highlandbroadband.com

0330 236 9900

Suite 2, Ground Floor Orchard Brae House,
30 Queensferry Road, Edinburgh, EH4 2HS

Recruitment Privacy Policy

Introduction

Highland Broadband Networks Ltd, ("us", "our" or "we") operate under the brands "HBNL", "Highland Broadband", "Lothian Broadband", and "Highland Wireless". We are committed to respecting your privacy and protecting your personal data. We define personal data broadly as information that directly identifies an individual or that makes an individual identifiable when combined with other information.
This Recruitment Privacy Notice ("Privacy Notice") describes how we handle and protect your personal data in connection with our recruitment processes and activities. In case of a conflict between this Privacy Notice and applicable law, applicable law will govern.

This Privacy Notice only applies to the personal data of:

- job applicants;
- potential candidates for employment or partnership; and,
- individuals who participate in our recruiting programs and events.

This Privacy Notice does not apply to the personal data of our employees, partners, clients, vendors or any other person from whom we collect personal data for other purposes, please refer to our general privacy policy.

How Data is Collected

- This personal data is submitted directly to us through the online application process and follow-up communications
- Through alternative channels (e.g., via professional recruiting firms).
- We may also collect and process your publicly available data when we engage in proactive searches on job boards and professional networking sites such as LinkedIn.
- Data is also collected from other sources provided by you such a reference checks and eligibility checks

By submitting your personal data to us, you acknowledge that:

- You have read and understood this Privacy Notice and agree to the use of your personal data as set out herein.
- Although our operations are mainly UK based, your personal data may be transferred and processed worldwide, including in countries that may not be deemed to provide the same level of data protection, for the purposes and in the manner specified in this Privacy Notice.
- You are not required to provide any requested information to us, but your failure to do so may result in our not being able to continue your candidacy for the job for which you have applied.

- All your representations are true and correct to the best of your knowledge and belief, and you have not knowingly omitted any relevant information. Providing any inaccurate information may make you ineligible for employment.
- This Privacy Notice does not form part of any contract of employment offered to candidates hired by us.

Personal data we collect

We usually collect personal data directly from you when you apply for a role with us, such as your name, address, contact information, photographs and videos, work and educational history, achievements, identity documents, and test results.

If you receive an offer from us, we may then conduct a background check and, where relevant to the job and permitted by applicable law, we may also collect data related to criminal offences and proceedings.

We also collect similar personal data about you from third parties, such as professional recruiting firms, your references, prior employers, our employees with whom you have interviewed or who recommended your candidacy, and employment background check providers.

We may also collect personal data about you online to the extent that you have chosen to make this information publicly available. For example, we may find your profile on professional social media websites (such as LinkedIn), and contact you about suitable roles.

Sensitive personal data

Sensitive personal data is a subset of personal data that includes ethnicity, health, trade union membership, philosophical beliefs, sexual orientation, and other categories as prescribed by law. We may collect sensitive personal data about a candidate to the extent permitted to do so by applicable equal opportunity law and to support our efforts to create an inclusive and diverse work environment.

We may also collect sensitive personal data to the extent that a candidate chooses, without being asked, to voluntarily disclose it during the recruiting process. Under limited circumstances and to the extent permitted by applicable law, we may also collect sensitive personal information relating to health and medical characteristics, such as status of infection, test results, and vaccination status, to address our public health and workplace safety obligations and to protect the business and its employees, clients, and third parties.

How we use your data

We collect and use your personal data for legitimate human resources and business management reasons, including:

- identifying and evaluating candidates for potential employment, as well as for future roles that may become available;
- maintaining records in relation to recruiting and hiring;
- ensuring compliance with legal requirements, including those relating to public health and workplace safety;
- fostering our diversity and inclusion programs and practices;
- conducting background checks relevant to the role and applicable law, including where appropriate criminal history checks;
- protecting our legal rights to the extent authorised or permitted by law;
- protecting the workplace and communicating with medical professionals, law enforcement, or other public authorities in the event of an emergency or public health event, such as when the health or safety of you or one or more individuals may be endangered, including, to the extent permitted by applicable law, sharing data about the status of an infection, test results, and vaccination status; and,
- We may also use your personal data for inhouse analytical purposes, including in aggregated/pseudonymized form, to improve our recruitment and hiring process and improve our ability to attract successful candidates.

