (but not sound) shall be collected by our CCTV if you attend the publicly accessible parts of our property.
- **Audio Data** – recordings of phone calls, which are taken for training and complaint management purposes.
- **Scope of Practice Data** – being your areas of practice speciality.
- Any further information that you disclose or choose to provide to us during the application process.

We will also collect, store and use the following more sensitive types of personal data:

- **Health Data** – details of your vaccinations and immunisations (as updated from time to time) as required under our obligations to RQIA, report submitted by Occupational Health together with any other Health Data that may be relevant to your application.
- **Sexual Orientation Data** – this may be passively collected when you identify your next of kin or marriage status. We do not actively request disclosure of this type of data.
- **Criminal Offence Data** – may be collected through an Access NI check, should the check return details of any convictions, cautions, barring services or other such information held by the police.

5: HOW IS YOUR PERSONAL DATA COLLECTED?

The Clinic will use different methods to collect personal data from and about you, including through:

- **Direct interactions** – primarily we collect personal data about you directly from you through the application process.
- **Third-parties** – in some circumstances, we shall receive personal data from the following third-party sources: your referees, your employer; agency firm, your responsible officer, Access NI or other background check provider.

6: HOW WE WILL USE YOUR PERSONAL DATA

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- In order to take steps prior to entering a contract with you.
- Where we need to comply with a legal obligation.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests

We may also use your personal data in the following situations, which are likely to be rare:

- Where it is needed in the public interest.

We have set out below a description of the ways we plan to use your personal data and sensitive data and which of the legal bases (legal grounds) we rely on to do so. Note that we may process your personal data on more than one legal basis, when several grounds exist.

Purposes	Description	Type of personal data	Lawful basis
To process and consider the application of a Candidate.	We will collect and process personal data before you are engaged as an Employee, Worker or Consultant member, from you and third parties as identified above. This will allow us to take the necessary steps required to assess your application, including verifying your identify, ensuring you are suitably qualified for the subject role and where applicable that	Contact Data Identity Data Application Data Scope of Practice Data	Save for as further identified below, it is necessary for us to process the data appearing opposite: (i) in order to take steps prior to entering a contract with you; (ii) necessary for our legitimate interests to keep our records updated; and

	<p>you are legally entitled to work as a medical professional.</p>	<p>Health Data</p> <p>Sexual Orientation Data (if disclosed by you)</p> <p>Criminal Offence Data</p>	<p>(iii) to comply with legal obligations.</p> <p>Necessary to process your Health Data to comply with our legal obligations to RQIA, for reasons of public interest in the area of public health and necessary pursuant to taking steps prior to entering a contract with any Candidate, being healthcare professionals.</p> <p>Necessary to process your Sexual Orientation Data in order to take steps prior to entering a contract with any Candidate, where such processing is carried out in the course of the Clinic's legitimate activities with appropriate safeguards as a not for profit body.</p> <p>Necessary to process your Criminal Offence Data in order to take steps prior to entering a contract with any Candidate. Further it is necessary to process your Criminal Offence Data for the purposes of protecting the public against dishonesty and for protecting individuals under 18 or who are at risk from harm. The lawful basis for Criminal Offence Data processing is further set out in our Appropriate Policy Document.</p>
<p>Management of the Clinic</p>	<p>For the proper conduct and management of the Clinic we shall process your personal data for management, planning and auditing purposes.</p>	<p>Contact Data</p> <p>Identity Data</p> <p>Application Data</p>	<p>We have a legitimate interest to process in these circumstances for the running of the Clinic and for the administration of the Clinic's operations.</p>
<p>Investigation of Complaints</p>	<p>It may be necessary to process personal data to investigate a complaints received from you in</p>	<p>Contact Data</p> <p>Identity Data</p>	<p>We have a legitimate interest in maintaining a complaint-handling service.</p>