How we process your data

Our processing of your personal data for the purposes mentioned above is based:

- in part, on our legitimate business interests in evaluating your application to manage our relationship with you, to ensure that we recruit appropriate employees, and to evaluate and maintain the efficacy of our recruiting process more generally; and in operating our business and protecting the Firm and its employees, clients, and third parties;
- in part, on our performing contractual and precontractual measures relating to our potential employment relationship with you;
- in part, on our complying with applicable law with regard to personal data necessary to satisfy our legal and regulatory obligations, including with regard to public health and workplace safety; and,
- in part, on your consent, if we offer you the opportunity to participate in our optional recruiting programs or if we collect sensitive personal data for legally permitted purposes other than compliance with our legal obligations regarding public health and workplace safety.

Background screening

If you receive an offer from us, we may conduct a background check on you or instruct a third party to do so on our behalf. Background screening will only be done where permitted by the law applicable to the location where the position is located and to the extent necessary and proportionate to the role that you are being offered. A background check will only involve criminal background data to the extent permitted by law. Our legal basis for background screening is our need to perform precontractual measures related to establishing our employment relationship. If a background screening is required, you may be contacted by a third-party background screening service provider to request authorisation for the release of your information, and at that time you will be

provided with further information about the process and what personal data it might involve.

Automated decisions

Within our recruitment system we may use software to assist us in the review applications. The software may determine suitability for a specific role via targeted questions relating to the role, and/or may identify and select individual personal information according to the stored characteristics. For example, the software may enable us to quickly identify individuals from our database who have specific skills, e.g. an engineer and exclude individuals whose characteristics do not match particular requirements of a job role (required languages etc). Applications that do not meet those requirements will be automatically rejected.

The automated results are always considered in tandem with, and not in lieu of, human judgement. We evaluate each individual candidate on their own merits.

Your consent

By applying for a role with us directly or via a recruitment service provider, or by opting in when presented with choices, you have consented for us to use your information in the following ways:

- to process your application for a job with Highland Broadband and affiliate organisations;
- to advise you of future job opportunities with Highland Broadband and affiliate organisations;
- to enable you to contact us and for us to respond to you; and,
- to conduct analytics and generate internal reports about recruitment activity
- to track which jobs you search for, view, and apply to.

We do not share your personal data with third parties other than for the sole purpose of processing your application (see data recipients below). This Company will not sell trade or rent your personal information to others.

Access to and Storage of Your Personal Information

Your data is submitted to Us and to assess your suitability for our roles we must process personal data (including when legally required, special category or 'sensitive' personal data). In so doing, the Company acts as a data controller. Data is stored in our applicant tracking system provided by our recruitment software partner (Hireful Ltd). We have limits in place on this system controlling wo has access to view and/or share your data.

GDPR imposes restrictions on the transfer of data outside of the EU. Hireful Ltd use EU based datacentres you can find out more about Hireful's GDPR processes and data storage here.

When you apply for a job via our system, this information is stored in our applicant tracking system, we will only hold this information for as long as the purpose for which the data was collected continues for employment regulations this would typically be one year. It is then archived or destroyed unless its retention is required to satisfy audit, legal, regulatory, or accounting requirements or to protect our interests.

If you accept an offer of employment with us, any relevant personal data collected during your pre-employment period will become part of your personnel records and will be retained in accordance with legal requirements and with the privacy notice applicable to our employees.

If we do not employ you, we may nevertheless continue to retain and use your personal data for a period 12 months for system administration purposes, to consider you for potential future roles, and to perform research. Thereafter, we retain a minimal amount of your personal data to record your recruiting activity with us.

To the extent that we have collected personal data, including sensitive personal data, for the specific purpose of fulfilling our legal obligations regarding public health or workplace safety, we will retain that data for the duration of those legal obligations. Thereafter, we retain a minimal amount of your personal data to establish our compliance with those obligations.

We may want to remain in contact with you and consider you for future employment opportunities. In such an event, we will seek your consent to stay in touch with us, either prior to or after you formally apply for a job opportunity. You will be asked to renew your consent annually.

Data recipients and international data transfers

Your personal data may be accessed by recruiters and interviewers working in the UK where we are based. Individuals performing administrative functions and IT personnel within our organisation may also have limited access to your personal data to the extent necessary perform their jobs.

We use third-party service providers to provide a recruiting software system. We also share your personal data with other third-party service providers that may assist us in identifying and recruiting talent, administering and evaluating pre-employment screening and testing, and improving our recruiting practices.

Except to the extent necessary to process your application for a job, we do not disclose your personal data to third parties. We also prohibit our service providers from using your personal data other than for the purposes outlined in this document. We do not otherwise share or sell your personal data to third parties.

In addition, we may disclose or transfer your personal data in the event of a re-organization, merger, sale, joint venture, assignment, or other transfer or disposition of all or any portion of our business.

Security

We use generally accepted standards of technical and operational security to secure your personal data. Only authorized personnel of Highland Broadband and of our third-party service providers are permitted to access personal data, and these employees and third-party service providers are required to treat this information as confidential. Despite these precautions, we cannot guarantee that unauthorized persons will not obtain access to your personal data.

Your rights

We take the protection of your personal data very seriously and it is important that you know your rights within that context, which include rights to:

- Request a copy of the personal data that we hold;
- Object to our processing of your data where that processing is based upon legitimate interest and there are no compelling grounds for the continued processing of that data;
- Request that we restrict processing of your data in certain circumstances;
- Request that data is erased where the continued use of that data cannot be justified;
- Object to any decision, which significantly affects you, being taken solely by a computer or via another automated process;
- Withdraw your consent to our processing of your personal data for a particular purpose at any stage. However, please note that we may continue to retain, or otherwise use your personal information thereafter where we have a legitimate interest or a legal or contractual obligation to do so. Our processing in that respect will be limited to what is necessary in furtherance of those interests or obligations;
- Request that inaccurate or incomplete data is rectified;
- Request that data provided directly by you and processed by automated means is transferred to you or another controller; this right only being applicable where our processing of your data is based either on your consent or in performance of a contract;
- Make a complaint to the Information Commissioner's Office;
- Request that direct marketing by us to you is stopped; and,
- Please note that should you exercise your right to request that we erase data or cease any processing activity, we may retain a record of this request and the action taken in order to both evidence our compliance, and to take steps to minimise the prospect of any data being processed in the future should it be received again from a third party source.

If you would like to make a request to access, review, correct, delete or port the personal data we have collected about you, to assert a right with regard to your personal data, or to discuss how we process your personal data, please use the contact information at the end of this Privacy Notice.

To help protect your privacy and security, we will take reasonable steps to verify your identity before granting you access to your personal data. We will make reasonable attempts to promptly investigate, comply with, or otherwise respond to your requests as may be required by applicable law. Depending upon the circumstances and the request, we may not be permitted to provide access to personal data or otherwise fully comply with your request; for example, where producing your information may reveal the identity of someone else. We reserve the right to charge an appropriate fee for complying with your request where allowed by applicable law, and/or to deny your requests where, in the Firm's discretion, they may be unfounded, excessive, or otherwise unacceptable under applicable law.

Cookies and other tracking technologies

We may use first party and third-party cookies, web beacons, pixels, clear gifs, and other similar technologies (collectively "Cookies and Other Tracking Technologies") to identify you and your interests, to remember your preferences, and to track your use of our websites. We also use Cookies and Other Tracking Technologies to control access to certain content on our websites, to protect the websites, and to process any requests that you make of us.

Some of our online recruiting activities are hosted by third parties. When you access sites operated by these third parties, they may, consistent with our Cookie Policy, place their own Cookies or Other Tracking Technologies on your device. You can learn more about our use of Cookies and other tracking technologies by reading our Privacy Policy and Cookie Policy.

Contacts

If you have any questions about this Privacy Notice or if you would like to communicate with us about Data Privacy, please contact us at: compliance@hbnl.com

Changes to this Policy

We reserve the right to modify this Privacy Notice. We will post any changes to our Privacy Notice on this page. Please check this page regularly to keep up-to-date.