	respect of the application process.	Application Data Audio Data	
CCTV	We operate CCTV throughout our premises (excluding wards, consulting rooms and theatres) to protect the property, our staff, our third-party contractors and patients. Our CCTV facilities record images only. Should you attend at our premises during the application process, your Image Data may be captured by our CCTV.	Image Data	We have a legitimate interest to ensure safety and security of patients, staff, contractors, visitors and our property and to also deter crime.
Telephone recording	Telephone enquiries may be recorded for training and quality purposes.	Audio Data (together with any other data you may disclose over the telephone)	We have a legitimate business interest in ensuring that all telephone enquiries are dealt with effectively.
Fraud Prevention	We may process your personal data to verify your identity, to prevent fraud, and to comply with anti-bribery obligations.	Contact Data Identity Data	We have a legitimate business interest to minimise fraud that could be damaging for patients and us. Necessary for compliance with legal obligations to which we are subject.
Enforcement of legal rights and defence of legal claims	We may process your personal data for the purposes of protecting our legal rights and defence of legal claims.	Contact Data Identity Data	We have a legitimate business interest to protect our business, interests and rights.
Data Subject Access Requests	We may process your personal data pursuant to a Data Subject Access Request to fulfil our legal obligation under the data protection laws.	Any personal data we hold in respect of you which falls within the scope of any access request you submit	Necessary for the purposes of compliance with the Data Protection Act 2018.

CHANGE OF PURPOSE

We will only use your personal data 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 data 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 data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

DO WE NEED YOUR CONSENT?

We do not need your consent if we use your personal data and sensitive data in accordance with our written policy to carry out our contractual or legal obligations and where we have a lawful basis to do so as identified above. Should we require your consent to process your personal data, we will provide you with full details of the data 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.

7: DATA SHARING

We may have to share your data with third parties, including other data controllers and third-party service providers. We require third parties to respect the security of your data and to treat it in accordance with the law. If we do, you can expect a similar degree of protection in respect of your personal data.

WHY MIGHT WE SHARE YOUR PERSONAL DATA WITH THIRD PARTIES?

We will only share your personal data with third parties where required by law, as required to take steps before entering a contract with you or when it is in our legitimate business interests as identified within the table above. We will only share personal data as necessary to achieve the purpose of the processing.

WHO WE SHARE YOUR PERSONAL DATA WITH

Other Data Controllers

We will share your personal data with the parties set out below in their capacity as controllers:

- your employer;
- your referees;
- our auditors as we may engage from time to time, who may on occasion request certain data sets which comprises your personal data; and
- our legal representatives, in connection with the defence of any claim or other analogous legal advice.

Third-party Processors

We will share your personal data with the following third-party service providers we engage, acting as data processors:

- our hardcopy storage providers we may instruct;
- third party providers who supply IT support and maintenance services in respect of our systems and equipment, which include, Acorn, Toadstool Technologies, together with other such providers; or
- providers of shredding services who we appoint from time to time.

SECURITY OF MY PERSONAL DATA SHARED WITH THIRD PARTY SERVICE PROVIDERS

All our third-party service providers are required to take appropriate security measures to protect your personal data in line with our policies and to treat your personal data in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and they are only permitted to process your personal data for specified purposes and in accordance with our instructions.

8: TRANSFERS OF PERSONAL DATA OUTSIDE THE UK

We do not transfer the personal data of candidates outside the United Kingdom. Should this change, we shall update this privacy notice and advise of the measures we take to ensure the security of your personal data.

9: DATA SECURITY

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know.

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

10: DATA RETENTION

We will only retain your personal data for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory or statutory reporting requirements. We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect of our relationship with you.

To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory or other requirements.

Below are the retention periods for the personal data we process in respect of candidates:

	Type of Data or Record	Retention Period
1	Application Data	12 months after notifying unsuccessful candidates. For successful candidates, for the duration of the contract/agreement and 3 years after termination of your contract
2	Access NI application form	3 months after Access NI vetting is complete

11: RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION

INFORM US OF CHANGES

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your treatment.

YOUR RIGHTS

Under certain circumstances, you have rights under data protection laws in relation to your personal data. Under such laws, you have the right to:

- **Request access** to your personal data (commonly known as a “data subject access request”). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal data that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have exercised your right to object to processing (see below). Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons, which will be notified to you (if applicable) at the time of your request.
- **Object to processing** of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms.
- **Request the restriction of processing** of your personal data. This enables you to ask us to suspend the processing of personal data about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal data to another party.

If you want to review, verify, correct or request erasure of your personal data, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact our DPO.

WITHDRAWING CONSENT

If we are relying on your consent to process any of your personal data, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact our DPO. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.